International Journal of Computer Applications Technology and Research
Volume 3– Issue 11, 661 - 663, 2014

Protecting Global Records Sharing with Identity Based Access Control List

Vidhya . P
Computer Science and Engineering
V.S.B Engineering College
Tamilnadu, India

A.P.V Raghavendra
Computer Science and Engineering
V.S.B Engineering College
Tamilnadu, India

Abstract: Generally, the information is stored in the database. Protecting sensitive information are encrypted before outsourcing to a service provider. We send the request to service provider through SQL queries. The query expressiveness is limited by means of any software-based cryptographical constructs then deployed, for server-side query working on the encrypted data.Data sharing in the service provider is emerging as a promising technique for allowing users to access data. The growing number of customers who stores their data in service provider is increasingly challenging users' privacy and the security of data. The TrustedDB an outsourced database prototype that allows clients to execute SQL queries with privacy and under regulatory compliance constraints by leveraging server-hosted. Tamper-proof believed hardware in crucial query processing levels, thereby removing any limits on the type of supported queries. It focuses on providing a dependable and secure data sharing service that allows users dynamic access to their information. TrustedDB is constructed and runs on hardware, and its performance and costs are evaluated here.

Keywords: Database architectures, security, privacy, special-purpose hardware**.**

1. INTRODUCTION

Although the benefits of outsourcing and clouds are well known, imperative challenges yet lie in the path of large-scale adoption since such services often require their customers to inherently trust the provider with full access to the outsourced data sets. Numerous instances of illicit insider behavior or data leaks have left clients backward to place known data under the control of a private, unknown provider, without practical assurances of privacy and confidentiality, especially in occupation, healthcare, and public sectors. Moreover, today's privacy assurance for such services are at best informative and subject customers to unreasonable fine-print clauses. For example, allowing the server operator to use customer behavior and content for commercial profiling or governmental control purposes.

Existing analysis addresses several such safety aspects, including entry's privacy and finds on enciphered data. In most of these efforts, data are encrypted before outsourcing. Once enciphered however, essential limitations in the types of basic operations that can be performed on encrypted data lead to fundamental expressiveness and practicality constraints. However, recent insights into the cost performance tradeoff seem to suggest that things stand somewhat differently. Specifically, at scale, in outsourced contexts,computation inside secure processors is orders of degree lower than any equivalent cryptographic operations performed on the provider's unsecured server hardware, despite the overall higher achievement cost of secure hardware.

We conclude that a complete privacy enabling secure database leveraging server-side trusted hardware can be built and run at a fraction of the cost of any (existing or future) cryptography-enabled private data working on common server hardware. We verify this by signing and building TrustedDB, an a SQL database processing engine that makes use of tamper-proof cryptographic coprocessors such as the IBM 4764 [1] in close adjacency to the outsourced data.

Change opposes designs, however, is imperatively constrained in both computational ability and memory capacity which makes implementing fully featured database solutions using secure coprocessors (SCPUs) very demand. Trusted complete this by applying common unsecured server resources to the maximum available duration. For example, Trusted permits the SCPU to clearly access external storage while protecting data confidentiality in the family of encryption. This removes the limitations on the size of databases that can be supported. Moreover, client queries are preprocessed to identify knowing components to be run inside the SCPU. Non knowing operations are offloaded to the interested server owner. This highly increases work and decrease the cost of the agreement.

Overall, despite the overheads and performance limitations of trusted hardware, the costs of running TrustedDB are orders of degree lower than any (existing or) potential future cryptography-only mechanisms. Moreover, it does not limit query expressiveness. This paper's improvement is triples:1)The opening of current cost setups and judgments that explain and specify the advantages of utilizing trusted hardware for data working, 2) the design and advancement of TrustedDB, a reliable hardware based relational database with full data confidentiality and no limitations on query expressiveness, and 3) defined query optimization approach in a trusted hardware-based query execution model.

2. RELATED WORK

Queries on encrypted data. To propose a division of data into secret partitions and rewriting of range queries over the original data in terms of the resulting separation qualifiers. This balances a judge between client and server-side working, as a function of the data subdivision size. Some authors explore optimal bucket sizes for range queries.

Vertical partitioning of relations amongst multiple untrusted servers is employed in [2]. Here, the privacy goal is to a prevent access of a subset of attributes by any single server. For example, {Name, Address} can be a privacy sensitive access-pair and query processing needs to ensure that they are not jointly visible to any single server. The client query is split into multiple queries wherein each subquery fetches the relevant data from a server and the client combines results from multiple servers. TrustedDB is equivalent to when the size of the privacy subset is one and hence a single server answers. In this case, each attributes column demand encryption to ensure privacy. Hence, TrustedDB to optimize for querying encrypted columns since otherwise they rely on client-side decryption and processing.

To introduce the concept of logical fragments to achieve the same partitioning effect on a single server. A fragment here is simply a relation wherein attributes not desired to be visible in that fragment are encrypted. TrustedDB (and other solutions) are in effect concrete mechanisms to efficiently query any individual fragment from [10]. The work on the other hand, can be used to determine the set of attributes that should be encrypted in TrustedDB.

The goal is to minimize the lifetime of sensitive data and keys in server memory after decryption. In TrustedDB, there is no such disclosure risk since decryptions are performed only within the SCPU. In TrustedDB, all decryptions are performed within the secure confinements of the SCPU, thereby processing is done on the plaintext data. This removes any limitation on the nature of predicates that can now be employed on encrypted attributes including arbitrary user decided functions. We note that certain solutions destined for a very specific set of predicates can be more efficient albeit at the loss of functionality.

Trusted hardware. In [4], SCPUs are used to retrieve X509 certificates from a database. However, this only supports key based lookup. Each record has a single key and a user can query for a record by specifying the key. Multiple SCPUs are used to provide key based search. The entire database is scanned by the SCPUs to return matching records. Chip-Secured Data Access [5] uses a smart card for query processing and for enforcing access rights. The client query is split such that the server performs the majority of the computation. The solution is limited by the fact that the client query executing within the smart card cannot generate any intermediate results since there is no storage available on the card. In follow-up work, GhostDB [6] proposes to embed a database inside a USB key equipped with a CPU. It allows linking of private data carried in the USB Key and public data available on a server. Ghost DB ensures that the only information revealed to a potential spy is the query issued and the public data accessed.

Both [5] and [6] are subject to the storage limitations of trusted hardware which in turn limits the size of the database and the queries that can processed. In contrast, TrustedDB uses external storage to store the entire database and reads information into the trusted hardware as needed which enables it to be used with large databases. Moreover, database pages can be swapped out of the trusted hardware to external storage during query processing.

3. MODULES DESCRIPTION

A. Query Parsing and Execution

In the first stage a client defines a database schema and partially occupy it. Knowing attributes are noted using the SENSITIVE keyword which the client layer transparent processes by encrypting the corresponding attributes:

```
CREATE TABLE customer (ID integer
    primary key,
Name char (72) SENSITIVE, Address
    char (120)  SENSITIVE).
```

(1) Later, a client sends a query request to the host server through a standard SQL interface. The query is clearly enciphered at the client site using the public key of the SCPU. The server owner thus cannot decipher the query.
(2) The server owner serves the enciphered query to the Request Handler inside the SCPU.
(3) The Request Handler deciphers the query and serves it to the Query Parser. The query is parsed achieving a set of ideas. Each idea is worked by editing the original client query into a set of sub-queries, and, presenting to their end data set allocation, each sub-query in the idea is qualified as being either public or private.
(4)The Query Optimizer then evaluates the execution costs of each of ideas and selects the best idea (one with least cost) for execution serving it to the dispatcher.
(5) The Query Dispatcher serves the public queries to the server owner and the private queries to the SCPU database engine while handling responsibilities. The net result is that the maximum possible work is run on the server owner reduced cycles.
(6) The final query result is assembled, enciphered, digitally signed by the SCPU Query Dispatcher, and dispatched to the client.

B. Query optimization process

At a high level query optimization in a database system works as follows. (i) The Query Plan Achiever works possibly multiple ideas for the client query. (ii) For each worked idea the Query Cost Evaluator computes an evaluate of the execution cost of that idea. (iii) The best idea i.e., one with the lowest cost, is then selected and passed on to the Query Idea Interpretor for execution. The query development process in TrustedDB works similarly with key differences in the Query Cost Evaluator due to the logical separating of data mentioned above.

C. System Catalog

Any query idea is composed of multiple individual execution steps. To evaluate the cost of the entire idea it is essential to evaluate the cost of individual steps and combine them. In order to evaluate these costs the Query Cost Evaluator needs access to some key information. E.g., the possibility of an index or the knowledge of possible distinct values of an attribute. These sets of instruction are collected and stored in the System Catalog. Most available databases today have some form of the continuously updated System Catalog.

D. Analysis of Basic Query Operations

The cost of an idea is the separate of the cost of the steps that comprise it. In this section we present how execution times for a certain set of basic query idea steps are evaluated.

4. SYSTEM FLOW DIAGRAM

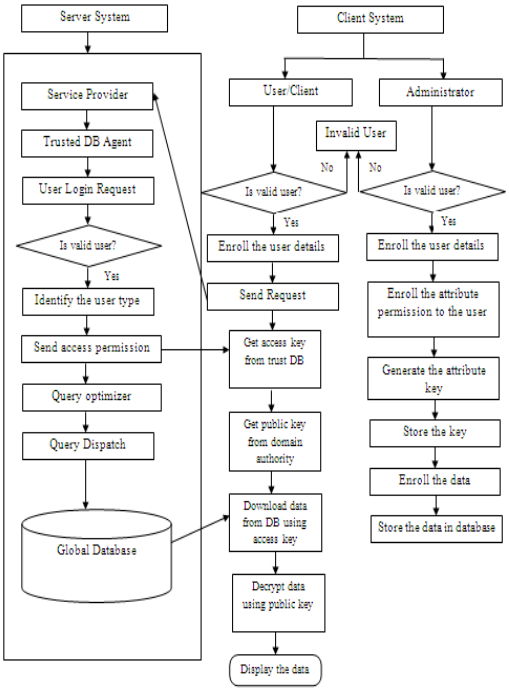


Fig: 1 System Flow Diagram

A client sends a query request to the host server through a standard SQL interface. The query is clearly enciphered at the client site using the public key of the SCPU. The server owner thus cannot decipher the query. The server owner serves the enciphered query to the Request Handler inside the SCPU. The Request Handler deciphers the query and serves it to the Query Parser. The query is parsed achieving a set of ideas. Each idea is worked by editing the original client query into a set of sub-queries, and, presenting to their end data set allocation, each sub-query in the idea is qualified as being either public or private. The Query Optimizer then evaluates the execution costs of each of ideas and selects the best idea (one with least cost) for execution serving it to the dispatcher. The Query Dispatcher serves the public queries to the server owner and the private queries to the SCPU database engine while handling responsibilities. The net result is that the maximum possible work is run on the server owner reduced cycles. The final query result is assembled, enciphered, digitally signed by the SCPU Query Dispatcher, and dispatched to the client.

4. CONCLUSION

This paper's improvement are triples:
1)The opening of current cost setups and judgments that explain and specify the advantages of utilizing trusted hardware for data working, 2) the design and advancement of TrustedDB, a reliable hardware based relational database with full data confidentiality and no limitations on query expressiveness, and 3) defined query optimization approach in a trusted hardware-based query execution model.

This work's inherent proposal is that, at order, in expand contexts, computation inside secure hardware processors is orders of degree lower than equivalent cryptography performed on suppliers' unsecured server hardware, even though the overall higher achievement cost of protected hardware. We thus propose to make reliable hardware a first-class member in the secure data management field. Moreover, we promise that cost-centric insights and architectural standards will fundamentally change the way systems and algorithms are signed.

5. REFERENCES

[1] IBM 4764 PCI-X Cryptographic Coprocessor, http://www03.ibm.com/security/cryptocards/pcixcc/overview.shtml, 2007.

[2] V. Ganapathy, D. Thomas, T. Feder, H. Garcia-Molina, and R.Motwani, "Distributing Data for Secure Database Services," Proc.Fourth Int'l Workshop Privacy and Anonymity in the Information Soc.(PAIS '11), pp. 8:1-8:10, 2011.

[3] V. Ciriani, S.D.C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi,and P. Samarati, "Combining Fragmentation and Encryption to Protect Privacy in Data Storage," ACM Trans. Information and System Security, vol. 13, no. 3, pp. 22:1-22:33, July 2010.

[4] A. Iliev and S.W. Smith, "Protecting Client Privacy with Trusted Computing at the Server," IEEE Security and Privacy, vol. 3, no. 2, pp. 20-28, Mar./Apr. 2005.

[5] L. Bouganim and P. Pucheral, "Chip-Secured Data Access:Confidential Data on Untrusted Server," Proc. 28th Int'l Conf.Very Large Data Bases (VLDB '02), pp. 131-141, 2002.

[6] N. Anciaux, M. Benzine, L. Bouganim, P. Pucheral, and D. Shasha,"GhostDB: Querying Visible and Hidden Data Without Leaks,"Proc. 26th Int'l ACM Conf. Managem ent of Data (SIGMOD), 2007.

International Journal of Computer Applications Technology and Research
Volume 3– Issue 11, 661 - 663, 2014

Protecting Global Records Sharing with Identity Based Access Control List

Vidhya . P
Computer Science and Engineering
V.S.B Engineering College
Tamilnadu, India

A.P.V Raghavendra
Computer Science and Engineering
V.S.B Engineering College
Tamilnadu, India

Abstract: Generally, the information is stored in the database. Protecting sensitive information are encrypted before outsourcing to a service provider. We send the request to service provider through SQL queries. The query expressiveness is limited by means of any software-based cryptographical constructs then deployed, for server-side query working on the encrypted data.Data sharing in the service provider is emerging as a promising technique for allowing users to access data. The growing number of customers who stores their data in service provider is increasingly challenging users' privacy and the security of data. The TrustedDB an outsourced database prototype that allows clients to execute SQL queries with privacy and under regulatory compliance constraints by leveraging server-hosted. Tamper-proof believed hardware in crucial query processing levels, thereby removing any limits on the type of supported queries. It focuses on providing a dependable and secure data sharing service that allows users dynamic access to their information. TrustedDB is constructed and runs on hardware, and its performance and costs are evaluated here.

Keywords: Database architectures, security, privacy, special-purpose hardware**.**

1. INTRODUCTION

Although the benefits of outsourcing and clouds are well known, imperative challenges yet lie in the path of large-scale adoption since such services often require their customers to inherently trust the provider with full access to the outsourced data sets. Numerous instances of illicit insider behavior or data leaks have left clients backward to place known data under the control of a private, unknown provider, without practical assurances of privacy and confidentiality, especially in occupation, healthcare, and public sectors. Moreover, today's privacy assurance for such services are at best informative and subject customers to unreasonable fine-print clauses. For example, allowing the server operator to use customer behavior and content for commercial profiling or governmental control purposes.

Existing analysis addresses several such safety aspects, including entry's privacy and finds on enciphered data. In most of these efforts, data are encrypted before outsourcing. Once enciphered however, essential limitations in the types of basic operations that can be performed on encrypted data lead to fundamental expressiveness and practicality constraints. However, recent insights into the cost performance tradeoff seem to suggest that things stand somewhat differently. Specifically, at scale, in outsourced contexts,computation inside secure processors is orders of degree lower than any equivalent cryptographic operations performed on the provider's unsecured server hardware, despite the overall higher achievement cost of secure hardware.

We conclude that a complete privacy enabling secure database leveraging server-side trusted hardware can be built and run at a fraction of the cost of any (existing or future) cryptography-enabled private data working on common server hardware. We verify this by signing and building TrustedDB, an a SQL database processing engine that makes use of tamper-proof cryptographic coprocessors such as the IBM 4764 [1] in close adjacency to the outsourced data.

Change opposes designs, however, is imperatively constrained in both computational ability and memory capacity which makes implementing fully featured database solutions using secure coprocessors (SCPUs) very demand. Trusted complete this by applying common unsecured server resources to the maximum available duration. For example, Trusted permits the SCPU to clearly access external storage while protecting data confidentiality in the family of encryption. This removes the limitations on the size of databases that can be supported. Moreover, client queries are preprocessed to identify knowing components to be run inside the SCPU. Non knowing operations are offloaded to the interested server owner. This highly increases work and decrease the cost of the agreement.

Overall, despite the overheads and performance limitations of trusted hardware, the costs of running TrustedDB are orders of degree lower than any (existing or) potential future cryptography-only mechanisms. Moreover, it does not limit query expressiveness. This paper's improvement is triples:1)The opening of current cost setups and judgments that explain and specify the advantages of utilizing trusted hardware for data working, 2) the design and advancement of TrustedDB, a reliable hardware based relational database with full data confidentiality and no limitations on query expressiveness, and 3) defined query optimization approach in a trusted hardware-based query execution model.

2. RELATED WORK

Queries on encrypted data. To propose a division of data into secret partitions and rewriting of range queries over the original data in terms of the resulting separation qualifiers. This balances a judge between client and server-side working, as a function of the data subdivision size. Some authors explore optimal bucket sizes for range queries.

Vertical partitioning of relations amongst multiple untrusted servers is employed in [2]. Here, the privacy goal is to a prevent access of a subset of attributes by any single server. For example, {Name, Address} can be a privacy sensitive access-pair and query processing needs to ensure that they are not jointly visible to any single server. The client query is split into multiple queries wherein each subquery fetches the relevant data from a server and the client combines results from multiple servers. TrustedDB is equivalent to when the size of the privacy subset is one and hence a single server answers. In this case, each attributes column demand encryption to ensure privacy. Hence, TrustedDB to optimize for querying encrypted columns since otherwise they rely on client-side decryption and processing.

To introduce the concept of logical fragments to achieve the same partitioning effect on a single server. A fragment here is simply a relation wherein attributes not desired to be visible in that fragment are encrypted. TrustedDB (and other solutions) are in effect concrete mechanisms to efficiently query any individual fragment from [10]. The work on the other hand, can be used to determine the set of attributes that should be encrypted in TrustedDB.

The goal is to minimize the lifetime of sensitive data and keys in server memory after decryption. In TrustedDB, there is no such disclosure risk since decryptions are performed only within the SCPU. In TrustedDB, all decryptions are performed within the secure confinements of the SCPU, thereby processing is done on the plaintext data. This removes any limitation on the nature of predicates that can now be employed on encrypted attributes including arbitrary user decided functions. We note that certain solutions destined for a very specific set of predicates can be more efficient albeit at the loss of functionality.

Trusted hardware. In [4], SCPUs are used to retrieve X509 certificates from a database. However, this only supports key based lookup. Each record has a single key and a user can query for a record by specifying the key. Multiple SCPUs are used to provide key based search. The entire database is scanned by the SCPUs to return matching records. Chip-Secured Data Access [5] uses a smart card for query processing and for enforcing access rights. The client query is split such that the server performs the majority of the computation. The solution is limited by the fact that the client query executing within the smart card cannot generate any intermediate results since there is no storage available on the card. In follow-up work, GhostDB [6] proposes to embed a database inside a USB key equipped with a CPU. It allows linking of private data carried in the USB Key and public data available on a server. Ghost DB ensures that the only information revealed to a potential spy is the query issued and the public data accessed.

Both [5] and [6] are subject to the storage limitations of trusted hardware which in turn limits the size of the database and the queries that can processed. In contrast, TrustedDB uses external storage to store the entire database and reads information into the trusted hardware as needed which enables it to be used with large databases. Moreover, database pages can be swapped out of the trusted hardware to external storage during query processing.

3. MODULES DESCRIPTION

A. Query Parsing and Execution

In the first stage a client defines a database schema and partially occupy it. Knowing attributes are noted using the SENSITIVE keyword which the client layer transparent processes by encrypting the corresponding attributes:

```
CREATE TABLE customer (ID integer
    primary key,
Name char (72) SENSITIVE, Address
    char (120)  SENSITIVE).
```

(1) Later, a client sends a query request to the host server through a standard SQL interface. The query is clearly enciphered at the client site using the public key of the SCPU. The server owner thus cannot decipher the query.
(2) The server owner serves the enciphered query to the Request Handler inside the SCPU.
(3) The Request Handler deciphers the query and serves it to the Query Parser. The query is parsed achieving a set of ideas. Each idea is worked by editing the original client query into a set of sub-queries, and, presenting to their end data set allocation, each sub-query in the idea is qualified as being either public or private.
(4)The Query Optimizer then evaluates the execution costs of each of ideas and selects the best idea (one with least cost) for execution serving it to the dispatcher.
(5) The Query Dispatcher serves the public queries to the server owner and the private queries to the SCPU database engine while handling responsibilities. The net result is that the maximum possible work is run on the server owner reduced cycles.
(6) The final query result is assembled, enciphered, digitally signed by the SCPU Query Dispatcher, and dispatched to the client.

B. Query optimization process

At a high level query optimization in a database system works as follows. (i) The Query Plan Achiever works possibly multiple ideas for the client query. (ii) For each worked idea the Query Cost Evaluator computes an evaluate of the execution cost of that idea. (iii) The best idea i.e., one with the lowest cost, is then selected and passed on to the Query Idea Interpretor for execution. The query development process in TrustedDB works similarly with key differences in the Query Cost Evaluator due to the logical separating of data mentioned above.

C. System Catalog

Any query idea is composed of multiple individual execution steps. To evaluate the cost of the entire idea it is essential to evaluate the cost of individual steps and combine them. In order to evaluate these costs the Query Cost Evaluator needs access to some key information. E.g., the possibility of an index or the knowledge of possible distinct values of an attribute. These sets of instruction are collected and stored in the System Catalog. Most available databases today have some form of the continuously updated System Catalog.

D. Analysis of Basic Query Operations

The cost of an idea is the separate of the cost of the steps that comprise it. In this section we present how execution times for a certain set of basic query idea steps are evaluated.

4. SYSTEM FLOW DIAGRAM

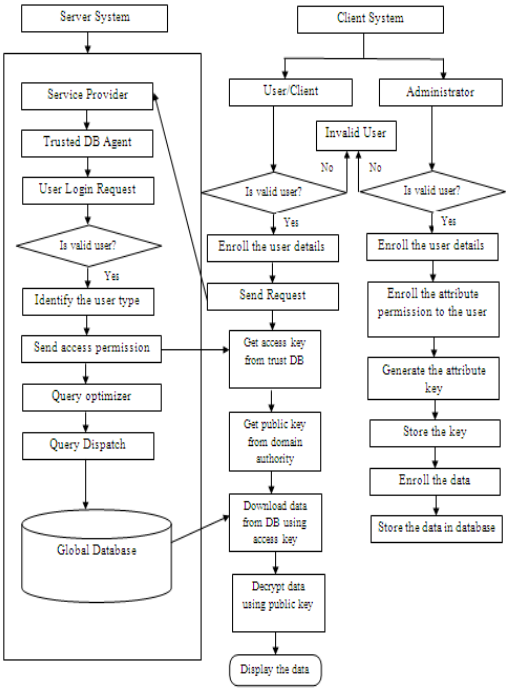


Fig: 1 System Flow Diagram

A client sends a query request to the host server through a standard SQL interface. The query is clearly enciphered at the client site using the public key of the SCPU. The server owner thus cannot decipher the query. The server owner serves the enciphered query to the Request Handler inside the SCPU. The Request Handler deciphers the query and serves it to the Query Parser. The query is parsed achieving a set of ideas. Each idea is worked by editing the original client query into a set of sub-queries, and, presenting to their end data set allocation, each sub-query in the idea is qualified as being either public or private. The Query Optimizer then evaluates the execution costs of each of ideas and selects the best idea (one with least cost) for execution serving it to the dispatcher. The Query Dispatcher serves the public queries to the server owner and the private queries to the SCPU database engine while handling responsibilities. The net result is that the maximum possible work is run on the server owner reduced cycles. The final query result is assembled, enciphered, digitally signed by the SCPU Query Dispatcher, and dispatched to the client.

4. CONCLUSION

This paper's improvement are triples:
1)The opening of current cost setups and judgments that explain and specify the advantages of utilizing trusted hardware for data working, 2) the design and advancement of TrustedDB, a reliable hardware based relational database with full data confidentiality and no limitations on query expressiveness, and 3) defined query optimization approach in a trusted hardware-based query execution model.

This work's inherent proposal is that, at order, in expand contexts, computation inside secure hardware processors is orders of degree lower than equivalent cryptography performed on suppliers' unsecured server hardware, even though the overall higher achievement cost of protected hardware. We thus propose to make reliable hardware a first-class member in the secure data management field. Moreover, we promise that cost-centric insights and architectural standards will fundamentally change the way systems and algorithms are signed.

5. REFERENCES

[1] IBM 4764 PCI-X Cryptographic Coprocessor, http://www03.ibm.com/security/cryptocards/pcixcc/overview.shtml, 2007.

[2] V. Ganapathy, D. Thomas, T. Feder, H. Garcia-Molina, and R.Motwani, "Distributing Data for Secure Database Services," Proc.Fourth Int'l Workshop Privacy and Anonymity in the Information Soc.(PAIS '11), pp. 8:1-8:10, 2011.

[3] V. Ciriani, S.D.C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi,and P. Samarati, "Combining Fragmentation and Encryption to Protect Privacy in Data Storage," ACM Trans. Information and System Security, vol. 13, no. 3, pp. 22:1-22:33, July 2010.

[4] A. Iliev and S.W. Smith, "Protecting Client Privacy with Trusted Computing at the Server," IEEE Security and Privacy, vol. 3, no. 2, pp. 20-28, Mar./Apr. 2005.

[5] L. Bouganim and P. Pucheral, "Chip-Secured Data Access:Confidential Data on Untrusted Server," Proc. 28th Int'l Conf.Very Large Data Bases (VLDB '02), pp. 131-141, 2002.

[6] N. Anciaux, M. Benzine, L. Bouganim, P. Pucheral, and D. Shasha,"GhostDB: Querying Visible and Hidden Data Without Leaks,"Proc. 26th Int'l ACM Conf. Managem ent of Data (SIGMOD), 2007.

International Journal of Computer Applications Technology and Research
Volume 3– Issue 11, 668 - 675, 2014

The Need to Integrate Usability Engineering into Agile Process Models for Mobile Applications and Devices Development

Denish Omondi Otieno
School of Computer Science and Information Technology
Jomo Kenyatta University of Agriculture and Technology (JKUAT)
Nairobi, Kenya

Wilson Cheruiyot
School of Computer Science and Information Technology
Jomo Kenyatta University of Agriculture and Technology (JKUAT)
Nairobi, Kenya

Michael Kimwele
School of Computer Science and Information Technology
Jomo Kenyatta University of Agriculture and Technology (JKUAT)
Nairobi, Kenya

Abstract: Reliability of an interactive mobile computing device or the lack of it is often reflected in user satisfaction. The rapid proliferation and ubiquity of smart devices in the consumer market has forced the Software Engineering (SE) community to quickly adapt development approaches conscious of the novel capabilities of mobile applications. However, the growth of this new computing platform has outpaced the software engineering work tailored to mobile application development. Designs in Human computer interaction (HCI) aim to create interactive products that are easy and enjoyable to use. However, owing the major gaps between HCI and SE in theory and practice, the multidisciplinary nature of HCI and the different value systems of interface users from various backgrounds and experiences, it is highly challenging for designers to create applications which are usable and affordable to such a heterogeneous set of users. Nowadays, users complain about the bad interaction design of mobile platform-based devices. The question is whether this problem is caused by the bad design of products or by the users' ignorance of the logics of HCI design? In this paper we focus on the need to integrate usability engineering in to agile process models for the enhancement of mobile application and devices development.

Keywords: usability engineering, agile process models, mobile devices

1. INTRODUCTION

The operation of human-computer interface is becoming more complicated due to the fast development in the digital technology. The un-usability of systems, products and services is a tremendous problem for users and consumers all over the world, despite the efforts put in by researchers, usability practitioners and designers. Using a mobile platform based device is different from working with a desktop or laptop computer. While gestures, sensors, and location data may be used in game consoles and traditional computers, they play a dominant role in many mobile applications. The smaller display and different styles of user interaction also have a major impact on usability design for mobile applications, which in turn has a strong influence on application development. Therefore, usability still needs to be the main focus of our activities. In practice, usability aspects are usually regarded very late (if at all) in software development. Software development does not stop with delivery, nor do usability issues. Systems and products are modified and improved in a number of releases over a number of years. Most efforts currently centered on usability matters stop after the initial development process. What do we do after delivery? Furthermore, software development models, such as agile, waterfall, Spiral, Rational Unified Process (RUP) and Dynamic Systems Development Method (DSDM) are widely used in the software development industry. These models are basically not user-centered and most of them provide limited support for usability activities.

1.1 Human computer interaction

Human-computer interaction (HCI) is a multi-disciplinary field with a focus on the interaction between humans and computers it is a discipline concerned with the design, evaluation and implementation of interactive computing systems for human use and with the study of major phenomena surrounding them Keith Andrews (2013). Humans are Individual users, a group of users working together, a sequence of users in an organization. Computers involve, desktop computers, large-scale computer system, Pocket PC, embedded system etc.

1.2 Mobile platform based devices

Mobile application development is a relatively new phenomenon that is increasing rapidly due to the ubiquity and popularity of smart phones among end-users. Mobile devices can be defined in different ways when they are looked at from different perspectives. They can be defined in terms of the services they offer or based on the level of functionality connected with the devices. According to Sharpet et al (2007) they refer to the devices that are handheld and intended to be used while on the move. Nowadays, mobile devices are being used by different people for various purposes. A mobile device refers to a pocket-sized computing device, typically having a small display screen, a small keypad with miniature buttons or a touch screen with stylus of input; mobile devices have wireless capability to connect to the Internet and home computer systems.

1.3 Usability

Usability is defined in Part 11 of the ISO 9241 standard as "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use." Effectiveness is the accuracy and completeness with which specified users can achieve specified goals in particular environments. Efficiency is defined as the resources expended in relation to the accuracy and completeness of the goals achieved. Satisfaction is the comfort and acceptability of the work system to its users and other people affected by its use.

2. WHY USABILITY ENGINEERING

Human-Computer Interaction (HCI) discipline provides the foundations to develop usable applications. "Usability Engineering" is a science that studies how to understand and systematically address the usability demand of a customer C lee et al (2007). Usability engineering deals with issues such as system learnability, efficiency, memorability, errors and user satisfaction. Usability engineering is an approach to product development that is based on customer data and feedback, on direct observation and interactions with customers to provide more reliable data than self-reporting techniques. Usability engineering begins in the conceptual phase with field studies and contextual inquiries to understand the functionality and design requirements of the product. It is an iterative design and evaluation to provide customer feedback on the usefulness and usability of a product's functionality and design throughout the development cycle. This results in products that are developed to meet the customers' needs.

3. UNIQUE DEVELOPMENT CHALLENGES FOR MOBILE PLATFORM BASED DEVICES

The creation of applications intended to execute on newer mobile devices such as smart phones and tablets involves unique requirements and challenges. Containing global positioning sensors, wireless connectivity, photo/video capabilities, built-in web browsers, voice recognition, among other sensors, mobile devices have enabled the development of mobile applications that can provide rich, highly-localized, context-aware content to users in handheld devices equipped with similar computational power as a standard personal computer (PC) Oulasvirta, et al (2011). Yet, these same novel features/sensors found in mobile devices present new challenges and requirements to application developers that are not found in traditional software applications Wassermann (2010).Traditional software engineering approaches may not directly apply in a mobile device context. First, mobile device user interfaces (UI) provide a new paradigm for new human-computer interaction sequences (e.g., multi-touch interfaces, QR code scanning, image recognition, augmented reality, etc.) that have not been previously explored in research and of which no established UI guidelines exist Oulasvirta, et al (2011) . Second, the divergent mobile platforms (e.g., iOS, Android, Windows 7, etc.), differing hardware makers for platforms (e.g., Android versions found on HTC, Google, Samsung) and mobile phone and tablet platforms (e.g., Apple's iPhone and iPad) have necessitated developers to make a series of the same application tailored for each type of device Wassermann (2010). Third, the novelty of a truly mobile computing platform provides both unique opportunities and challenges below we outline the fundamental, unique challenges to the state-of-practice in mobile application development.

3.1 Form factors

The first and most obvious unique aspect of mobile applications is that the form factor for display and user interaction is significantly different from prior forms of software. Smart phones usually provide only a four-inch area in which to display the application content and offer lower screen resolution pixel density compared to personal computer (PC) displays, which are trending toward greater display sizes and number of screen pixels. Even tablet devices have generally lower display sizes than PCs, especially when compared to the large flat-screen displays in use for newer desktop PCs. A smaller form factor means that the amount of data displayed to the end user, and layout of that data, needs to be different for these applications than for apps expected to run on PC devices. Significantly less data can be displayed at one time and therefore it must be exactly the "right" data, most relevant to what the user needs at that point in the application.

3.2 Usability and user interaction design

Several factors motivate the need for more attention to usability and user interaction design for mobile applications. One is the difference in form factors and user input methods. It is much more difficult and time consuming to plan how to display only the data that is precisely necessary than it is to simply display all possible data and let the end users visually sift through it for what they want. The mobile app designer has to consider the screen real estate.

3.3 Creating universal user interfaces

There has been some preliminary research in creating a universal user interface for mobile devices Oulasvirta, et al (2011), Balagtas, et al (2009). Each mobile platform has a unique guide to address developer user interface requirements. The user interface guidelines have several overlapping themes. A significant consideration for mobile UI development relates to screen size and resolution. For example, Apple devices are limited to two sizes based on the size of the iPhone and the iPad whereas Windows 7, Android, and Blackberry provide screens of varying sizes and screen resolutions. As a result, UI design is difficult and mobile application developers must anticipate the targeted device(s).

3.4 User input technology

Another obvious physical difference for mobile applications is that the mechanisms for user input are different. Mobile devices have pioneered the use of non-keyboard "gestures" as an effective and popular method of user input. Touch, swipe, and pinch gestures must be planned for and supported in a satisfying mobile application user experience. These tactile end user input mechanisms have proven to be so popular that they are now being retrofitted into traditional desktop PC systems such as the Apple "Lion" OS X release and Windows 8 "Metro" OS. In addition to tactile user input, mobile devices are a natural target for voice-based user input. Besides input directly from the end user, mobile devices have the capability to receive input from other sources, such as geo-location input from the GPS component of the device and image information from the camera typically built into the device. These unique forms of input must be considered during mobile application design and development. They offer new and valuable mechanisms to make mobile apps more powerful and useful than applications with a more limited array of input possibilities.

3.5 Enabling software reuse across mobile platforms

Mobile applications currently span several different operating system platforms (e.g., iOS, Android, Windows 7, etc.), different hardware makers (Apple, HTC, Samsung, etc.), delivery methods (i.e., native application, mobile web application) and computing platforms (i.e., Smartphone, tablet). Each of these options must be considered during mobile application development as they have a direct influence on the software requirements. Companies currently need to make a business decision to target a single mobile device platform with rich features, multiple platforms through a mobile website with less rich features or spend the resources necessary to broadly target the gamut of mobile devices with rich, native applications.

3.6 Choice of implementation technology

There is a spectrum of implementation choices for mobile applications in the market. There is no one perfect answer for the choice of implementation for a mobile application, and all of the choices across the spectrum have their advantages and disadvantages. Therefore, the challenge for mobile development teams is to understand the trade-offs between the technologies and make a choice based on the specific application requirements. The choice of implementation technology for a mobile project will have an impact on other decisions related to the application's development. It may limit the choices for development tools. The implementation choice will likely have an impact on the team roles and structure. It may have an impact on how the application is tested and verified, and how it is distributed and delivered to the end user. So, the choice of implementation approach for a mobile application is a crucial, early-stage decision to be made very carefully.

3.7 Designing context-aware mobile applications

Mobile devices represent a dramatic departure from traditional computing platforms as they no longer represent a "static notion of context, where changes are absent, small or predictable" Roman, et al (2000).Rather, mobile devices are highly personalized and must continuously monitor its environment, thereby making mobile applications inherently context aware (collectively time-aware, location-aware, device-aware, etc.) Hofer, et al (2003), Dey, et al (2008). Mobile applications are now contextualizing proximity, location, weather, time, etc. To deliver hyper-specialized, dynamic, rich content to users through context-aware applications. Previously, web applications would often provide contextualized content based on time, detected location and language. However, the extent of context-awareness currently possible in mobile applications is beyond what software engineering approaches have encountered outside of agent-oriented software engineering. The consideration of context-awareness as a first-class feature in mobile application development is needed so that the requisite attention is paid by developers when analyzing these requirements resulting in better designed context-aware applications.

3.8 Behavioral consistency versus specific HCI guidelines

Ideally, a given mobile app should provide the same functionality and behavior regardless of the target platform it is running on. However, due to the internal differences in various mobile devices and operating systems, "a generic design for all platforms does not exist". "An Android design cannot work all the way for the iPhone." This is mainly due to the fact that HCI guidelines are quite different across platforms, since no standards exist for the mobile world, as they do for the Web for instance. On the other hand, developers would like their application to behave similarly across platforms, e.g., user interaction with a certain feature on Blackberry should be the same as on iPhone and Android thus, creating a reusable basic design that will translate easily to all platforms while preserving the behavioral consistency is challenging.

3.9 Balancing agility and uncertainty in requirements

While most mobile application developers utilize an agile approach or a nearly ad hoc approach, the growing demand for context-aware applications, competition amongst mobile applications and low tolerance by users for unstable and/or unresponsive mobile applications (even if free) necessitates a more semi-formal approach. This should be integrated into agile engineering to specify and analyze mobile application requirements.

3.10 Mobile application build and delivery

The strong business motivation to deliver mobile applications into the market quickly has made mobile development projects typically to have extremely aggressive time lines. Inception-to-delivery periods of a few months are common. The pressure to deliver mobile apps quickly results in the adoption of agile development methods for most mobile projects. An important element in agile development practices is continuous integration and builds. Application changes delivered by developers need to be processed immediately for all of the mobile operating systems on which the application is required to execute. If the mobile application is a hybrid or native implementation, several different builds of the application need to be triggered each time a change set for the application is delivered by a developer. The build setup and configuration for each supported mobile environment will be different from the others, and it is most likely that a small "farm" of build servers will need to be provisioned and available to handle these builds of the mobile application for multiple operating systems.

3.11 Testing of applications

Another area where mobile application development poses a huge challenge is testing. Testing for mobile applications represents a quantum leap in complexity and cost over more traditional applications. Unlike traditional PC and web applications, the range of potentially supported mobile devices and release levels is staggering. It is quite common to see test matrices for mobile projects that contain hundreds, and even thousands, of permutations of device, mobile OS level, network carrier, locale, and device orientation combinations.

4. HARDWARE CHALLENGES

Due to the limitations of size and weight for portability purpose, the interface design for mobile devices comes with more hardware challenges when compared to other regularized devices such as desktop phones or printers; these challenges include limited input facilities, limited output facilities, and designing for mobility.

4.1 Limited input facilities

According to Muhanna (2007), there are three main input facilities for mobile devices that are on the market:

- The keyboard,
- The stylus with the touch screen, and
- The scroll wheel.

The keyboard allows a user to hit a key to perform a task or navigate through the mobile menu functionalities; the stylus with the touch screen allows a user to hit the screen to do the task; the scroll wheel can be scrolled and pushed by a user to do a task and also navigate through the menus and submenus. The design of keyboards for mobile devices has been a challenge because the space for key installation on a mobile device is limited.

Mobile interfaces can be quite tricky and cumbersome to use when compared to the fully-blown GUI, especially for those with poor manual dexterity or fat fingers and those who have difficulty in selecting tiny buttons on mobile devices, Siek et al (2005). Research directions on this limitation have come up with different alternatives and solutions. Green et al (2004) described a specialized keyboard 'Stick' that maps row to decrease the physical space. However, a drastic key reduction in order to achieve sufficient portability decreases text entry performance, and requires additional effort to learn a new typing method. The stylus and touch screen which are widely used in personal digital assistants and smart phones can be a good alternative for the keyboard in some cases. However, touch input would be problematic if the screen of a mobile device is small and that would lead a user's fingers to occlude the graphical elements he wishes to work with.

4.2 Limited output facilities

There are various output facilities that are used on mobile devices. The small-sized screen is one of the mainly and most commonly used output facilities for mobile devices. Designing the screen for outputting is a trade-off challenge that needs to be experimentally studied to find out which is the efficient and most effective size of the screen that can be used for the different types of mobile devices Muhanna (2007). For example, having a larger screen can solve a limited output facilities challenge; however, it will bring up another challenge of designing for mobility.

The audio output is another output facility that is commonly used on mobile devices. It can be a good output facility for feedback messages to the user, and can be used in conjunction with the graphics and text messages to have an effective interaction between the human and the device Muhanna (2007).

4.3 Designing for mobility

A mobile device should be portable and easy to be held by the user, and this brings up the big challenge of designing for mobility, Myers (2004).The power facility in a mobile device is the main challenge of designing for mobility that is characterized by limited and dynamically varying available resources and stringent application requirements. Ashwini et al (2006) indicated that the power consumed by an application depends on the performance level requested by the user or application, and that the mobile device can be viewed as the collection of devices. Therefore, it is very crucial to design a power management unit which collects information in hardware so that the performance of the system is not degraded Hwang (2008)**.**

5. THE GAPS IN INDUSTRY PRACTICES

Jerome and Kazman analyze the gaps between SE and usability in HCI in practice Jerome, et al (2005) from a survey of 63 HCI practitioners and 33 software engineers; they found that the state of practice is not very encouraging. They report that there is substantial lack of mutual understanding among software engineers and HCI practitioners and the two disciplines hardly follow each other. They also do not collaborate much in projects. 68% software engineers report that they made key software design decisions that affect the user interface without consulting HCI practitioners. Even greater proportion of HCI practitioners (91%) believe that software engineers were making key design decisions without consulting any HCI practitioners. When collaboration does occur, it usually happens too late. Only 1 out of 21 software engineers and 2 out of 60 HCI practitioners reported that they collaborated during the specifications phase below we explore the challenges.

5.1 Usability engineering inputs are not taken during requirements specifications

Usability engineering inputs are needed early in the process before requirements are finalized. Use cases in requirements documents routinely over-specified the usability design, including details such as the sequence, the contents of dialog boxes in the application, navigating and browsing for mobile devices that generally have small screens etc. This over-specification happened possibly because there is a physical and cultural distance between the developers and users, the development teams are less familiar with the context of users, and the requirements specifiers want to have a control on the user interface.

5.2 Porting projects get minimal HCI inputs

Every software project represents an opportunity to improve the user experience. Conversely, every project also represents a risk of degrading the user experience. This applies even to porting and migration projects. Less importance is normally given to requirements gathering in general and usability requirements. It is assumed that most requirements are well-understood and had to be "copied over" from earlier version. However, projects often involve a change of delivery platform, a change of context, or a change of users and coping over can have a big impact on usability design and the corresponding requirements.

5.3 Client representatives take design decisions

Client representative routinely drives many HCI design and usability considerations. Such a person may have never been a user himself or may have moved out of that role a long time ago. His / her sign-off may not imply that the product is usable. This can be revealed only by usability evaluations with real users.

5.4 Usability engineering skills do not have process support

Software Engineering projects have some involvement of Usability engineering practitioners, though they still ended with unresolved usability issues that they knew could be solved Jerome, et al (2005). A multi-disciplinary team needs to work together. The team needs to be armed with appropriate user inputs and needs a common set of work products and a common process to approach the product development holistically and add value. Role of each discipline needs to be mutually understood and respected, first within the team and then across the organizations.

5.5 Too little and too late is not good enough

In projects, Usability engineering practitioners are pulled in towards the end when too many obvious usability problems surfaced Jerome, et al (2005). In these situations, Usability engineering practitioners work under severe constraints. They have no time to understand the scope of the project and no budget to do usability activities they would have done earlier. Even if some Usability engineering activities were done, most of the recommendations they come up with to improve the User Interface seemed too impractical to implement in the given situation. Few cosmetic changes would be made, mainly to satisfy the client representative, and the project would be pushed through.

6. AGILE PROCESS MODELS

Agile process models have come to represent the iterative nature of software development as shown in figure 1 below. Several process models have emerged. Pressman summarizes seven agile process models: Extreme Programming, Adaptive Software Development, Dynamic Systems Development Method, Scrum, Crystal, Feature Driven Development, and Agile Modeling Pressman (2005 pp. 103-124). These process models may vary in their details, but they have several common elements best captured by the agile manifesto Agile Manifesto (2001).

- Individuals and interactions over processes and tools
- Working software over comprehensive documentation
- Customer collaboration over contract negotiation
- Responding to change over following a plan.

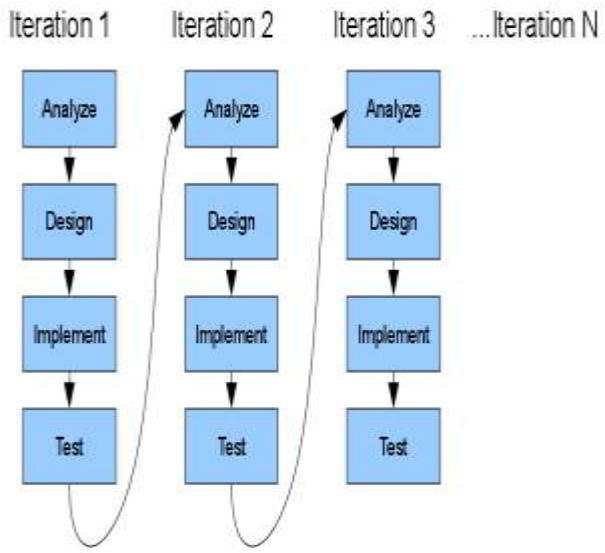


Figure. 1 Agile process

The last point is particularly important. In agile processes, it is typical to solve a small part of the problem to begin with and to grow the solution in iterations. Agile processes believe that changes in software requirements will necessarily happen. Agile processes are designed to accommodate changes even late in the process to harness change for the customer's competitive advantage Agile Manifesto (2001). Fowler lists many reasons why requirements change, and in fact why they ought to be changeable Fowler (2005). Firstly, customers cannot recognize what options they have while specifying requirements. Even if they could, they cannot make an informed decision at this stage primarily because the cost to each new requirement cannot be predicted right up front. Software development is a design activity and thus hard to plan and cost. Further, the basic ingredients of software keep changing rapidly. In addition, costs are dependent on the individuals involved and their experience. Finally, software is intangible and yet malleable. Only when they use an early version of some software do the customers really begin to understand which features are valuable and which are not Fowler (2005). Even if we could get an accurate and stable set of requirements early, Fowler believes that you are still doomed. The fundamental business forces in today's economy are so dynamic that every six months, new requirements are likely to emerge.

In agile processes, the main measure of progress is working software agile methods deliver working software in small pieces frequently and sometimes as frequently as once a week. This length of time forms a heartbeat for the project and helps maintain pace. Agile methods also insist that development needs to happen smoothly, without the developers working overtime. Each iteration of an agile process follows a mini-waterfall within itself. Sufficient requirements are expressed, analyzed, the software architecture is re-factored if necessary, the code is written or re-written, tested and released. If some requirements could not be completed in the current iteration, they are carried over to the next iteration.

Agile methods do not plan a timeline for the whole project. Because new versions of the software are constantly being released, it makes it easier for everyone (including the customer) to see momentum in the project. This makes it easier to estimate the time needed to achieve the overall vision of the project and to make course corrections. While testing is important in all software process models, agile methods emphasize on testing. Agile methods suggest not only testing the current version of the product, but setting up of automated testing procedures so that testing is frequent and when changes happen during iterations, the automated regression testing detects the breaks soon. Automated regression testing is particularly important because it saves on time compared to manual testing. Agile methods depend a lot on teamwork and internal communication. It is believed that best architectures, requirements, and designs emerge from self organizing teams. Developers work alongside customers during the development. There is usually little documentation, but there is a lot of emphasis on face-to-face communication between team members.

Pair-programming (programming done by two developers together) and daily stand-up meetings (that last no more than 15 minutes) help in maintaining communication going among team members. Usability engineering processes share several qualities with agile processes. Usability engineering design is intrinsically an iterative process consisting of analysis, design, and usability evaluation. The problems found during the evaluation are fixed in the next iteration. Such iterations continue until no problems are found and user experience goals are met. Given this preference for iterations, agile methods seem a good fit for integrating usability engineering activities within the agile processes. The emphasis on people and deliverable products rather than documentation and planning are also common qualities just like agile programmers, usability engineering designers are more of doers. The informality of the agile methods gels well with the informal culture of design. Designers are more at ease in face-to-face communication and visual presentation of ideas than with wading through long documents. Most critiques agree that there is potential to integrate user-centred activities with

agile development. Nielsen acknowledges that agile methods hold promise for addressing the many ways in which traditional development methodologies erected systematic barriers to good usability practice Nielsen (2008). However, despite the similarities, several Usability engineering issues still emerge with agile process models. Design in the Usability Engineering world involves working with the user to understand the problem and come up with a user interface – typically on paper - of the entire system before turning it over, in Big Design Upfront (BDUF) manner, to the rest of the development team to build. Following our surveys the following were found to be a challenge in the current agile development paradigm.

6.1 Software engineers are asked to design

The most important issue with agile process models is that they pay little attention to users and Usability Engineering. Agile methods do not acknowledge that Usability Engineering activities require a different set of specialized and important skills. This is reflected in the team composition. Agile teams primarily consist of software engineers, and working code is considered the primary deliverable. Anyone who does not deliver code (e.g. a designer) does not easily fit in culturally. Several critiques have reflected this view. Blomkvist comments that though agile processes value people, skills, and teamwork in other areas, they do not regard that usability and interaction design skills as important Blomkvist (2005). Nielsen identifies threats of agile methods Nielsen (2008). The biggest threat, according to Nielsen, is that agile methodologies are developed by programmers to address the implementation side of software development, overlooking Usability Engineering design. While Nielsen is not against Usability Engineering design being performed by the same people who do the coding, he feels it must be recognized as a separate activity rather than leaving it to happen as a "side effect of coding". Constantine concludes that agile methods seem to be at their best in applications that are not GUI intensive Constantine (2002).

6.2 Users are asked to design

To help design a new system, agile methods put representative customers or users in the team. This may give a feeling to the development team that the voice of users is being heard, this may not be true critics. Bayer et al. argue that there is no such thing as representative users. At best, they are a sub-set of users and often, they only represent themselves Beyer, et al (2004). Further, even real users are unable to articulate what they do and how, particularly when they are not in the context of that work, and certainly if they have not been doing the work for a while. Finally, users are not able to make design decisions for a new system. Users may not have the appropriate skills required to create visions of future systems. Design of interactive systems requires a complex set of skills and it is inappropriate to assume that all representative users would have it. User should be involved, but not for making the design decisions. Skilled Usability Engineering practitioners can design good systems by observing users in their contexts, by involving them in participatory design activities, or by asking them to try out prototypes during usability tests.

6.3 Change is managed well but anticipated poorly

Agile methods plan very little up front because it is assumed that the business needs and requirements will change any way. However, as Allen Cooper puts it, this is a self fulfilling prophecy. Requirements change because planning is avoided Cooper (2008). Managing change is one of the strengths of agile methods. As a result, agile methods shun Big-Design-Up-Front. Agile methods do not seem to be differentiating between elaborate planning and deeply understanding user needs, between software design and design for human beings, and between intra- and extra-lifecycle changes. They tend to club these in to one basket and shun them equally. We categorize changes to Usability Engineering into five types:

- Changes that arise because a new user need or user problem is discovered after requirements are frozen.
- Changes that arise because someone thinks of a new idea after the requirements were frozen.
- Changes that arise because something that was thought to be technically feasible turns out not to be so and a workaround is required.
- Changes that arise because late usability evaluations of early releases throw up unanticipated usability problems that were not captured on early prototypes and
- Finally, changes that could not have been anticipated.

Agile methods seem to give a license to do a poor job at anticipating and containing change. Proponents of agile methods seem to do little introspection about the reasons for intra-lifecycle changes, which are the most common type of changes in projects. Usability Engineering activities can help in anticipating many of the intra-lifecycle changes that arise out of human needs and business processes.

6.4 Agile user stories are not interaction design scenarios

Agile teams use user stories to define, manage, and test features of a product. It is tempting to think of these as parallel to scenarios in interaction design and to think of stories as a direct link between Usability Engineering and agile methods. However, a closer look at tells a different story. Agile user stories are written by customers, focus on the user interface of one feature, and are supposed to be about three sentences long, Wells (2009). The length of the story is determined by the time it takes to implement it in code. Scenarios in interaction design are lot richer than three-sentence-long user stories. They are created by designers to envision new products. A scenario may involve more than one feature and may involve one or more personas. Scenarios narratives are never only three sentences long, are often accompanied by storyboards or videos, and only sometimes describe details of the user interface. The main purpose of a scenario is to explain the high-level impact of the future product on the life of the user in a particular situation Cooper, et al (2003 pp. 77-82). It is difficult to imagine how a scenario can be chopped or merged just so that it can be developed in three weeks.

6.5 Short Iterations

An important Usability Engineering issue is that breaking down product development into small parts and constant change can potentially undermine the totality of the user experience. While some Usability Engineering researchers have no issues with this, a few have critiqued this of agile methods Constantine (2002), (Nielsen, 2008). Piecemeal design could lead to lack of cohesiveness and allow inconsistencies to creep in. Maintaining a comprehensible and consistent user interface as new features are added becomes increasingly difficult. Short iterations cause further problems as the usability team tries to maintain the project.

7. DISCUSSION

The relevance of usability as a quality factor is continually increasing for software engineering organizations: usability and user acceptance are about to become the ultimate measurement for the quality of today's, telematics applications, e-commerce web sites, mobile services and tomorrow's proactive assistance technology. Taking these circumstances into account, Usability Engineering methods for developing interactive systems are changing from a last minute add-on to a crucial part of the software engineering lifecycle.

It is well accepted both among software practitioners and in the Usability Engineering research community that structured approaches are required to build interactive systems with high usability. On the other hand specific knowledge about exactly how to most efficiently and smoothly integrate Usability engineering methods into established software development processes is still missing Eduard et al (2004), while approaches such as the usability maturity model (UMM) provide means to assess an organization's capability to perform usability development processes they lack guidance on how to actually implement process improvement in usability Engineering. It often remains unclear to users of Usability engineering methods why certain tools and methods are better suited in a certain development context than others Metzker and Reiterer, (2002). We need strategies and tools that support engineering organizations. Little research has been done on integrating methods and tools of usability in to software engineering development process for the enhancement of interactive mobile platform based devices and on gathering knowledge about Usability Engineering activities in a form that can capture relationships between mobile platform development contexts, applicable methods, tools and their impact on the engineering process.

8. CONCLUSION

Early computer systems were expensive and were developed mainly for particular tasks, like advanced number-crunching; as such, these systems were employed only by specialist computer users. Often the systems had command-line interfaces, with obscure commands known only by these specialist users. Thus, the user had to adapt to the system, and learning how to use the system required much effort. Computing systems, however, are no longer the province of the specialist user. As the price of PCs and computer-based technologies has fallen, the ownership of these types of goods by non-specialists has widened. The need for the design and development of user interfaces that support the tasks people want to do and that can be used easily by a variety of people with varying abilities has become an important issue. Users are more comfortable with mobile platform based devices that are easy to use, easy to understand, and enable them to attain their goals with minimum frustration. Poor or bad user interfaces design leads to user frustration and dissatisfaction and that's why we highlight different issue to be addressed in regards to achieving better mobile applications and devices.

9. REFERENCES

[1] A. I. Wasserman, "Software engineering issues for mobile application development," in *Proceedings of the FSE/SDP workshop on Future of software engineering research - FoSER '10*, 2010, pp. 397-400.

[2] A. Muhanna, "Exploration of human-computer interaction challenges in designing software for mobile devices," master's thesis, University of Nevada, Reno, USA, 2007.

[3] A. Oulasvirta, M. Wahlström, and K. Anders Ericsson, "What does it mean to be good at using a mobile device? An investigation of three levels of experience and skill," *International Journal of Human-Computer Studies*, vol. 69, no. 3, pp. 155-169, Mar. 2011.

[4] Agile Manifesto 2001, Accessed June 1, 2009, http://agilemanifesto.org/.

[5] B. A. Myers, J. Nichols, J. O. Wobbrock, and R. C. Miller, "Taking handheld devices to the next level," *IEEE Computer Journal*, vol. 37,no. 12, 36−43, 2004.

[6] Bevan N Classifying and Selecting UX and Usability Measures, International Workshop on Meaningful Measures: Valid Useful User Experience Measurement, 2008.

[7] Beyer H, Holtzblatt K, and Baker L, An Agile Customer-Centered Method: Rapid Contextual Design, XP / Agile Universe, 2004.

[8] Blomkvist S Towards a Model for Bridging Agile Development and User-Centred Design, in Human Centred Software Engineering, Seffah A, Gulliksen J, and Desmarais M (eds.), Springer, 2005.

[9] C. Lee and D, S, McCrickard, "Towards extreme(ly) usable software: exploring tensions between usability and agile software development," Proc, AGILE 2007 conference, (Agile '07), IEEE Press,2 007, pp, 59-71.

[10] Carroll J Human Computer Interaction, Interaction-Design.org, 2009

[11] Christer Nordberg (2010), Exploring the text free interface for illiterate users Designing an icon-based prototype for mobile phones

[12] Constantine L Process Agility and Software Usability: Toward Lightweight Usage Centered Design, Information Age, 2002

[13] Cooper A and Reimann R About Face 2.0, Wiley, 2003.

[14] Cooper A Allen's Keynote at Agile 2008.

[15] Da silva, t. S. *Et al.* "User-Centered Design and Agile Methods: A Systematic Review". In: Agile COnference. 2011, pp. 77-86.

[16] F. Balagtas-Fernandez, J. Forrai, and H. Hussmann, "Evaluation of user interface design and input methods for applications on mobile touch screen devices," *Human-Computer Interaction*, pp. 243–246, 2009.

[17] F. Bomarius et al. (Eds.): PROFES 2009, LNBIP 32, pp. 386–400, 2009.The Waterfall Model in Large-Scale Development, Springer-Verlag Berlin Heidelberg 2009.

[18] Fowler M The New Methodology, December 13, 2005.

[19] Ferreira, j.; sharp, h.; robinson, h. "User experience design and agile development: managing cooperation through articulation work". *Softw. Pract. Exper.*,New York, NY, USA, vol. 41, August 2011, pp. 963-974.

[20] G. C. Roman, G. P. Picco, and A. L. Murphy, "Software engineering for mobility: a roadmap," in *Proc. of the Conf. on the Future of Software Engineering*, 2000, pp. 241–258.

[21] Gulliksen J, Cajander A, and Eriksson E Only Figures Matter? – If Measuring Usability and User Experience in Practice is Insanity or a Necessity, International Workshop on Meaningful Measures: Valid Useful User Experience Measurement, 2008.

[22] H. S. Ashwini, A. Thawani, and Y. N. Srikant, "Middleware for efficient power management in mobile devices," in *Proceedings of the 3rd International Conference on Mobile Technology, Applications and Systems*, 2006.

[23] IXDA About Interaction Design, Interaction Design Association, 2009.

[24] J. Dey, Anind K., Hakkila, "Context-Awareness and Mobile Devices," 2008.

[25] Jerome B and Kazman R Surveying the Solitudes: An Invetigation into the Relationships between HCI and SE in Practice, in Human Centred Software Engineering, Springer, 2005.

[26] Kai Petersen, Claes Wohlin, and Dejan Baca1 *The Waterfall Model in Large-Scale Development*, LNBIP 32, pp. 386–400, 2009.

[27] Kay H. Connelly, Katie A. Siek, Valerie Lafond Favieres, and Gisele Bennett. Planes, pains, and phosphorane: Usability studies in non-traditional environments. In Adjunct Proc. From Interact 2005, 2005.

[28] Katie A. Siek, Yvonne Rogers, and Kay H. Connelly. Fat finger worries: How older and younger users physically interact with PDAs. In Proc. of Interact 2005, pages 267–280. LNCS 3585, 2005.

[29] Keith Andrews, *Human-Computer Interaction Course Notes* Version of 28 May 2013

[30] Metzker, E. and Reiterer, H. (2002), *Evidence-based Usability Engineering*. in Computer-aided Design of User Interfaces (CADUI2002). 2002. Valenciennes, France.

[31] Nielsen J Agile Development Projects and Usability, November 17, 2008

[32] N. Green, J. Kruger, C. Faldu, and R. Amant, "A reduced QWERTY keyboard for mobile text entry," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2004, pp.1429−1432.

[33] p, McBreen, "Quality assurance and testing in agile projects," McBreen Consulting, [online] Available: http://www.mcbreen.ab.caltalksiCAMUG.pdf [Accessed: December 2009]

[34] Pressman R Software Engineering – a Practitioner's Approach (6th Edition), McGraw Hill, 2005.

[35] Software Engineering Institute CMMI for Development Version 1.2, August 2006.

[36] Sohaib, o.; khan, k. "integrating Usability Engineering and Agile Software Development: A Literature Review". Computer Design and Applications ICCDA 2010 International Conference on, vol. 2, 2010,

[37] Sharples, M., Taylor, J., & Vavoula, G. (2007) A Theory of Learning for the Mobile Age. In R. Andrews and C. Haythornthwaite (eds.) The Sage Handbook of Elearning Research. London.

[38] T. Hofer, W. Schwinger, M. Pichler, G. Leonhartsberger, J. Altmann, and W. Retschitzegger, "Context-awareness on mobile devices - the hydrogen approach," in *36th Annual Hawaii International Conference on System Sciences, 2003. Proceedings of the*, 2003.

[39] Usability Professionals Association, Usability Body of Knowledge, 2004, 2010.

[40] Wells D User Stories, Extreme Programming, 2009. http://www.extremeprogramming.org/rules/userstories.html

[41] Welle-Strand, A., & Thune, T. (2009, April 24). *Store Norske Leksikon*. Retrieved May 30, 2010, from Analfabetisme: http://www.snl.no/analfabetisme

[42] Y. S. Hwang, S. K. Ku, C. M. Jung, and K. S. Chung, "Predictive power aware management for embedded mobile devices," in *Proceedings of the 2008 Conference on Asia and South Pacific Design Automation*,2008, pp. 36−41.

International Journal of Computer Applications Technology and Research
Volume 3– Issue 11, 676 - 678, 2014

Dynamic Chunks Distribution Scheme for Multiservice Load Balancing Using Fibonacci Bases Approach

D.Dhivya,
Computer Science and Engineering,
V.S.B Engineering College,
Tamilnadu, India,

U.Gowrisankar
Computer Science and Engineering,
V.S.B Engineering College,
Tamilnadu, India,

Abstract: Cloud computing is collection of distributed hosts which allows services on demand to user. The Centralized cloud based multimedia system CMS[4], materialized because huge number of users demand for various multimedia services through the Internet at the same time and it is hard to design effective load balancing algorithm. Load Balancing is the process which are used to distribute workloads across aggregate computing resources that maximize throughput, minimize latency. In this paper videos are split up into no of chunks and stored at hosts in a distributed manner, The chunk size increased to reduce time lag and improve performance. The cluster heads will monitor all the distribution host loads and client request which could not allow the direct communication between Client and host .Fibonacci-based breaking scheme is introduced to split a video file into number of chunks that allows to reduce the provisioning delay received by users and to optimize the resource utilization by reducing the idle time. The proposed scheme will able to view the whole video by the end user without any delay.

Keywords: Cloud computing, load balancing, multimedia system, Fibonacci splitting approach.

1. INTRODUCTION

Cloud computing is a model in which the resources are shared by the cloud users via internet. Resources include servers, files, network, applications and services. The important features of cloud computing are broad network access, resource pooling, rapid elasticity, measured service, multi-tenancy. The cloud service providers offer the utilities based on cloud facilities to clients and need to pay for the utilized resources by the time. On demand of number of users for various multimedia computing cloud based multimedia system was emerged [1]. In the proposed system videos are divided into segments that are then further divided into chunks.

These chunks are encoded into independent parts that are distributed to different servers for local storage [2]. The chunk size progressively increased to reduce delay improves performance and reduces the loading time. Since the video data is divided into chunks and stored at peers' local storage in a distributed manner. The cluster heads will monitor all the distribution server loads and client request. This may not allow the direct communication between Client and server and the Server offline problem also managed. Fibonacci-based splitting strategy is introduced to split a video file into number of chunks.

2 .EXISTING SYSTEM

For optimization genetic algorithm approach was implemented. It is a search algorithm based on the principles of evolution and natural genetics[4]. GA combines the exploitation of past results with the exploration of new areas of the search space. By using survival of the fittest techniques combined with a structured yet randomized information exchange, a GA can mimic some of the innovative flair of a human search.

3. PROPOSED SYSTEM

As in proposed describes multimedia system for cloud computing a cluster based multimedia application for the distributed of media files.It addresses how a cloud can perform distributed multimedia processing ,storage and provide quality of service (QoS) provisioning for multimedia services. Different multimedia data dissemination strategies have been analyzed and an innovative technique, based on the Fibonacci series, is proposed .By using this method client can pick up any server without any additional searches.

3.1 FIBONACCI METHOD

The Fibonacci sequence is a set of numbers that starts with a one or a zero, followed by a one each number is equal to the sum of the preceding two numbers. If the Fibonacci sequence is denoted as F (n), where n is the first term in the sequence, where the equation follows,

F (0) = 0, 1, 1, 2, 3, 5, 8, 13, 21, 34

In mathematical terms, the sequence Fn of Fibonacci numbers is defined by the recurrence relation.

$$F_n = F_{n-1} + F_{n-2},$$

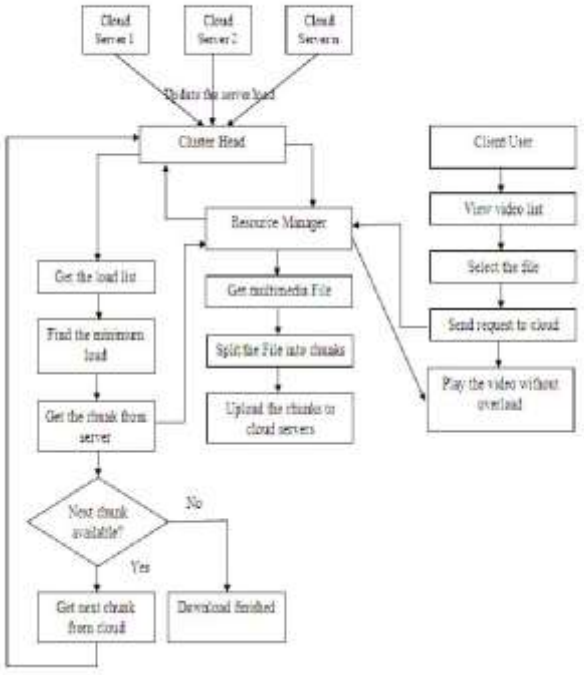


Fig1 Architectural design

3.2 MODULE DESCRIPTION

3.2.1 USERINTERFACE DESIGN

The goal of user interface design is to create the user's fundamental interaction as mere and efficient as possible, in terms of achieving user goals what is often called user-centered design. Graphic design may be utilized to support its usability. The design process must balance technical functionality and visual elements to create a system that is not only operational but also usable and adaptable to changing user needs.

3.2.2 THE FIBONACCI VIDEO DIFFUSION APPROACH

This module develop for QOS technique able to manage cloud resources in order to both guarantee service continuity and reduce the provisioning initial delay of the streaming multimedia files[3]. The chunks are used for improves the system performance, allowing the distributed and parallel execution of the tasks needed to the service provisioning. However, once the number of chunks is fixed, different performance can be observed concerned to the splitting strategies, which refer to the decisions about the size of each chunk. Splitting strategies influence different aspects of the system performance. The initial delay perceived by user, the service continuity, and. This process helps to overhead due to the parallel execution, in terms of system efficiency.

3.2.3 MULTIMEDIA UPLOAD TO SERVERS

The Multimedia Upload activity copes with the storage of multimedia contents on the cloud servers. The media files is uploaded in a cloud node and then split (Splitting phase) into number chunks in order to allow the data dissemination and then the parallel tailoring at same time. The number of chunks and the adopted splitting strategies influence the system performances in terms, for example, of delays during the streaming. It is then necessary to carefully carry out the splitting according to the available cloud resources and performing, if possible, different chunk splitting of the same media file, thus responding to different QOS requests.

3.2.4 MULTIMEDIA STREAMING FROM CLOUD

The Multimedia Streaming activity deals with user requests. Users request content with media list what file the user want to view or watch. The different chunks are then recovered and tailored, according to the requested characteristics, by a number of cloud server equal to the chunks number. In this module gather the video files from different cloud servers with in a network area and video chunks are stored in number of cloud servers. When client use our application list of videos will display in the user browsing window. The user can select any of the video from the window what they wish to watch, that particular file is send as a request to the resource manager that resource manager tailors the all chunks from different cloud servers and response to the client those who request the video.

3.2.5 RESOURCE MANAGER MANAGEMENT

Multimedia streaming services involve stringent QOS requirements, typical of soft real time applications. The resource manager of the CMS is in pursuit of fairly distributing the task load across server clusters, and hence, it is of importance and interest to be able to cope with load balancing in the CMS. Resource manager and a number of server clusters are coordinated by a cluster head[2]. Different from the decentralized CMS, each time it receives clients' requests for multimedia service tasks, the resource manager of the centralized CMS stores the global service task load information collected from server clusters, and decides the amount of client's requests assigned to each server cluster so that the load of each server cluster is distributed as balanced as possible in terms of the cost of transmitting multimedia data between server clusters and clients.

4. CONCLUSION AND FUTURE WORKS

In the existing system client search for the particular server for an requested data or video to the where it take more time to process it and then only it was delivered to client from server. In order to avoid this problem videos are splitted by using this Fibonacci approach as they are divide into number of chunks .This chunks are present in all servers which will prevent loading buffering problem are reduced . It will lead to quick video or file display to the end user without any delay thus enabling the provisioning of services with different QOS levels.

5. REFERENCES

[1] W. Zhu, C. Luo, J. Wang, and S. Li, ―Multimedia cloud computing:An emerging technology for providing multimedia services and applications,‖*IEEE Signal Process. Mag.*, vol. 28, no. 3, pp. 59–69, May 2011.

[2]Yung-Cheng Kao, Chung-Nan Lee, Peng-Jung Wu, and Hui- Hsiang Kao – ―A Network Coding Equivalent Content Distribution Scheme for Efficient Peer-to-Peer Interactive VoD Streaming‖ VOL. 23, NO. 6, JUNE 2012.

[3] W. Hui, H. Zhao, C. Lin, and Y. Yang,―Effective load balancing forcloud-based multimedia system,‖ in *Proc. Int. Conf. Electron. Mech. Eng.Inform. Technol.*, 2011, pp. 165–168.

[4]Dynamic Multiservice Load Balancing inCloud-Based Multimedia System Chun-Cheng Lin, *Member, IEEE,* Hui-Hsin Chin,*Student Member, IEEE,* and Der-Jiunn Deng, MARCH 2014.

[5] C.-F. Lai, Y.-M. Huang, and H.-C. Chao, "DLNA-based multimedia
IEEE Syst. J., vol. 4, no. 2, pp. 262–270, Jun. 2010.
sharing system over OSGI framework with extension to P2P network,"

International Journal of Computer Applications Technology and Research
Volume 3– Issue 11, 679 - 681, 2014

Enhanced Detection System for Trust Aware P2P Communication Networks

K. Kalaivani
Computer Science and Engineering
V.S.B Engineering college
Karur, India

C.Suguna
Computer Science and Engineering
V.S.B Engineering College
Karur, India

Abstract: Botnet is a number of computers that have been set up to forward transmissions to other computers unknowingly to the user of the system and it is most significant to detect the botnets. However, peer-to-peer (P2P) structured botnets are very difficult to detect because, it doesn't have any centralized server. In this paper, we deliver an infrastructure of P2P that will improve the trust of the peers and its data. In order to identify the botnets we provide a technique called data provenance integrity. It will ensure the correct origin or source of information and prevents opponents from using host resources. A reputation based trust model is used for selecting the trusted peer. In this model, each peer has a reputation value which is calculated based on its past activity. Here a hash table is used for efficient file searching and data stored in it is based on the reputation value.

Keywords: provenance, p2p system, trust, reputation, hash table

1. INTRODUCTION

A botnet is a collection of compromised hosts (bots) that are remotely controlled by the botmaster. In the centralized architecture the botmaster can send commands to the bots through the command and control (C&C) channel. The disadvantage of this is, the bots can be easily identified and removed. In order to overcome this problem botmasters have implement botnets in peer to peer (p2p) networks. Botnets are dynamic in nature. It can range from larger network to smaller network [5].

Peer to Peer (P2P) network can be configured by itself and it is decentralized. Comparing to the traditional client server network, the p2p network can dispense more malicious or forged content, malicious code, worms, viruses and Trojans because of its decentralized nature. It is shown that the system where peers work only for their selfish interests. Policing these types of networks is extremely difficult because of the decentralized and the ad hoc nature. In the centralized approach, the disadvantage is that the central authority can be turned into malicious. If there is no central authority, repository, or global information means, then there is no mechanism for protecting the P2P networks. Structured P2P systems and unstructured P2P systems are the two types of decentralized network.

The structured peer-to-peer network is structured on a specific topology, and the protocol ensures that any node can efficiently search the network for a file or resource, even if the resource is extremely rare. The unstructured p2p network is formed by establishing arbitrary connection between the peers. The multicast overlays such as peer-to-peer overlays (e.g. Gnutella) are also incorporated in the overlay networks. When the overlay links are acknowledged randomly an unstructured P2P network is formed. The p2p network can be easily build, if a new peer that wants to join the network can replica the existing links of another node and then forms its own links over time.

The decentralized P2P networks are independent of a single server and they have to invest in server farms to guarantee the scalability of their systems [6]. There are some obvious advantages to decentralizing the C7C mechanism "self-healing" nature of the network, along with "servers" that actually share files. Each peer is frequently advertising its presence, as well as requesting updates from other peers [3]. There are many approaches that have been for detecting the botnets such as botminer and botgrep. The botminer can detect the botnets that have similar malicious activities [4]. It can differentiate between the authenticated and malicious user. But botminer has some limitations [1]. It can't able to identify the user with mixed characteristics. The botgrep can identify the botnets based on the network traffic. The disadvantage of this method is it is hard to maintain the traffic information. So, in order to detect the botnets we are using a security property called data provenance integrity. It is used to verify the origin of data.

The p2p systems have the advantage of having a hash table. It can provide the efficient and quick way of retrieving the data. It can identify the rare files more easily [2]. In this paper we use this hash table for file searching. In addition to this, for verifying the identity of the peers a self certificate based approach is used. These certificates can be exchanged between the peers during communication. These certificates are generated by the peer itself. The Self Certification mechanism helps to identify the malicious content and makes the search more effective. In self certification each peer is having their own certificate authority. The certificate authority issues the identity certificate. The self certification is used for assuring secure and appropriate availability of the reputation information of a peer.

The main requirements for these are:

1. A self certificate based identity approach
2. A trivial and straightforward reputation model.

3. An attack resistant cryptographic protocol for creation of reliable global reputation information of a peer.

2. DATA PROVENANCE INTEGRITY

In P2P file-sharing systems, all peers are both sender and receiver of resources and can contact each other directly without any middle agents. Thus the security becomes a problem in unstructured p2p network. For this, data provenance integrity is used as the security property. It is used to verify the origin of the data. It is a security control and it is mainly related to the data integrity. By using this property we can identify the unwanted changes in data. It can enhance the trustworthiness of data. Data provenance integrity measures the level of trustworthiness of both data and data providers by assigning values to them. Based on these values, peers can make their more informed decisions whether to use the data or not. The way in which the data was collected is also an important aspect when determining the trustworthiness of the data. For example, if a number of self-governing sources provide the same data, such data is most expected to be true. Reputation model is serving as a data provenance property.

In p2p networks peers cooperate to perform a function. Among the independent peers some may be authentic and provide high quality service and some may be malicious which provide harmful services such as the nodes may violate the rules and behave maliciously so as to obtain some personal gain and it is possible that a third party may inject some misbehaving nodes so as to disrupt the network service to gain a competitive edge in a commercial market. In order to overcome these problems a reputation based model is used. For each peer in the network, the trust management system maintains a universal trust label. When the system is reputation-based, the label is a combination of the local opinions of all peers in the network which is based on their previous experiences with other peers. To compute it, each opinion of the peer is weighted by the reputation of the opiner, thus peers with good reputations are more influential than those with poor reputations or no reputation.

An objective of the trust management system is to permit only trusted peers to get high reputations with high prospect. This allows trusted agents to easily recognize the malicious agents and potentially cut them from transactions. For example, a file served from a un-trusted peer might be given a low integrity value by the receiving host. Likewise, the routing protocol might keep away from forwarding messages through dishonest peers. These overall reputations permit each peer to get advantage from the experiences of all other peers in the network.

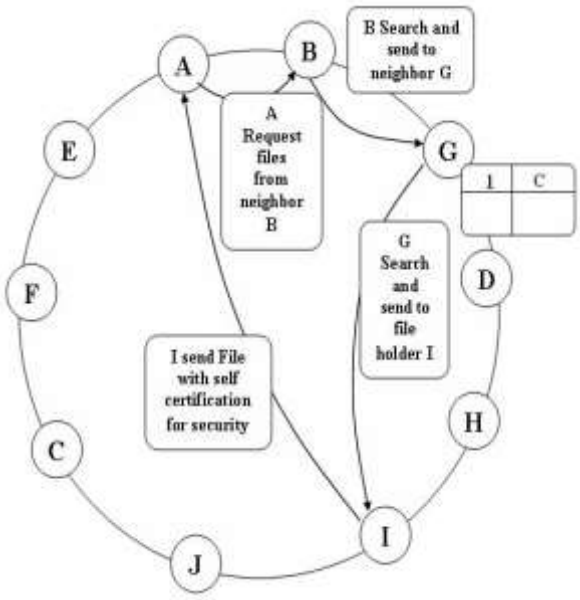


Fig 1: An overview of peer to peer unstructured network using self certification

The conversation of peer to peer networks is shown in fig 1. The node A can send the file searching request to node B. Node B can search the file in its hash table but the file is not present so it can forward the request to the node G. G can found the file in its hash table and it can forward the request to the node I because I contains that appropriate file. The node I has the file and it maintains self certification with node A to transfer the file securely.

Based on the reputation value the file searching is done in p2p network. The peer with highest reputation value is considered to be authenticated peer and the peer with lowest reputation value is considered as malicious peer. In order to receive a file from a peer, the reputation value is checked. If the value is high means then the file can be received or else it will be rejected. Thus we can prevent the peer from getting malicious data by using this reputation value. The data in the hash table is also stored based on these values.

In the decentralized P2P network, if a peer wants to find out a required file in the network then the request is passed through the network. This results in finding many peers that share their data. The major disadvantage of passing the request in the network is that the request may not always be determined. If the peer is searching for some popular data or file then the probability of finding the data is high. In other case where a peer is searching for rare data which is shared by only some peers, then it is highly doubtful that the search will be successful. As the peer and the content management store the data separately, there is no guarantee that the request will find a peer that has the required data. This passing of request causes a high amount of traffic in the network. These networks typically have poor searching efficiency. Popular P2P networks are generally unstructured. Thus a hash table is used for file searching.

A. Neighbor peer extraction

Self-governing nodes are available in many network services and some rules are required for these nodes to work together and to attain a given network functionality. To understand such network service, the neighbor node must communicate with other subset of nodes in the network e.g., send packets to neighbors, and receive packets from neighbors and so on. To assure the correct functionality of the network service such that every node can get service with desired performance, nodes must follow the predefined protocols when they participate in the communication with their neighbors.

Peer's construct its neighbors by sending connection request with its own certification likewise all peers shares its identity and its self certificate with its neighbor peer's. This certificate is compare by neighbor peer when the peer send file search request to the one of neighbor peer thus avoids unwanted flow of packets which reduce the traffic. Source peer select the neighbor peer as per highest reputation metric/value. The reputation value is calculated under each peer's total entry in the hash table or its load status.

B. Self Certification based approach

All the peers share its identity and its self certificate with its neighbor peers. The self certification is attached with identity of the peer. This certificate is compared by the neighbor peer when the peer sends file searching request to one of its neighbor peer. If the certificate is matched then the peer searches its hash table with the file name. It uses the concept of RSA and DSS.

C. Hash table based searching

In the unstructured P2P networks, peers distributing the file they have and forwarding the file searching request will plays an important role. The hash table is maintained in all the peers. It consists of its own file and the files which are received from other peers. If a file searching request is arriving means then the peer can search it in hash table. The file is present means then the request is forwarded to the peer which is the owner of that file. The anticipated system uses the hash table where each and every peer has the detached hash table.

Based on the reputation value, which is calculated based on the past activities of peer, the files are stored in the hash table. This stored information helps to achieve the file searching operation skillfully. On receiving the file searching request the peer first checks the reputation value. If the value is high then the peer can accept the request. A self certificate is exchanged between the peers to ensure the secure access of data. The hash table is used for forward the file searching request to the appropriate peer instead of the neighbor peer.

D. Trustworthy peer communication

After the successful match of self certification, each neighbor peer must recognize the source file request . Thus, the malicious peers which attempt to compromise with other peer address can be avoided. Then the source a request from the starting neighbor peer is advanced to the next peer with the hidden identity of source peer thus reduces the possibilities of unwanted rebroadcast packets and also malicious behaviors. So the initiate neighbor peer acts as temporary source, then forward the source request to its neighbor peer and this will continues until the file is found. The destination peer sends the file to the initiate neighbor and the initiate neighbor peer sends the file to the source thus avoid the length of the packet flow and control the misbehave peers.

3. CONCLUSION

This project presents the reputation model and a cryptographic protocol that provide generation of global reputation data in a P2P network, in order to detect rogues. This can improve the trustworthiness of peer and its data. It can also prevent the peers from getting malicious data from a malicious peer. The main technological contributions that are proposed in this project are the model and operations of cryptographic provenance verification in a host-based security setting and shows the provenance verification approach in a lightweight framework for ensuring the integrity of outbound packets of a host.

4. REFERENCES

[1] Junjie Zhang, Roberto Perdisci, Wenke Lee, Xiapu Luo, and Unum Sarfraz "Building a Scalable System for Stealthy P2P-Botnet Detection" IEEE transactions on information forensics and security, vol. 9, no. 1, january 2014.

[2] S. Rhea, D. Geels, T. Roscoe, and J. Kubiatowicz, "Handling churn in a DHT," in *Proc. Annu. Conf. USENIX Annu. Tech. Conf.*, 2004, pp. 127–140.

[3] S. Stover, D. Dittrich, J. Hernandez, and S. Dietrich, "Analysis of the storm and nugache trojans: P2P is here," in *Proc. USENIX*, vol. 32. 2007, pp. 18–27.

[4] G. Gu, R. Perdisci, J. Zhang, and W. Lee, "Botminer: Clustering analysis of network traffic for protocol- and structure-independent botnet detection," in *Proc. USENIX Security*, 2008, pp. 139–154. Forman, G. 2003.

[5] D. Dagon, G. Gu, C. Lee, and W. Lee, "A taxonomy of botnet structures," in Proc. 33rd Annu. Comput. Security Appl. Conf., 2007, pp. 325-33.

[6] A. Binzenhofer, D. Staehle, and R. Henjes, "On the stability of chordbased P2P systems," i*n Proc. IEEE Global Telecommun. Conf.*, vol. 2. Nov./Dec. 2005, pp. 884–888.

International Journal of Computer Applications Technology and Research
Volume 3– Issue 11, 682 - 684, 2014

Ensure Security and Scalable Performance in Multiple Relay Networks

V.Eswaramurthy
Computer Science and Engineering
V.S.B Engineering College
Karur,India

A.P.V Raghavendra
Computer Science and Engineering
V.S.B Engineering College
Karur,India

Abstract: A relay network is a broad class of network topology commonly used in networks, where the source and destination are interconnected by means of a some nodes. In such a network the source and destination cannot transmit to each other directly because the distance between the source and destination is greater than the transmission range of both of them, hence the demand for intermediate node(s) to relay. The problem of detecting malicious relay nodes in single source, multi-relay networks has been studied in the literature for different relaying schemes. Relay nodes in apply network coding while those in and follow the decode-and-forward protocol. The authors consider a peer-to-peer (P2P) network in which peers receive and forward a linear combination of the exogenous data packets. To check out the integrity of the received packets, a key signature vector is generated at the source node and broadcasted to all nodes where it is used to check the integrity of the received packets. In and several information theoretic algorithms for mitigating falsified data injection effects are proposed. The network modeling used in these works is composed of a single source, multiple intermediate nodes which utilize network coding. We consider a multiple access relay network where multiple sources send independent data to a single destination through multiple relays, which may interject falsified data into the network. To detect the malevolent relays and dispose (efface) data from them, trace bits are embedded in the information data at each source node.

Keywords: Multiple access relay network, trade-off between reliability and security, falsified data injection and forward error correction**.**

1. INTRODUCTION

Multiple access relay networks, relay nodes may combine the packets received from different sources to generate parity symbols (packets) and send them to the destination. Then, the destination may usage the network generated parity symbols (packets) to enhance the reliability by decoding. While this technology is promising in improving communication quality, it also represents a new challenge at the physical layer due to the dependency of the cooperation. That is, reliance on implicit trust relationship among participating nodes makes it more vulnerable to falsified data injection. Although this might also occur in a traditionalistic system without cooperative communication, its effect is far-off more serious with cooperative communication. If a false packet is interjected into the buffer of a node, the output of the node will become improve, and this may soon propagate to the full network.

The problem of detecting malevolent relay nodes in single-source, multi-relay networks has been studied in the literature for different relaying schemes. Relay nodes in apply network coding while those in follow the decode-and-forward protocol. In the authors consider a peer-to-peer (P2P) network in which peers receive and forward a linear combination of the exogenous data packets. To check out the integrity of the received packets, a key signature vector is generated at the source node and broad-casted to all nodes where it is used to check the integrity of the received packets. In lot of information theoretic algorithms for mitigating falsified data injection effects are proposed. The network modeling used in these works is composed of a single source, multiple intermediate nodes which utilize network coding.

In all algorithms proposed in there are two fundamental assumptions. First, all exogenous data packets are known at a single node to generate the hash or the signature vector. Therefore, these algorithms cannot be applied in multi-source scenarios because each source generates independent packets and thus the packets of all sources are not available at a single node. Second, each received packet is decrypted independently, and then the integrity from the decoded packet is checked using the hash or the signature vector. However, when the received packets are combined before decoding, a different approach needs to be developed to check the credibility (integrity) of the received packets. For example, in three-terminal cooperative diversity systems, the packets of the source and that from the relay are combined (e.g. using maximal ratio combining (MRC)) before decoding the message packet and then the integrity is checked on the decoded message packet. In the authors consider inserting a number of tracing bits in the data stream at the source in a cryptographically secure manner in single source scenario. The receiver then calculates the ground truth of the tracing bits and compares them with the tracing bits received from the relay path to determine whether a relay node is adversarial or cooperative. If the correlation coefficient between them is above a threshold then we decide that the relay node is cooperative and, otherwise, it is malevolent. The threshold can be chosen to achieve a target false alarm, misdetection, or error probability. The authors of propose a statistical detection technique in order to mitigate malevolent behavior in adaptive decode-and-forward (DF) cooperative diversity.

To exploit the detection outcome to enhance the reliability of decoding by erasing (discarding) the data received from the adversarial nodes and correcting the erasures. The motivating is that erasures can be corrected twice as many as errors. However, the information in the presence of attack may not be perfect in practice. The false alarm results in an erasure of correct bit, while the miss detecting may result in an error in place of an erasure. Since the chance of false alarm and that of miss detection depend on the amount of tracing bits and the

errors-and-erasures correction capability depends on the amount of parity bits, we require there exists an optimal allocation of the redundancy between tracing bits and parity bits that minimizes the probability of decoding error at the destination. Here, the tracing bits are to identify the malevolent relay nodes and erase the data received by them, while the parity bits are to the correct errors caused by channel and noise. For a given redundance, more parity bits (more reliability) implies less tracing bits (less security), and vice versa. That is, there exists a trade-off between reliability and security. We enquiry the optimal allocation of a given amount of redundancy (trade-off) between tracing bits and parity bits.

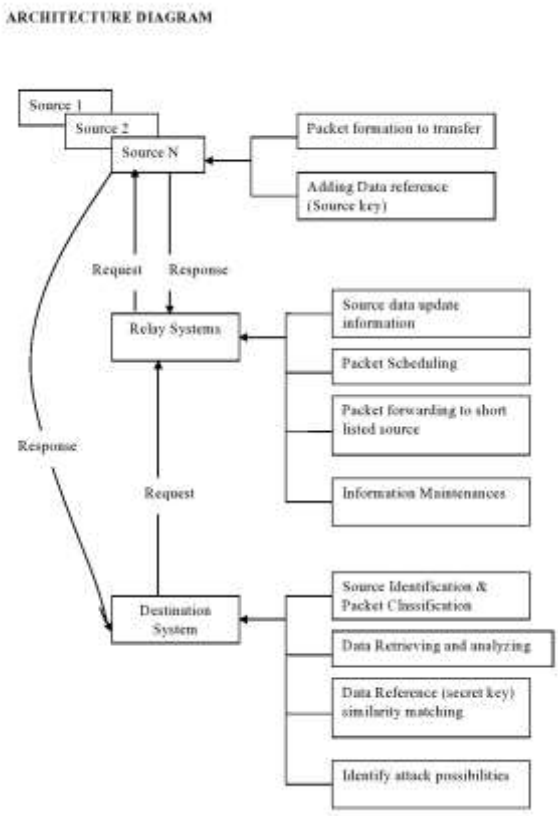


Fig. 1 Architecture Flow Diagram

2. RELATED WORK

2.1 Multiple Access Relay System

A multiple access relay network where multiple sources send independent data to a single destination through multiple relays. Multiple relay systems maintain the current information of the sources connection details and the respective files details. As per request and response relay system communicate with the source systems. In multiple access relay networks, relay nodes may combine the information's received from different sources to generate scheduling process as per destination request and forward the request to respective short listed source.

2.2 Source Response System

As per relay node request each source send the periodic update information about its connection status and the files information. The source generates independent packets after get the file request from the relay node then generate source key which is based on the contents in the file like

- Mitigation by Forwarding Misbehaviors in Multiple access relay network

reference/tracing bits. Then classify the destination system form the request packet and route the file to the destination system. At each source, the tracing bits are embedded in the k message bits using a position key κp which is common for all sources and is known to all source nodes and the destination. The generation and position keys are assumed to be unknown to the relay nodes. So, even if a relay is compromised the information on the tracing bits cannot be released to the attacker.

2.3 Destination Request System

To detect the malevolent relays and discard (erase) data from them, tracing bits are embedded in the data at each source node. The destination node then computes the ground truth of the tracing bits and compares them with the tracing bits received from the relay path to determine whether a relay node is adversarial or cooperative. Destination system sends the file request to the relay node and waits till the file gets download. After getting download request from the source system, the destination system accept the download request and classify the packet for to identify any false data may injected and identify the malevolent relay node.

2.4 False Data Injection Attack Detection

This module exploit the detection outcome to enhance the reliability of decoding by erasing (discarding) the data received from the adversarial nodes and correcting the erasures. Here, the tracing bits are to identify the malevolent relay nodes and erase the data received from them. Generate the data references for the content in the received file and calculate the distance between the data and find the similarity than compare with threshold, finally identify the malevolent activity of relay node and the injected data's.

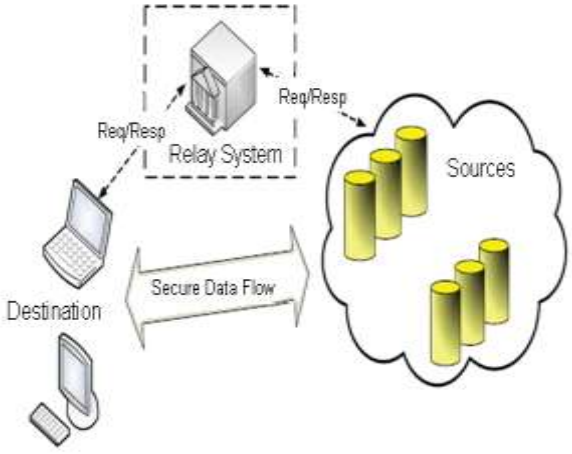


Fig. 2 Architecture Design

3. SECURE AND SCALABLE SCHEDULING PROCESS IN RELAY NETWORKS

We believed a multiple access relay network and investigated the following three processes:

- Trade-off between reliability and security under falsified data injection attacks
- Prioritized analog relaying

In the first process, a multiple access relay network where multiple sources send independent data to a single destination

through multiple relays which may inject a falsified data into the network. To detect the malevolent relays and discard (erase) data from them, tracing bits or secure key or data reference are embedded in the data at each source node. The performance metrics gains provided by the update optimal allocation/scheduling of data forwarding and the tradeoff between reliability and security are analyzed.

In the second process, a multiple access relay network where multiple sources send independent data simultaneously to a common destination through multiple relay nodes. Relay systems maintain update information about the source and its data. As per destination request relay system schedule the source and send the request packet to the respective source.

In the third process, a destination layer approach to detect the relay node that injects false data or adds channel errors into the network encoder in multiple access relay networks.

The misbehaving relay is detected by using the source key or data reference detection rule which is optimal in the sense of minimizing the probability of incorrect decision (false alarm and miss detection). The proposed schema does not require sending extra bits at the source, such as hashish function or message authentication check bits, and hence there is no more transmission overhead. The side data regarding the presence of forwarding misbehavior is exploited at the decoder to enhance the reliability of decoding.

4. CONCLUSION

Optimal allocation of redundancy between tracing bits and parity bits that minimizes the probability of decoding error or maximizing the throughput. The generation and position keys are assumed to be unknown to the relay nodes. So, even if a relay is compromised the information on the tracing bits cannot be released to the attacker. When the total amount of redundancy (sum of tracing bits and parity bits) is fixed, more redundancy should be allocated to the tracing bits for higher probability of being malicious and less on the tracing bits for lower SNR. Analyzed the energy gain (saving) and the throughput gain provided by the optimal redundancy allocation.

5. FUTURE ENHANCEMENT

To overcome the drawbacks, enhance the system to achieve more scalability. If any sources update any file location, it needs to update the location information which maintain in the relay system thus overcome the false routing. If any source goes offline i.e. disconnect from the relay systems thus is must indicate offline mode in the relay node if so it must not consider for routing. By implementing these steps as our enhancement with the system, we overcome the drawbacks and get the high scalability as well as certain information about the source mode status and files location.

6. REFERENCES

[1] Taha A. Khalaf, Sang Wu Kim, and Alaa E. Abdel-Hakim, "Tradeoff Between Reliability and Security in Multiple Access Relay Networks Under Falsified Data Injection Attack" *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*, VOL. 9, NO. 3, MARCH 2014.

[2] J. N. Laneman, D. N. C. Tse, and G. Wornell, "Cooperative diversity in wireless networks: Efficient protocols and outage behavior," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3062–3080, Dec. 2004.

[3] A. Nosratinia, T. E. Hunter, and A. Hedayat, "Cooperative communication in wireless networks," *IEEE Commun. Mag.*, vol. 42, no. 10,pp. 74–80, Oct. 2004.

[4] S. W. Kim, "Cooperative spatial multiplexing in mobile ad hoc networks," in *Proc. IEEE Int. Conf. Mobile Ad Hoc Sensor Syst. Conf.*,Washington, DC, USA, Nov. 2005, pp. 387–395.

[5] A. Host-Madsen and A. Nosratinia, "The multiplexing gain of wireless networks," in *Proc. IEEE ISIT*, Adelaide, SA, USA, Sep. 2005,pp. 2065–2069.

[6] Y. Chen, S. Kishore, and J. Li, "Wireless diversity through network coding," in *Proc. IEEE WCNC*, Las Vegas, NV, USA, Apr. 2006,pp. 1681–1686.

[7] X. Bao and J. Li, "Matching code-on-graph with networks-on-graph: Adaptive network coding for wireless relay networks," in *Proc. Allerton Conf. Commun., Control Comput.*, Champaign, IL, USA, Sep. 2005,pp. 1–10.

[8] C. Hausl and P. Dupraz, "Joint network-channel coding for the multipleaccess relay channel," in *Proc. 3rd Annu. IEEE Commun. Soc. Sensor Ad Hoc Commun. Netw.*, Reston, VA, USA, Sep. 2006, pp. 817–822.

International Journal of Computer Applications Technology and Research
Volume 3– Issue 11, 685 - 692, 2014

Adoption of Integrated Healthcare Information System in Nairobi County: Kenyatta National Hospital versus Mater Hospital

Kirichu Caroline Njeri
Faculty of Information Science and Technology
Kisii University
Nairobi, Kenya

Samuel Matende
Associate Faculty
Kisii University
Nairobi, Kenya

Nicodemus Mokaya
Associate Faculty
Kisii University
Nairobi, Kenya

Jades Kalunda Muema
School of Computer Science and Information Technology
Dedan Kimathi University
Nyeri, Kenya

Abstract: Health care information systems are aimed at facilitating the smooth running and interoperability of the health care delivery processes to ensure efficiency and effectiveness; however, the complexity, heterogeneity and diversity of the health care sector especially in Kenya poses serious challenges especially in relation to integration of the systems. There is a large disconnect between the public and private health care delivery systems characterized by fragmentation of services, locally within hospitals (among primary, secondary and tertiary health care settings) and across different health care centers. This research is aimed at examining the adoption of integrated healthcare information system in Nairobi County; Kenyatta National Hospital represents the public sector and The Mater Hospital the private sector. A sample size of 100 users on information system from the two hospitals picked from the primary secondary and tertiary levels were selected and questionnaires administered to them. Data was analyzed through descriptive statistics with the aid of SPSS. The results of the study indicated that there was a huge disparity between healthcare information system adoption in the public and private sectors with the private sector's adoption being at an advanced stage. The major barriers to adoption including social political barriers, financial constraints and technical/technological barriers also presented.

Keywords: Integrated healthcare, Adoption, Hospital

1. INTRODUCTION

The introductory chapter covers areas such as the background of the study, statement of the problem, objectives of the study, significance of the study and the conceptual framework.

1.1. Background of the Study

Health is a state of complete physical, mental and social well-being and not merely the absence of disease or infirmity (World Health Organisation, 2003). Health care systems are systems which are connected and have independent parts or agents bound by a common purpose and acting on their knowledge (Institute of medicine 2001). Public health care is usually provided by the government through national healthcare institutions. Private health care can be provided through "for profit" hospitals and self-employed practitioners, and "not for profit" non-government providers, including faith-based organizations. Both the private and public sectors have engaged in numerous efforts to promote use of IT within health care institutions and across care delivery settings. (Healthcare Financial Management Association 2004; iHealthBeat, 2003).

In Kenya, the use of information systems in the public health sector is limited. The Government through the Ministry of Health has initiated reforms towards decentralization of health care services and development and integration of Information Technology. However, a large number of these plans have not been successfully implemented. There is a large disconnect between the public and private healthcare sector and the entire health sector as far as information sharing is concerned. The main reason for choosing this topic is due to the fact that successful health care is considered to be the cornerstone of any successful patient-centered health care delivery system and therefore requires special attention to ensure success The Lack of integration and interoperability among the subsystems and cross sector provide a fertile research ground. USAID, (2010).

There is also the need for continuity of care and information exchange within the health sector has introduced an imperative call for successful adoption of health care information system (WHO 2002). There have been numerous attempts to introduce integrated and interoperable health care information system in the public and private healthcare domains with varied results. What has been evident however is the private and public healthcare delivery systems have varied approaches to information systems development and adoption; as such it is important to perform a comparative review of the two with the aim of aiding the health sector to gain from the best of both worlds. Health care information systems are a prerequisite for coordinated, integrated, and evidence-informed health care (WHO 2002).

1.2. Statement of the Problem

The health care systems in Kenya are typically made up of a number of relatively independent health programs and services which all maintain their own vertical and uncoordinated reporting systems. A patient's medical records are recorded on paper, electronically or a combination of both, and are typically held in different locations. This makes it difficult to get a complete picture of the patient's healthcare journey. Additionally, fragmentation of services, locally within hospitals and between primary, secondary and tertiary health care settings, alongside the use of different information systems in different care settings can make it difficult to safely communicate information. This may lead to miscommunication or missing patient information, ultimately compromising patient safety. The problem of HIS fragmentation and integration of health care information system is consequently a priority that needs to be addressed to realise successful patient centred healthcare delivery in the country. (African Development Bank et al, 2012), Health Information and Quality Authority, Brailer, 2013).

According to Mwangi, (2013). Studies have not only indicated insufficient adoption of HIS system in the country but also a major disconnect between public and private adoption.

Therefore this research seeks to address this problem by comparing healthcare Information System as implemented in both private and public Hospitals.

1.3. Research Objectives

The main objective of this research is to study the adoption of integrated healthcare information system in Nairobi County; in this regard KNH will represent public hospitals and The Mater Hospital, private hospitals. The specific objectives in this regard are:

i. To evaluate and compare the existing health care information systems in Nairobi County.
ii. To determine key success factors in the successful adoption of healthcare information system in Nairobi County.
iii. To determine the barriers to successful adoption of healthcare information system in Nairobi County.

1.4. Significance of the Study

The findings and recommendations of this study will provide an insight and add to academic knowledge both in the field of Information Systems (and their adoption) and health care delivery. The comparative study will reduce the disparities that exist between the private and public health hospitals together with the insufficient information sharing among the stake holders.

This study will also go a long way in helping the healthcare providers and information systems developers in the development and adoption of health care information systems that are patient-centered, interoperable and integrated to ensure not only effective and efficient operations but also facilitate the sharing of relevant health care information across the health care delivery spectrum. The knowledge gained from the study will provide great insights and guidelines to the leaders, managers and authorities including the government in decision making, policy formulation, strategic planning and regulation of the health care sector in regards to information management to improve service delivery and improvement of health care. The primary stakeholders of the health care system would also be beneficiaries of this study by adopting and implementing their information systems in a way that they integrate and interoperate with the healthcare system and as such be able to share information.

1.5. Conceptual Framework

The conceptual framework uses the attributes of the updated DeLone and McLean (D&M) information system success model which are also the key success factors for successful implementation (Zaied, 2012); the researcher has also modified the model and included other parameters for evaluation that are important for this study including management support, training, perceived usefulness. It also uses aspects of TAM model (Davis, 1989) to determine the adoption factor of HIS systems. These additional parameters include: Management support, level of training, perceived usefulness, Perceived ease of use, behavioral intention.

Numerous studies have been done on healthcare information system in Kenya both in the public and private sectors. However no study has been done on the comparison of the adoption of integrated health care information system between public and private hospitals in Kenya, more so with focus on integration and interoperability. This research aims to fill this gap in a unique way by modifying the existing model and present a unique perspective of the Kenyan health care information system.

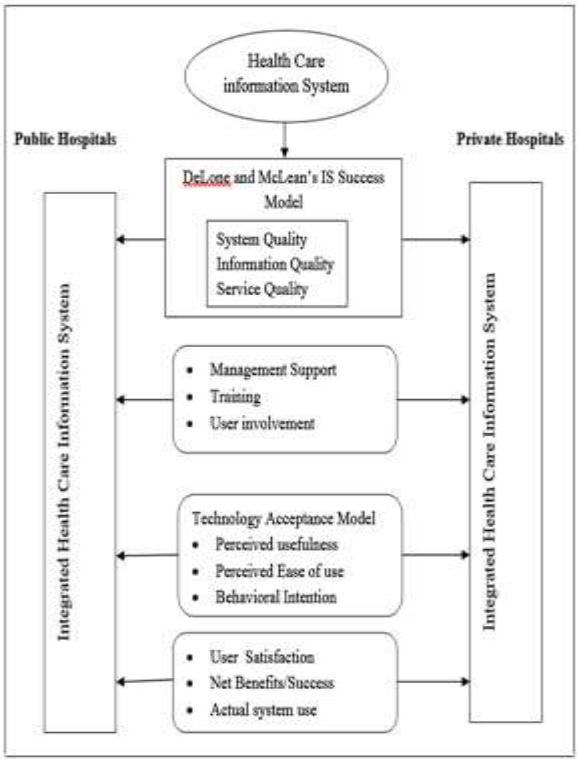


Figure 1: Conceptual Framework

2. LITERATURE REVIEW

2.1. Overview of Healthcare Information Systems

Health care systems are a set of connected or interdependent parts or agents including care givers and patients bound by a common purpose and acting on their knowledge (Institute of Medicine 2001). Health care information systems that are successfully developed and implemented can improve health care efficiency and effectiveness. Despite its importance, the health care domain has been underrepresented in the debate on the development of information systems from both an empirical as well as theoretical viewpoint. (Fichman et al., 2011; (Callen et al., 2007).

The health care information system management structure consists of the following components: health care information system resources including persons, supplies, and a set of organizational rules (definition of staff responsibilities, supply management procedures, and computer maintenance procedures), to ensure efficient use of health care information system resources. At each level of the hospital organizational structure, health care information system has specific functions that require specific decisions to be made, intended ultimately to improve the health status of the patients. (Nyamtema, 2010; Locatelli, 2010).

2.2. Healthcare Information Systems Function in Health Care Delivery

Healthcare information systems facilitate the efficient, effective and timely collection and sharing of relevant and correct data among these stakeholders to ensure patient centered service delivery. In general it is a combination of Health Information and Management Information. Health care information systems are a prerequisite for coordinated, integrated, and evidence-informed health care (HIQA, 2010).

To provide optimal care, healthcare institutions need timely patient information from various sources at the point-of-care, and need a comprehensive, complete and fully functional system to fulfil all these needs. One way to achieve this is through the use of IS in health care. Appropriate information and Health care Information Systems are seen as crucial to strengthening the health system in developing countries and in pursuing the particular MDGs. Successful systems are most likely to be the ones that offer opportunities for ongoing professional involvement, relative stability and security, and the capacity to support improvements in practice with useful and timely information. (AbouZahr and Boerma, 2005; WHO, 2004, HIQA, 2010).

2.3. Health Care Organization and Management of Public and Private Hospitals in Kenya

The health sector in Kenya comprises the public and private health care providers. A typical patient journey should start with contact with primary care for an initial diagnostic consultation, and might then involve the patient being referred to secondary care for more specialized treatment, or a tertiary service for even more specialized follow-up. (Walshe and Smith, 2010). However, these sectors overlap and it is frequently true that an individual patient may receive services within more than one sector at the same time (Walshe and Smith, 2010; Lapão and Dussault, 2012).

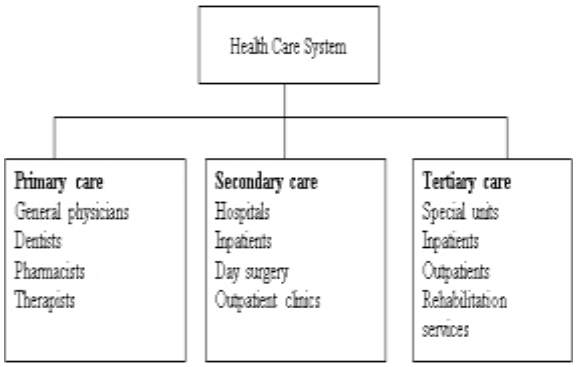


Figure 2: Generic structure of a healthcare system (Walshe and Smith, 2010)

2.4. Health Care Information Systems Success Model

Different approaches have been developed concerning information systems evaluation and each of them have both positive characteristics and flaws as well. The evaluation of a system in terms of its success is an inherently complex phenomenon. It is of vital importance that during the evaluation process both the technology that is used and the role of the users that participate and their relation to the technology must be taken into account. (Prodromos et al, 2012). For this study the researcher will use two theoretical models; the Technology Acceptance Model (TAM) and the updated DeLone and McLean's Model.

The TAM model, developed by Davis (1989) is used to measure the acceptance, adoption and use of information technology. It is very popular and two constructs are used in TAM, perceived ease of use and perceived usefulness. TAM indicates the relationship between external variables, perceived useful-ness, perceived ease of use, attitude toward use and actual usage. TAM provides information on how the design choices influence user acceptance of technology. According to Davis, if the system appears useful to the users then they are more willing to use it. (Prodromos et al, 2012). Perceived usefulness is the degree to which an individual believes that using a particular information system or information technology would enhance his or her job. Perceived ease of use is the degree to which a person believes that using a particular information technology would be free of effort. TAM model has gained wide popularity among the researchers and is one of the most influential model. This is different from other models as it does not measure success but it is used to study and predict the user's intention to use IT. (Davis, 1989; Prodromos et al, 2012).

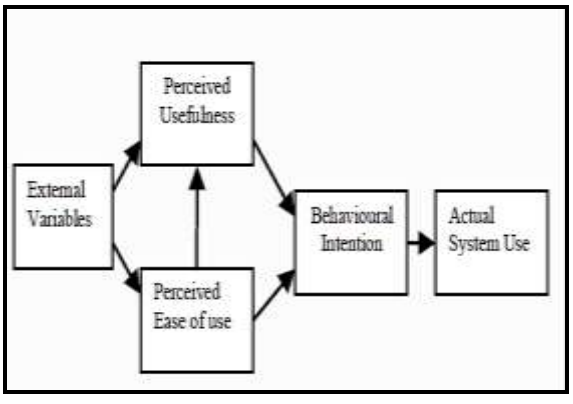


Figure 3: Technology Acceptance Model (Davis, 1989)

Six dimensions of IS success have been identified by DeLoan and McLean: system quality, information quality, information use, individual impact, and organizational impact. All these six dimensions characterize an IS both from the organizational viewpoint and the socio-technical viewpoint. Later added one more dimension, service quality. (Prodromos et al, 2012).

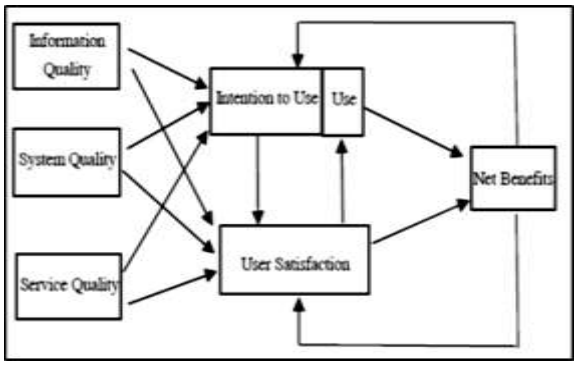


Figure 4: The updated DeLone and McLean's Model. (Zaied, 2012)

The following parameters adopted from updated DeLone and McLean's Model were used to interrogate the private and public health care information systems and bring forth the key success factors; system quality, information quality, service quality, system use, user satisfaction, and net benefits. (Nasser, 2012; Zaied, 2012).

3. RESEARCH METHODOLOGY

The target population of the research was end users in the health care facilities who interact directly with the information system at various levels in the hospitals organization structure primary, secondary and tertiary care. These include the hospitals point of entry, pharmacy, laboratories, and all other departments. Managers and Information system professionals were excluded. To facilitate data collection, the study's sampling frame constituting of respondents from the KNH, The Mater Hospital that are end users of their respective healthcare information system. The researcher used a sample size of 100 respondents from the population of 133 end users to who questionnaires were administered to collect data which was analyzed using SPSS. Descriptive statistics is used to describe the basic features of the data in this study.

4. DATA PRESENTATION, ANALYSIS, RESULTS AND DISCUSSIONS

4.1. General Information about Respondents Participation

The study was conducted at The Matter Hospital and Kenyatta National Hospital with 50% of the respondents picked from each hospital as indicated in table 1.

Table 1: Respondents participation

Sector	Target Population	Responses	Rate
Public	50	50	100%
Private	50	50	100%
Total	100	10	100%

There was 100% response rate in this study, this could be attributed to the consistent follow up by the research team who were on standby to provide explanation and answer any questions from the respondents. The fact that permission was sought from immediate superiors some of whom participated in the research and requested their juniors to participate is also a factor in this

response rate. This response rate therefore means that the study is valid.

4.2. System quality

The descriptive statistics table 2 shows the total number of variables that were involved in the analysis. Maintainability, usability and interoperability were the system quality factors considered by most respondents.

Table 2: System quality

System Quality	Mean	Std. Deviation	Analysis N
Reliability	2.07	.871	100
Usability	2.80	1.285	100
Adaptability	2.36	1.227	100
Trust	2.13	1.010	100
Maintainability	4.07	1.006	100
Integration	2.46	1.206	100
Interoperability	2.52	1.293	100

4.3. Information quality

Table 3 indicates the factors variables that were involved in the analysis on regards to information quality. Majority of the respondents felt that information availability, security and accuracy with a mean of 3.75, 3.20 and 3.07 respectively were the key factors in the determination of its quality.

Table 3: Information quality

	Mean	Std. Deviation	Analysis N
Completeness	2.66	1.210	100
Understandability	2.82	1.208	100
Security	3.20	1.212	100
Availability	3.75	1.164	100
Accuracy	3.07	1.305	100

4.4. Service Quality

According to the survey and as indicated in table 4, information system efficiency and functionality with a mean of 6.32 and 5.95 were regarded as the most significant variables when determining its service quality.

Table 4: Service quality

	Mean	Std. Deviation	Analysis N
Reliability	2.75	1.268	100
Integrity	5.18	3.406	100
Functionality	5.95	3.083	100
Efficiency	6.32	3.369	100

4.5. Management Support

In Mater hospital the respondents unanimously agreed that the management supports the adoption and use of HIS in all its daily operations not only by encouraging of the use of the system but also by addressing the problems associated with the system. This is shown in table 5 below.

Table 5: Management Support - Mater

	Discuss HIS Problems		Encourage HIS use	
	Frequency	Percentage	Frequency	Percentage
Neutral	3	6	0	0
Agree	6	12	2	4
Strongly disagree	41	82	48	96
Total	50	100	50	100

In KNH on the other hand over 60% of the respondents felt that the management was supporting the adoption and use of HIS as indicated in table 6. However the breadth of support in Mater is greater than that KNH.

Table 6: Management Support - KNH

	Discuss HIS Problems		Encourage HIS use	
	Frequency	Percentage	Frequency	Percentage
Disagree	0	0	4	8
Neutral	12	24	8	16
Agree	30	60	36	72
Strongly disagree	8	16	2	4
Total	50	100	50	100

4.6. User involvement

Table 7: User involvement - Mater Hospital

	Involvement in input design		Involvement in output design	
	Frequency	Percentage	Frequency	Percentage
Strongly Disagree	42	84	42	84
Disagree	3	6	3	6
Total	50	100	50	100

The survey shows that both The Mater hospital and KNH did not involve their users during HIS development according to 84% and 96% of the respondents even in issues that directly affect them including involvement in output and input design as indicated in tables 4.19 and 4.20.

Table 8: User involvement - KNH

	Involvement in input design	Involvement in output design

	Frequency	Percentage	Frequency	Percentage
Strongly Disagree	48	96	48	96
Disagree	2	4	2	4
Total	50	100	50	100

4.7. Perceived ease of use

The descriptive statistics table 9 shows the total number of variables that were involved in the analysis. According to the survey, the respondents felt that the IS should be easy to learn, compatible and simple.

Table 9: Perceived ease of use

	Mean	Std. Deviation	Analysis N
Easy to learn	7.46	3.443	100
Easy to manage	1.93	.912	100
Self-efficiency	1.91	1.032	100
Simplicity	2.93	1.248	100
Compatibility	2.71	.967	100

Table 10: Behavioral intention

	Mean	Std. Deviation	Analysis N
Personalization	2.27	1.328	100
Response time	1.84	.930	100
Interactivity	2.45	1.334	100
Uncertainty avoidance	3.02	1.198	100
Number of transactions executed.	3.32	1.064	100

According to the survey, number of transactions executed (mean 3.32) and uncertainty avoidance (3.02) were regarded as the most influential factors on their behavioral intention to use HIS as shown in table 10.

4.8. User satisfaction

The survey response indicates that as far as user satisfaction is concerned, the majority of the respondents were of the opinion that self-efficacy was the most important factor with a mean of 3.20 followed by personalization with a mean of 2.77 as indicated in table 10.

Table 10: User satisfaction

	Mean	Std. Deviation	Analysis N
Self-efficacy	3.20	1.086	100
Personalization	2.77	.972	100
Perceived risk	1.86	.883	100
Enjoyment	2.23	1.079	100

4.9. Barriers to Adoption of Health Care Information System:

The survey showed that majority of the respondents felt that social political barriers were the most significant with a mean of 8.21, followed by time constraints and technical\technological factors as indicated in table 11.

Table 10: Barriers to Adoption of Health Care Information System

	Mean	Std. Deviation	Analysis N
Financial constraints	4.84	3.627	100
Technical/Technology	6.70	3.613	100
Time constraints	7.84	3.468	100
Social political barriers	8.21	3.789	100
Organizational (structural)	2.02	.924	100
Change Process	2.46	1.361	100

5. SUMMARY OF RESEARCH FINDINGS

Both Mater hospital and KNH use a combination of both IS and paper based systems, however the level of HIS use in Mater hospital is far more extensive than that of KNH. Mater hospitals' HIS is viewed as to have had significant influence in ensuring effectiveness and efficiency of healthcare delivery than that of KNH. This could be attributed to its extensive use and interoperability. This is however not the case for KNH whose activities are mainly paper based and as such computerized HIS have not had as much impact on healthcare delivery. Mater hospital uses information Technology to manage virtually all their health information including collection, processing, storage, transmission, and retrieval. KNH on the other hand health information management is a combination of both paper based and computer based health information management with the later taking precedence and as such their computerized information management not as effective.

In regards to HIS information quality the users regarded reliability, maintainability and adaptability respectively as the most desirable features to ensure successful adoption. In relation to information the study determined that to the users of ranked highly information availability and security. In regard to service quality, the HIS users considered system functionality and efficiency as the most desired quality. Management's encouragement, discussing problems associated with the system were rated highly by users as being key in ensuring successful HIS adoption. The users felt that it was important that they be involved especially in the input and output design. To determine the perceived usefulness of the HIS users mostly looked at whether the system would lead to improved productivity and improved performance as key measures to determine the systems perceived usefulness of the IS. Enjoyment and

self-efficacy of the system were regarded as the key factors when it came to users' satisfaction.

The study indicated that social political barriers, financial constraints and technical/technological barriers were the major barriers to the successful adoption of HIS.

6. CONCLUSION

Both the private and public sector have adopted HIS into their hospitals with mixed results. Mater hospitals has a higher level of integration of HIS and information technology into their activities in general compared to KNH. The HIS users in Mater hospital with the encouragement and policies of the management (including training) use their HIS in most if not all of their information management; they also do not feel that there is need for significant reforms in their HIS implying that overall the system is sufficient to ensure efficient and effective health care delivery.

The users in KNH feel that their system is in dire need of significant reforms and support from the management (including training and provision of training materials on the system) to ensure successful use and improve service delivery. In regards to successful adoption of HIS system the desired characteristics were similar across the board. Social political barriers, time constraints and technical/technological barriers were deemed as the most significant barriers to successful HIS in the health care sector in Nairobi County.

7. RECOMMENDATIONS

In the view of the findings of the research, the researcher recommends that the key stakeholders in the healthcare sector device an approach that would ensure a successful adoption of HIS that is integrated and interoperable across both the private and public sector. The public sector should learn from the private sector how they have managed to successfully adopt and use HIS to improve health care service delivery and make amends on their approach. Users of HIS are seldom involved in the system design and as such their input should be sought and considered especially considering they will be the ones to use the systems and as such their needs and requirements should be considered. The healthcare sector managers should encourage and insist on the use of HIS and provide the necessary support in terms of resource allocation and involvement for successful adoption.

The barriers to successful adoption should be addressed and be minimized if not eliminated to ensure not only successful adoption but also improvement in health care service delivery.

Suggested area for further study

The three most significant barriers to successful HIS adoption in Nairobi County should be addressed if the sector is to ensure efficient and effective service delivery. The researcher therefore suggests that studies be carried out to determine systematic approaches that would be used to minimize this impediments from their root causes and ensure successful adoption of HIS in an effort to provide efficient and effective patient centered health care delivery. Further studies should focus on implementation of HIS that are not sector centered but ones that cut across the board

8. REFERENCES

Anderson, G. (2009). Improving Patient Safety with Information Technology, In: Handbook of Research on Advances in Health Informatics and Electronic Healthcare Application, Khoumbati, et al (Eds.), pp. 1-16, Medical Information Science Reference, ISBN 978-1-60566-030-1, Hershey (PA).

Brailer J. (2013). Interoperability: The Key to the Future Health Care System. Health Affairs. http://www.ncbi.nlm.nih.gov/pubmed/15659454. Accessed on: 29 27 February 2014.

Casey G. et al. (2012). Introduction to Information System: Support and Transforming Business (Fourth Edition). New Jersey: John Wiley and Sons, Inc.

Christensen M. et al; (2009). The Innovator's Prescription: A Disruptive Solution for Health Care, McGraw–Hill, ISBN 978-0-07-159209-3, New York

Davis, F. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technolo-gy. MIS Quarterly 13 (3), 319-340.

Finchman, G. et al (2011). Editorial Overview - The role of IS in Healthcare. Information Systems Research, Vol. 22, No. 3, pp. 419-428

Floden J. (2013). Essentials of Information Systems. Gazelle Book Services.

Gay R. and Peter A. (2012). Selecting Samples. Prentice Hall. Upper Saddle River, New Jersey, Columbus Ohio.

Government of Kenya (2007). Kenya Vision 2030. A Globally Competitive and Prosperous Kenya.

Health Information and Quality Authority. (2013). Developing National eHealth Interoperability Standards for Ireland: A Consultation Document. Health Information and Quality Authority Dublin Regional Office George's Court George's Lane Smithfield Dublin 7.

Healthcare Financial Management Association. 2004. Financing the future report 2: How are hospitals financing the future? The future of capital spending. Westchester, IL: HFMA.

IHCO (2011). ICT in Health Care: Innovation in Search of an Author, School of Management of Politecnico di Milano.

Kaplan, R. and Porter, M. (2011) How to solve the cost crisis in health care, Harvard Business Review.

Mwangi C. (2013). Computerization of the Kenyan Health Care Records. Helsinki Metropolia University of Applied Sciences. Helsinki.

Nasser H. (2012). An Integrated Success Model for Evaluating Information System in Public Sectors. Journal of Emerging Trends in Computing and Information Sciences. VOL. 3, NO. 6, ISSN 2079-8407

Nyamtema S. (2010). Bridging the gaps in the Health Management Information System in the context of a changing health sector. BMC Medical Informatics and Decision Making, vol. 10, pp. 1-36.

Prodromos D. et al (2012). Hospital Information System Evaluation. 10th International Conference on Information Communication Technologies in Health, Samos Island Greece

Rada, R. (2008). Information Systems and Healthcare Enterprises, IGI Publishing, Hershey (PA)

Rainer R.et al (2013). Introduction to Information Systems, Third Canadian Edition. John Wiley \& Sons Canada, Limited

Reynolds G. and, Stair R. (2013). Information System Essentials. Cengage South-Western

Rolli, J. (2012). Fundamentals of Information Systems. SeyfKashani, NajibeAfnan, Semat Publications, Tehran.

Sandiford, P. et al (1992). What can Information Systems do for Primary Health Care? An International Perspective, Social Science and Medicine (34:10), pp. 1077-1087.

United States Agency for International Development. (USAID), (2010). Kenya Health System Assessment 2010. Bethesda, MD: Health Systems 20/20 project, Abt Associates Inc.

Zaied H. (2012). An Integrated Success Model for Evaluating Information System in Public Sectors. Journal of Emerging Trends in Computing and Information Sciences. VOL. 3, NO. 6. CIS Journal. ISSN 2079-8407.

International Journal of Computer Applications Technology and Research
Volume 3– Issue 11, 693 - 696, 2014

Hop- by- Hop Message Authentication and Wormhole Detection Mechanism in Wireless Sensor Network

S.Subha
Computer Science and Engineering
V.S.B Engineering College
Karur, India

U.Gowri Sankar
Computer Science And Engineering
V.S.B Engineering College
Karur, India

Abstract: One of the most effective way to prevent unauthorized and corrupted message from being forward in wireless sensor network. So to restrict these problems many authentication schemes have been developed based on symmetric key cryptosystem. But there is high computational and communication overhead in addition to lack of scalability and resilience to node compromise attacks. So to address these isuues polynomial based scheme[1] was introduced. But in these methods it having the threshold problem that means to send the limited message only because to send larger number of message means the attacker can fully recover. So in my existing system a scalable message authentication scheme based on elliptic curve cryptography. This scheme allows any node to transmit an unlimited number of messages without suffering the threshold problem. But these method only detect the black hole and grey hole attacks are dected but does not detect the worm hole attack. In my proposed system to detect the worm hole attack. Worm hole attack is one of the harmful attack to which degrade the network performance. So, in the proposed system, one innovative technique is introduced which is called an efficient wormhole detection mechanism in the wireless sensor networks. In this method, considers the RTT between two successive nodes and those nodes' neighbor number which is needed to compare those values of other successive nodes. The identification of wormhole attacks is based on the two faces. The first consideration is that the transmission time between two wormhole attack affected nodes is considerable higher than that between two normal neighbor nodes. The second detection mechanism is based on the fact that by introducing new links into the network, the adversary increases the number of neighbors of the nodes within its radius. An experimental result shows that the proposed method achieves high network performance..

Keywords: **Hop-by-hop authentication, public-key cryptosystem, source privacy, Modified ELGamal signature, Round Trip Time.**

1. INTRODUCTION

A Wireless Sensor Network is a self-configuring network of small sensor nodes communicating among themselves using radio signals, and deployed in quantity to sense, monitor and understand the physical world.A sensor network consists of multiple detection stations called sensor nodes, each of which is small, lightweight and portable. Every sensor node is equipped with a transducer, microcomputer, transceiver and power source. The transducer generates electrical signals based on sensed physical effects and phenomena. The microcomputer processes and stores the sensor output. The transceiver, which can be hard-wired or wireless, receives commands from a central computer and transmits data to that computer. The power for each sensor node is derived from the electric utility or from a battery.

2. PREVIOUS WORK

A message authentication code [11] is a short piece of information used to authenticate a message and to provide integrity and authenticity assurances on the message. So in wireless communication the message will be hacked by the attacker can modify message. So to avoid the attacker so many methods are introduced in wireless sensor networks. Many message authentication scheme have been developed. It have the limitation of high computational and communication overhead in addition to lack of scalability to node compromised attack. So to avoid this problem we introduce polynomial based scheme was introduce. But this algorithms also having some problem. While enabling intermediate node authentication[2]. When the number of message transmitted is lager then the threshold , the attacker can fully recover the polynomial. So to avoid this problem in my existing system to introduce Modified Elgamal Signature[4] scheme was developed this is used for signature verification process. Then another method was also implemented that is SAMA on elliptic curve these is used in verification process. This scheme allows any node to transmit an unlimited number of message without suffering the threshold problem. This method also detect the block hole and gray hole attack.

DRAWBACK OF EXISTING SYSTEM

1. This method does not detect the wormhole attack.
2. Degrade the network performance.
3. It does not have computational and communication overhead.
4. It have less efficiency.

3. TERMINOLOGY AND PRELIMINORY

3.1 Model And Assumption

Security is an important concern in the wireless sensor networks. Message authentication plays a key role in thwarting unauthorized and corrupted messages from being forwarded in networks to save the precious sensor energy. In addition to that, in the wireless sensor networks, wormhole attacks can cause severe damage to the route discovery mechanism used in many routing protocols. In a wormhole attack, the malicious nodes will tunnel the eavesdropped packets to a remote position in the network and retransmit them to generate fake neighbor connections, thus spoiling the

routing protocols and weakening some security enhancements.

3.2 Terminology

i. Modified ElGamal Signature Scheme

The modified elgamal signature [5] scheme consist of three algorithms:

Key generation algorithm. Let p be a large prime and g be a generator of $\mathbb{Z}$: Both p and g are made public. For a random private key^{p} x 2 $\mathbb{Z}_p$, the public key y is computed from y ¼ g^x mod p.

Signature algorithm. The MES can also have many variants. For the purpose of efficiency, we will describe the variant, called optimal scheme. To sign a message m, one chooses a random K€$Z^*_{p-1,}$then computes the exponentiation $r=g^k$ mod p.

Verification algorithm. The verifier checks whether the signature equation g^s ¼ $ry^{rh\eth m;r\flat}$ mod p: If the equality holds true, then the verifier Accepts the signature, and rejects otherwise.

4. PROPOSED WORK

In my existing system to detect the black hole and gray hole attack. But does not detect the wormhole attack[9]. So one innovative techniques is used in my proposed work which is called on efficient wormhole detection mechanism in wireless sensor network.

Definition: In this section, to detect the wormhole attack which is based on the RTT of the message between successive nodes and their neighbor numbers.So we finding wormhole attack by using two mechnisums:

1. **Route Finding**: At that phase, the source node is responsible to construct the hierarchical routing tree to other nodes in the sensor field. The node sends the route request (R_{REQ}) message to the neighbor node and save the time of its R_{REQ} sending T_{REQ}. The intermediate node also forward the R_{REQ} message and save T_{REQ} of its sending time. When the R_{REQ} message reach to the destination node, it reply route reply message (R_{REP}) with the reserved path. When the intermediate node receives the R_{REP} message, it saves the time of receiving of R_{REP} T_{REP}. Our assumption is based on the RTT of the route request and reply. The RTT can be calculated as

$$\mathbf{RTT = T_{REP}-T_{REQ}}$$

All intermediate nodes save this information and then send it also to the base station.

2.Construction of neighbor list: In this first phase, each node broadcast the neighbor request (N_{REQ}) message. The N_{REQ} receiving node responds to the neighbor reply (N_{REP}) message. The requesting node constructs the neighbor lists based on the received of N_{REP} messages and counts its neighbor number (*nn*). After that the source node starts the route construction phase.

ADVANTAGE OF PROPOSED WORK

1. To detect the wormhole detection
2. It give high network performance
3. This method having high efficiency
4. It give high message source privacy.

5.RELATED WORK

In my existing system secret polynomial-based message authentication scheme was introduced. This sharing scheme, where the number of message transmition is below the threshold means system will be secure and the enables the intermediate to node to verify the authenticity of message. But the message is large than the threshold means the system should be compromised by the attacker, then system should be completely broken. Then to avoid these threshold problem to introduce Modified ELGamal[5] Signature scheme which is used in my existing system. While enabling intermediate node authentication allows any node to transmit unlimited number of message without suffering the threshold problem. Then the system should be in very secure and attacker does not compromise the nodes. Then these type of MES schemes also to find the block hole and gray hole attack. But this method does not detect worm hole attack because worm hole attack is one harm full attack which degrade the network performance.

So in my proposed system to find the wormhole attack by using the RTT between two successive nodes. Then worm hole attack is a malicious node tunnels message received in one part of the network over a low latency link and replay them in a different part. Due to the nature of wireless transmission, the attacker can create a wormhole even for packets not addressed to itself, since it can overhear them in wireless transmission and tunnel them to the colluding attacker at the opposite end of the wormhole.

6. PROPOSED WORMHOLE DETECTION MECHANISUM

In this section we present our wormhole detection[9] mechanism. Our detection is based on the RTT of the message between nodes.

System modules: These wormhole detection mechanism using some method to detect the attacker that's are:

1. Route Finding
2. **Construction of neighbor list**
3. **Wormhole Attack Detection**
4. **Calculation of RTT**
5.

Phase1: Route Finding

At that phase, the source node is responsible to construct the hierarchical routing tree to other nodes in the sensor field. The node sends the route request (R_{REQ}) message to the neighbor node and save the time of its R_{REQ} sending T_{REQ}. The intermediate node also forward the R_{REQ} message and save T_{REQ} of its sending time. When the R_{REQ} message reach to the destination node, it reply route reply message (R_{REP}) with the reserved path. When the intermediate node receives the R_{REP} message, it saves the time of receiving of R_{REP} T_{REP}. Our assumption is based on the RTT of the route request and reply. The RTT can be calculated as

$$\mathbf{RTT = T_{REP} - T_{REQ}}$$

All intermediate nodes save this information and then send it also to the base station.

Phase2: **Construction of neighbor list**

In this first phase, each node broadcast the neighbor request [11] (N_{REQ}) message. The N_{REQ} receiving node responds to the neighbor reply (N_{REP}) message.The requesting node constructs the neighbor lists based on the received of N_{REP} messages and counts its neighbor number (nn). After that the source node starts the route construction phase.

Phase3: Wormhole Attack Detection

In this phase, the source node calculates the RTT [9] of all intermediate nodes and also it and destination. It calculates the RTT of successive nodes and compares the value to check whether the wormhole attack can be there or not. If there is no attack, the values of them are nearly the same. If the RTT value is higher than other successive nodes, it can be suspected as wormhole attack between this link. The nextdetection mechanism is based on the fact that by introducing new links into the network graph, the adversary increases the number of neighbors of the nodes within its radius. So it needs to check the nn of these two nodes which find in section 4.2. Equation (2) is adopted form [5] to estimate average number of neighbors d. It is approximated as

$$\mathbf{d = (N-1)\,\pi\, r^2 / A}$$

where A is the area of the region, N is the number of nodes in that region and r is the common transmission radius. For example, if the RTT value between A to B is considerably greater than for other links, it needs to check the value of nn for A and B. If also the nn value for A and B is higher than the average neighbor number d, there is a suspect that a wormhole link is between nodes A and B. In this way the mechanism can pin point the location of the wormhole attack.

Phase 4: Calculation of RTT

In this subsection, the detailed calculation of the RTT is discussed. The value of RTT is considered the time difference between a node receives R_{REP} from a destination to it send R_{REQ} to the destination. During route setup procedure, the time of sending R_{REQ} and receiving R_{REP} is described in Figure 1. In this case, every node will save the time they forward R_{REQ} and the time they receive R_{REP} from the destination to calculate the RTT. Given all RTT values between nodes in the route and the destination, RTT between two successive nodes, say A and B, can be calculated as follows:

$$RTT_{A,B} = RTT_A - RTT_B$$

Where RTT_A is the RTT between node A and the destination, RTT_B is the RTT between node B and the destination. For example, the route from source (S) to destination (D) pass through node A, and B so which routing path includes:

$$\mathbf{S \rightarrow A \rightarrow B \rightarrow D}$$

whereas $T(S)$, $T(A)_{REQ}$, $T(B)_{REQ}$, $T(D)_{REQ}$ is the time the node S, A, B, D forward R_{REQ} and $T(S)_{REP}$, $T(A)_{REP}$, $T(B)_{REP}$, T(D)REP is the time the node S, A, B, D forward REP. Then the RTT between S, A, B and D will be calculated based on equation as follows:

$$\mathbf{RTT_S = T(S)_{REP} - T(S)_{REQ}}$$

$$\mathbf{RTT_A = T(A)_{REP} - T(A)_{REQ}}$$

$$\mathbf{RTT_B = T(B)_{REP} - T(B)_{REQ}}$$

$$\mathbf{RTT_D = T(D)_{REP} - T(D)_{REQ}}$$

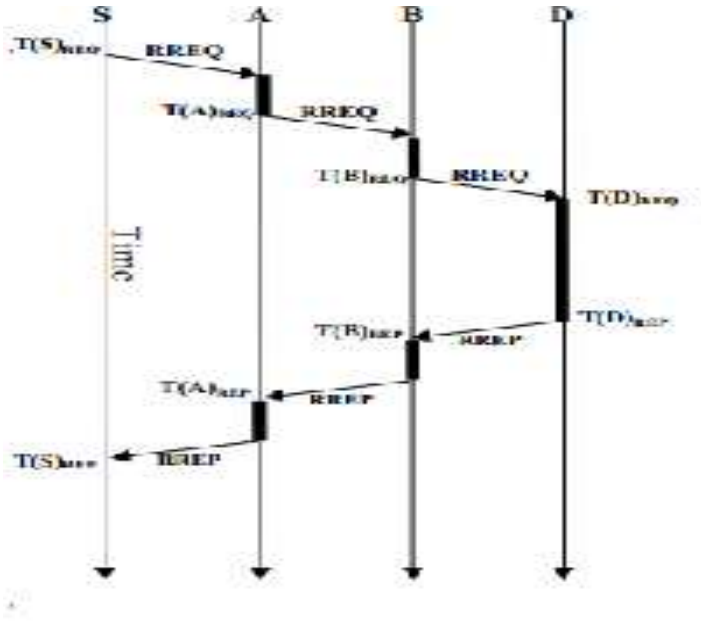
And the RTT values between two successive nodes along the path will be calculated based on equation :

$$\mathbf{RTT_{S,A} = RTT_S - RTT_A}$$

$$\mathbf{RTT_{A,B} = RTT_A - RTT_B}$$

$$\mathbf{RTT_{B,D} = RTT_B - RTT_D}$$

Under normal circumstances, $RTT_{S,A}$, $RTT_{A,B}$, $RTT_{B,D}$ are similar value in range. If there is a wormhole line between two nodes, the RTT value may considerably higher than other successive RTT values and suspected that there may be a wormhole link between these two nodes.



7. CONCLUSION

In this paper, we first proposed a novel and efficient worm hole detection based on RTT. While ensuring message sender privacy. RTT can be applied to any message to provide message content authenticity and then node compromised attack. To provide hop by hop message authentication without the weakness of the build in block hole attack. We proposed hop by hop message authentication scheme based on RTT. When applied to the wireless sensor network with fixed number of sink nodes, we also discussed in possible

techniques for compromised node identification. We compare our proposed scheme with MES scheme through simulation using NS-2 simulator. The simulation results show that our system has acceptable range of performance and applicability. Both theoretical and simulation result shows that, in comparable scenario, our proposed scheme is more efficient then the MES scheme in terms of computational overhead, energy consumption, message delay and memory consumption.

8. REFERENCES

[1] M. Albrecht, C. Gentry, S. Halevi, and J. Katz, "Attacking Cryptographic Schemes Based on 'Perturbation Polynomials'," Report 2009/098, http://eprint.iacr.org/, 2009.

[2] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-Secure Key Distribution for Dynamic Conferences," Proc. Advances in Cryptology (Crypto '92), pp. 471-486, Apr. 1992.

[3] D. Chaum, "The Dinning Cryptographer Problem: Unconditional Sender and Recipient Untraceability," J. Cryptology, vol. 1, no. 1, pp. 65-75, 1988.

[4]T.A. ElGamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," IEEE Trans. Information Theory, vol. IT-31, no. 4, pp. 469-472, July 1985.

[5] A. Perrig, R. Canetti, J. Tygar, and D. Song, "Efficient Authentication and Signing of Multicast Streams over Lossy Channels," Proc. IEEE Symp. Security and Privacy, May 2000.

[6] D. Pointcheval and J. Stern, "Security Proofs for Signature Schemes," Proc. Advances in Cryptology (EUROCRYPT), pp. 387- 398, 1996.

[7] A. Pfitzmann and M. Hansen, "Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management a Proposal for Terminology," http://dud.inf.tu-dresden.de/ literatur/Anon_Terminology_v0.31.pdf, Feb. 2008.

[8] [7] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Comm. ACM, vol. 21, no. 2, pp. 120-126, 1978.

[9] N. Song, L. Qian, and X. Li. Wormhole Attacks Detections in Wireless Ad Hoc Networks: A Statistical Analysis Approach. In Proceeding of the 19th International Parallel and Distributed Processing Symposium.

[10] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An Interleaved Hop-By- Hop Authentication Scheme for Filtering False Data in Sensor Networks," Proc. IEEE Symp. Security and Privacy, 2004.

[11] W. Zhang, N. Subramanian, and G. Wang, "Lightweight and Compromise-Resilient Message Authentication in Sensor Networks," Proc. IEEE INFOCOM, Apr. 2008.

International Journal of Computer Applications Technology and Research
Volume 3– Issue 11, 697 - 700, 2014

Stationary Computer Based Voting Process at Polling Booth

Vetrivel.D.S.B
Electronics and Communication Engineering,
PSNA College of Engineering and Technology
Dindigul, India

Niranjan Ravi
Electronics and Communication Engineering,
PSNA College of Engineering and Technology
Dindigul, India

Vishal Sundarrajan
Electronics and Communication Engineering,
PSNA College of Engineering and Technology
Dindigul, India

Abstract: System based voting is capable of saving considerable printing stationery and transport of large volumes of electoral material. It is easy to transport, store, and maintain. It completely rules out the chance of invalid votes. Its use results in reduction of polling time, resulting in fewer problems in electoral preparations, law and order, candidates' expenditure, etc. easy and accurate counting without any mischief at the counting centre. Though all these can be done by Electronic Voting Machine (EVMs), there are still some disadvantages that can be overcome by the use of computer providing the same level of security maintenance, distribution and sharing of votes in the polling booth. Since the computer can ease the addition process by processing it internally in CPU when executing the codes, it is also possible to extend the memory allocation and quick processing for the prompt publishing of results. Following the recent advancement in touch technology, it is possible for a voter to directly interact with the computer.

Keywords: EVMs, Database, VB.NET, Polling booth, LAN connected computers.

1. INTRODUCTION

EVMs in INDIA an Electronic Voting Machine consists of two Units – a Control Unit and a Balloting Unit – joined by a five-meter cable. The Control Unit is with the Presiding Officer or a Polling Officer and the Balloting Unit is placed inside the voting compartment. Instead of issuing a ballot paper, the Polling Officer in-charge of the Control Unit will press the Ballot Button. This will enable the voter to cast his vote by pressing the blue button on the Balloting Unit against the candidate and symbol of his choice. EVMs can record a maximum of 3840 votes. EVMs can cater to a maximum of 64 candidates. There is provision for 16 candidates in a Balloting Unit. If the total number of candidates exceeds 16, a second Balloting Unit can be linked parallel to the first Balloting Unit. Similarly, if the total number of candidates exceeds 32, a third Balloting Unit can be attached and if the total number of candidates exceeds 48, a fourth Balloting Unit can be attached to cater to a maximum of 64 candidates. In case the number of contesting candidates goes beyond 64 in any constituency, EVMs cannot be used in such a constituency.

The conventional method of voting by means of ballot box and ballot paper will have to be adopted in such a constituency. In case of miscreants, EVMs allow them to record five votes per minute. The normal rule is to count the votes polling station-wise and this is what is being done when EVM is used in each polling station. The mixing system of counting is done only in those constituencies specially notified by the Election Commission. Even in such cases, the result from each EVM can be fed into a Master Counting Machine in which case, only the total result of an Assembly Constituency will be known and not the result in each individual polling station. [1]

It is clear from the above that polling officer need to manually operate or pass it to the Master Counting Machine. This however is not required in case of computer as it is intrinsic in CPU and it does not allow any voter to record more than one vote at a time once the authentication is given to a particular voter by polling officer. The only disadvantage of computer voting system is the power consumption while other features are almost the same compared to the former.

Though there are other high level languages available for efficient programming, we have designed using VB.net, an object-oriented computer programming language that can be viewed as an evolution of the classic Visual Basic (VB), implemented on the .NET Framework. Microsoft currently supplies two main editions of IDEs for developing in Visual Basic: Microsoft Visual Studio 2012, with a backhand database maintained by MS Access.[2]

Two or more computers can be connected for parallel processing through LAN connection. New applications being developed are often designed so that they can transfer data securely across insecure networks. i.e. some type of authentication or encryption is built-in IP level encryption (for TCP/IP networks) offers a secure channel between two machines, even over insecure networks. [3]

2. RELATED WORKS

Democratic countries like India, US deploy electronic voting system. India uses EVMs (Electronic Voting Machines) as discussed in the introduction passage. Though it is highly secured the problems surrounding the voting machine can cause potential vulnerabilities. One demonstration attack was based on replacing the part inside the control unit that actually displays the candidates' vote totals. The study showed how a substitute, "dishonest" part could output fraudulent election results. This component can be programmed to steal a percentage of the votes in favor of a chosen candidate. The second demonstration attack used a small clip-on device to manipulate the vote storage memory inside the machine.

Votes stored in the EVM between the election and the public counting session can be changed by using a specially made pocket-sized device. When you open the machine, you find micro-controllers, under which are electrically enabled programs, with 'read-only' memory. It is used only for storage. However, you can read and write memory from an external interface. The researchers developed a small clip with a chip on the top to read votes inside the memory and manipulate the data by swapping the vote from one candidate to another. In

order to mitigate these threats, the researchers suggest moving to a voting system that provides greater transparency, such as paper ballots, precinct count optical scan, or a voter verified paper audit trail, since, in any of these systems, skeptical voters could, in principle, observe the physical counting process to gain confidence that the outcome is fair. [4] However, these problems can easily be eliminated by the use of Computer programming.

3. MODULES DESCRIPTION

3.1 Verification and Authentication

Here the authentication is provided by checking the details of the voter as it is already maintained in the database. The details must be valid for recording the vote for a particular Candidate.(In the current voting system, the details are verified by a human evaluator). Once the access is given for a voter by the polling officer he can vote only once for a particular candidate. Once the party has been chosen the window asks for confirmation. By confirming, the voter can be displayed a message 'Your vote has been Recorded'. Alternative signals like beep sound light can also be made possible by the use of proper coding.

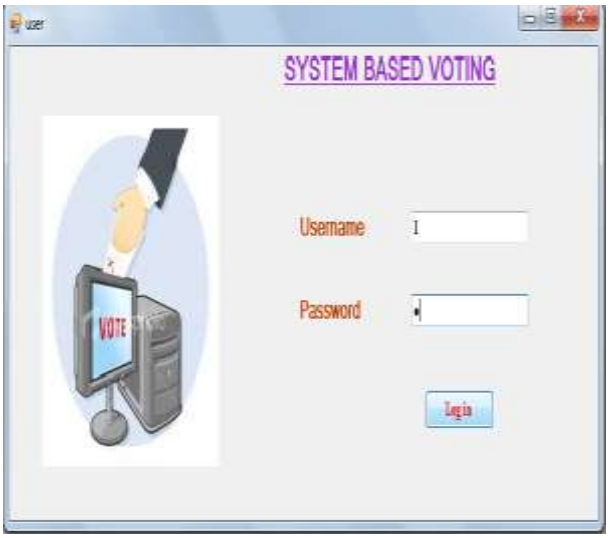


Figure. 1 Example of an Authentication form

3.2 Counting Process

The counting of votes can be done simultaneously when each voter record his/her vote. The window showed the symbol with the name of the party where the voter should select his/her candidate by the use of radio button before pressing the vote button to record their vote. By clicking on the vote button, the confirmation form will display 'YOU HAVE VOTED FOR …'.The voting is highly secured because no other peers or even the electoral officer can come to know whom a particular voter voted for. Since the counting is done real-time by computer the result can be unveiled immediately after the elections. This saves more time as it all happens inside a single electronic component, computer. No need to feed the accumulated data to Master EVMs. [7]

Figure. 2 Example of a Voting form

Figure. 3 Example of a Confirmation form

3.3 Database Maintenance

The database should store all the details of the voter. Efficient database software such as Big Data, MySQL, IBM DB2,ORACLE can be used for fast searching process. Public key fingerprint or digital verification can also help for the verification of details. This way of connecting to a DB provides a highly secured and there would be no chance of any miscreants.

3.4 Displaying Results

The result form is made to hide from the voter and candidature in the same way as giving authentication to a particular voter. Only the higher officials from the election commission should know the password and by the time of counting the corresponding password from each ward is typed to see the results. In the previous system, the button is sealed and total number of votes is calculated by pressing the 'Total' button.

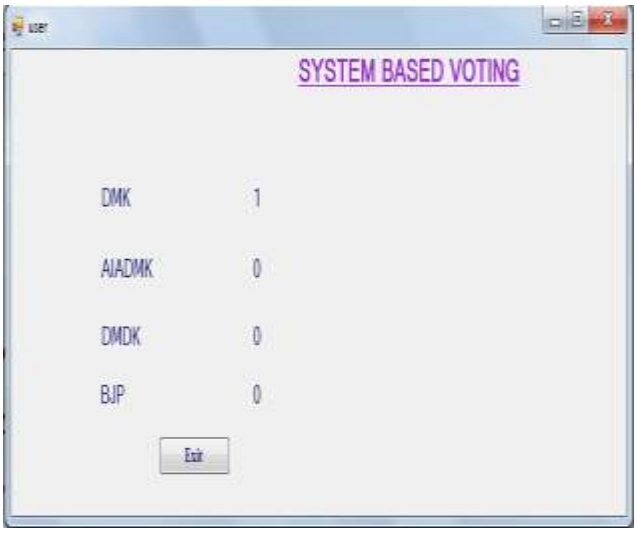


Figure. 4 Example of a Results form

4. PROPOSED ALGORITHM

4.1 Voting Process

1. The voter will be checked for their details.

2. After verification, the legal voter will be provided authentication to vote for his candidate.

3. The voter should select his/her candidate by choose radio button option and press on vote button.

4. A confirmation page will ask for confirmation. After confirming, his vote will be recorded.

5. The computer will once again ask for officer authentication for next voter and the process repeats.

4.2 Counting Process

1. Higher officials will be given credentials to access the form.

2. By typing the credentials, the results of election for each ward will be displayed. (It is also possible to calculate results in individual polling station)

5. ADVANTAGES

5.1 Vulnerability to hacking

If there is no external communications pathway, then there is no risk of hacking, or gaining unauthorized entry into the tabulation system. Since we are not dealing with any modem transfer it is practically impossible to hack the independent computer. [9]

5.2 Disabled Voters and Computer based Voting

Touchscreens are the only system which allows a voter with a disability to cast a secret and independent vote. The audio ballot and adaptive aids, such as sip and puff and jelly switches, make it possible for all of these citizens to cast a secret and independent ballot. [10]

5.3 Accuracy in Capturing Voters' Intent

The advantages of DRE systems include: no 'chad'; eliminating the possibility of an 'over vote' (or making more selections than permissible) and advising the voter of any 'under vote' (when a voter makes fewer than the maximum number of permissible selections in a contest).Because the confirmation page asks for the final decision the voter is less likely to make a mistake the second time.

5.4 Secure storage of cast votes

Concerns about security of the collection and counting process have always been important. Computers offer the first technology that can easily make copies of information in different forms for archival preservation. [11]

5.5 Malicious Software Programming

The concern that unscrupulous programmers will try to rig elections through deceptive software has led to specific processes and policies to avoid such an event. For example, software code passes through numerous internal and external checks before use in an actual election, including rigorous certification testing by independent certification bodies. Voting system software is engineered months in advance of actual elections, making it very unlikely for programmers to know who candidates will be and impossible to know how their names will appear on ballots. The source code is held in escrow by various state and federal officials, and local officials do not have access to it, thus preventing code changes at the local level.

5.6 Physical security of machines

Attempts to tamper with terminals, via privacy security screen removal and unlocking of bay doors, would be quickly noticed by the diligent, trained Election Judge and others in the polling place.

6. CONCLUSION

Doing such social projects should be favourable to people. Since the people who are not aware of the technology should be taught. In the above mentioned system there would be nothing other than selecting the candidate and confirmation button. Since the voting is being carried out in the polling booth there would be no chance of invading of hacker as each machine works independently providing its own backup. In

case of goes out of order, EVMs can be switched to be connected in parallel or replaced with spare EVMs. Another advantage is that it reduces the works of presiding officer in that particular polling booth because human beings are always prone to mistakes. The main confession of using this system is that it cannot be used in the places where there is no power supply. Since EVMs work on a 6V battery it is possible to use even in the places with no power connections. But Developing countries like India should consider such technology by looking at the future.

7. REFERENCES

[1] Bellis, M. (2011).The History of Voting Machines. www.about.com. Retrieved 25th October, 2011.

[2] Buchsbaum, T. (2004). "E-voting: International developments and lessons learnt". Proceedings of Electronic Voting in Europe Technology, Law, Politics and Society

[3] Friel, B., (2006) Let the Recounts Begin, National Journal Government Accountability Office (May 2004) "Electronic Voting Offers Opportunities and Presents Challenges" Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

[4] Rubin, A.D., (2002) "Security considerations for remote electronic voting", Communications of the ACM, 45(12): 39–44, December 2002.

[5] INDIAN VOTING MACHINES reference from Wikipedia http://en.wikipedia.org/wiki/Indian_voting_machine

[6] Daniel Barrett, Richard Silverman, Robert Byrnes – 2003 *books.google.co.in/books?isbn=0596003919*

[7] Official website of Election commission of India http://eci.nic.in/eci_main1/evm.aspx

[8] Visual Basic.Net:The Complete Reference by Shapiro-2002 *books.google.co.in/books?isbn=0070495114*

[9] *Dana DeBeauvoir Elections Administrator and County Clerk,TravisCounty,Texas "Prevention of Attack, Not Detection After the Fact," submitted as an appendix to testimony before the U.S. Election Assistance Commission may5,2004*

[10] JimDickson,Vice President, American Association of People with Disabilities. Testimony before the U.S. Election Assistance Commission may 5,2004

[11] TedSelker,PhDDirector, Caltech/MIT Voting Technology Project "Security Vulnerabilities and Problems with VVPT," Caltech/MIT Voting Technology Project Working Paper 13 Apr. 2004

International Journal of Computer Applications Technology and Research
Volume 3– Issue 11, 701 - 705, 2014

Image Morphing: A Literature Study

Harmandeep Singh
Sliet University
Sangrur, India

Amandeep Kumar
Sliet University
Sangrur, India

Gurpreet Singh
Punjabi University
Patiala, India

Abstract: Image morphing has been the subject of much attention in recent years. It has proven to be a powerful visual effects tool in film and television, depicting the fluid transformation of one digital image into another. This paper reviews the growth of this field and describes recent advances in image morphing in terms of three areas: feature specification, warp generation methods, and transition control. These areas relate to the ease of use and quality of results. We will describe the role of radial basis functions, thin plate splines, energy minimization, and multilevel free-form deformations in advancing the state-of-the-art in image morphing. A comparison of various techniques for morphing one digital image in to another is made. We will compare various morphing techniques such as Feature based image morphing, Mesh and Thin Plate Splines based image morphing based on different attributes such as Computational Time, Visual Quality of Morphs obtained and Complexity involved in Selection of features. We will demonstrate the pros and cons of various techniques so as to allow the user to make an informed decision to suit his particular needs. Recent work on a generalized framework for morphing among multiple images will be described.

Keywords: Morphing, feature extraction, warping, transition control, mesh-warping, thin plate splines.

1. INTRODUCTION

Morphing can be defined as an animated transformation of one image into another image. Morphing involves image processing techniques like warping and cross dissolving. Cross dissolving means that one image fades to another image using linear interpolation. This technique is visually poor because the features of both images are not aligned, and that will result in double exposure in misaligned regions. In order to overcome this problem, warping is used to align the two images before cross dissolving. Warping determines the way pixels from one image are correlated with corresponding pixels from the other image. It is needed to map the important pixels, else warping doesn't work. Moving other pixels is obtained by extrapolating the information specified for the control pixels. Knowing cross dissolving is very simple; the real problem of morphing becomes the warping technique. Morphing is actually a cross dissolving applied to warped images. Warping techniques vary in the way the mapping of control pixels is specified and the interpolating technique that is used for other pixels[5.6,7].

Morphing applications are very easy to find. Film makers from Hollywood use advanced morphing techniques to generate special effects. Even Disney animations are made using morphing, for speeding production. Because there are a small number of applications to generate face morphing, there is an increased interest in this domain.

2. MORPHING PRINCIPLE

Image morphing combines image warping with a method that controls the color transition in the intermediate images produced. To morph one image to another, new positions and color transition rates for the pixels in each of the images in the sequence must be calculated. Three processes are involved in this method

(i) Feature specification
(ii) Warp generation
(iii) Transition control

2.1 Feature Specification:

Feature specification is the most tedious aspect of morphing. Although the choice of allowable primitives may vary, all morphing approaches require careful attention to the precise placement of primitives. Given feature correspondence constraints between both images, a warp function over the whole image plane must be derived. This process, which we refer to as warp generation, is essentially an interpolation problem. Another interesting problem in image morphing is transition control. If transition rates are allowed to vary locally across in between images, more interesting animations are possible.

2.2 Warp Generation:

Warp generation is an algorithm that calculates and transforms the pixels in one image to new positions in the other image. Many algorithms have already been proposed to do warping. Once the pixels are in position, transition control blends in the colors between the two images. Transition control has also received a lot of attention. Originally, cross-dissolve was the color blending method of choice, but this method produced undesirable artifacts referred to as "ghosts".

2.3 Transition Control:

Transition control determines the rate of warping and color blending across the morph sequence. If transition rates differ from part to part in in between images, more interesting animations are possible. Such non uniform transition functions can dramatically improve the visual content.

3. IMAGE MORPHING TECHNIQUES

3.1 Cross Dissolve Morphing

Before the development of morphing, image transitions were generally achieved through the use of cross-dissolves, e.g., linear interpolation to fade from one image to another .Figure. 1 depicts this process applied over five frames. The result is poor, owing to the double-exposure effect apparent in misaligned regions. This problem is particularly apparent in the middle frame, where both input images contribute equally to the output. Morphing achieves a fluid transformation by incorporating warping to maintain geometric alignment throughout the cross-dissolve process.

Figure.-1 (a-f). Example of cross-dissolve morphing [4].

3.2 Mesh Warping

Mesh warping was pioneered at Industrial Light & Magic (ILM) by Douglas Smythe for use in the movie Willow in 1988. It has been successfully used in many subsequent motion pictures[1]. To illustrate the 2-pass mesh warping algorithm, consider the image sequence shown in Fig.-2. The five frames in the middle row represent a metamorphosis (or morph) between the two faces at both ends of the row[1]. We will refer to these two images as IS and IT, the source and the target images, respectively. ‘five source image has mesh MS associated with it that specifies the coordinates of control points, or landmarks. A second mesh, MT , specifies their corresponding positions in the target image. Meshes MS and MT are respectively shown overlaid on Is and IT in the upper left and lower right images of the figure. Notice that landmarks such as the eyes, nose, and lips lie below corresponding grid lines in both meshes. Together, MS and MT are used to define the spatial transformation that maps all points in IS onto IT. The meshes are constrained to be topologically equivalent, i.e., no folding or discontinuities are permitted. Therefore, the nodes in MT may wander as far from MS as necessary, as long as they do not cause self-intersection. Furthermore, for simplicity, the meshes are constrained to have frozen borders. All intermediate frames in the morph sequence are the product of a 4-step process:

For each frame f do
linearly interpolate mesh M, between MS and MT
warp IS to I I , using meshes MS and M
warp IT to 12, using meshes MT and M
linearly interpolate image I f , between I1 and I2
end

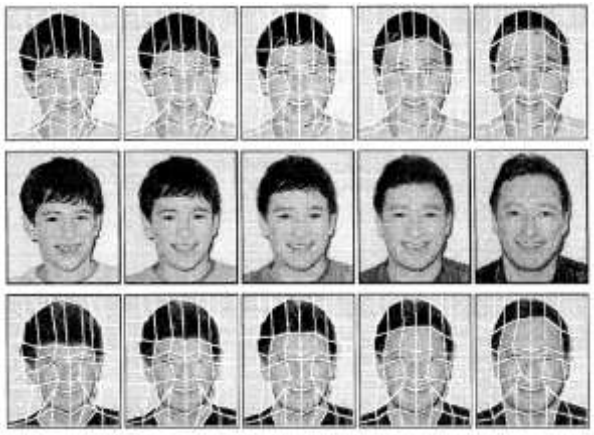


Figure.-2: Mesh warping[1]

Figure.-2 depicts this process. In the top row of the figure, mesh MS is shown deforming to mesh MT, producing an intermediate mesh M for each frame JF. Those meshes are used to warp IS into increasingly deformed images, thereby deforming IS from its original state to those defined by the intermediate meshes. The identical process is shown in reverse order in the: bottom row of the, figure, where IT is shown deforming from its original state. The purpose of this procedure is to maintain the alignment of landmarks between IS and IT as they both deform to some intermediate state, producing the pair of I1 and I2 images shown in the top and bottom rows, respectively. Only after this alignment is maintained does a cross-dissolve between successive pairs of I1 and 12 become meaningful, as shown in the morph sequence in the middle row. This sequeince was produced by applying the weights [l, .75, .5, .25,0] and [0, .25, .5, .75,1] to the five images in the top and bottom rows, respectively, and adding the two sets together. This process demonstrates that morphing is simply a cross-dissolve applied to warped imagery. The important role that warping plays here is readily apparent by (comparing the morph sequence in Figure.-2 with the cross-dissolve result in Figure.-1. The use of meshes for feature specification facilitates a straightforward solution for warp generation: bicubic spline interpolation.

3.3 Field Morphing

While meshes appear to be a convenient manner of specifying pairs of feature points, they are, however, sometimes cumbersome to use[1]. The field morphing algorithm developed by Beier and Neely at Pacific Data Images grew out of the desire to simplify the user interface to handle correspondence by means of line pairs. A pair of

corresponding lines in the source and target images defines a coordinate mapping between the two images. In addition to the straightforward correspondence provided for all points along the lines, the mapping of points in the vicinity of the line can be determined by their distance from the line. Since multiple line pairs are usually given, the displacement of a point in the source image is actually a weighted sum of the mappings due to each line pair, with the weights attributed to distance and line length. This approach has the benefit of being more expressive than mesh warping. For example, rather than requiring the correspondence points of Fig. 3 to all lie on a mesh, line pairs can be drawn along the mouth, nose, eyes, and cheeks of the source and target images. Therefore only key feature points need be given. Although this approach simplifies the specification of feature correspondence, it complicates warp generation. This is due to the fact that all line pairs must be considered before the mapping of each source point is known. This global algorithm is slower than mesh warping, which uses bicubic interpolation to determine the mapping of all points not lying on the mesh. A more serious difficulty, though, is that unexpected displacements may be generated after the influence of all line pairs are considered at a single point. Additional line pairs must sometimes be supplied to counter the ill-effects of a previous set. In the hands of talented animators, though, the mesh warping and field morphing algorithms have both been used to produce startling visual effects.

3.4 Radial Basis Functions / Thin Plate Splines

Thin-plate Spline is a conventional tool for surface interpolation over scattered data. It is an interpolation method that finds a *"minimally bended"* smooth surface that passes through all given points. The name "Thin Plate" comes from the fact that a TPS more or less simulates how a thin metal plate would behave if it was forced through the same control points. Let us denote the target function values *vi* at locations (*xi* , *yi*) in the plane, with i=1,2,…….p , where p is the number of feature points. In particular, we will set *vi* equal to the coordinates *(xi' , yi'*) in turn to obtain one continuous transformation for each coordinate. An assumption is made that the locations (*xi* , *yi*) are all different and are not collinear[3].

The Figure-3. is a simple example of coordinate transformation using TPS. It starts from two sets of points for which it is assumed that the correspondences are known (a). The TPS warping allows an alignment of the points and the bending of the grid shows the deformation needed to bring the two sets on top of each other (b). In the case of TPS applied to coordinate transformation we actually use two splines, one for the displacement in the x direction and one for the displacement in the y direction. The two resulting transformations are combined into a single mapping.

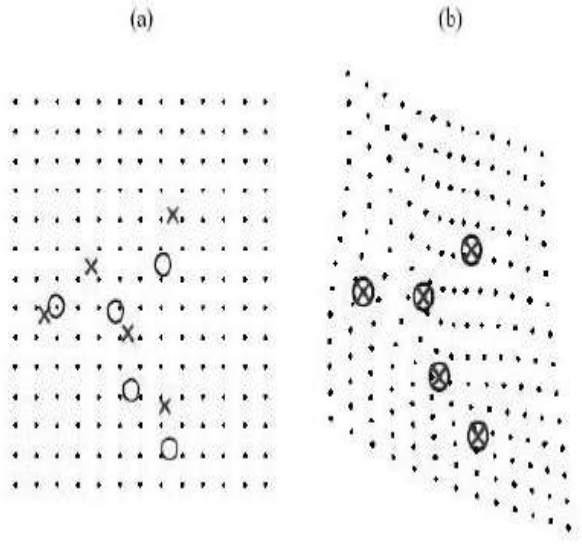


Figure-3: Example of coordinate transformation using TPS[4].

3.5 Energy Minimization

All of the methods described above do not guarantee the one-to-one property of the generated warp functions. When a warp is applied to an image, the one-to-one property prevents the warped image from folding back upon itself. An energy minimization method has been proposed for deriving one-to-one warp functions in. That method allowsm extensive feature specification primitives such as points, polylines, and curves. Internally, all primitives are sampled and reduced to a collection of points. These points are then used to generate a warp, interpreted as a 2D deformation of a rectangular plate. A deformation technique is provided to derive C'-continuous and one-to-one warps from the positional constraints. The requirements for a warp are represented by energy terms and satisfied by minimizing their sum[1]. The technique generates natural warps since it is based on physically meaningful energy terms. The performance of this method, however, is hampered by its high computational cost.

3.6 Multi-Level Free-Form Deformation

A new warp generation method was presented in this chapter that is much simpler and faster than the related energy minimization method [1]. Large performance gains are achieved by applying multilevel free-form deformation (MFFD) across a hierarchy of control lattices to generate one-to-one and C2-continuous warp function. In particular, warps were derived from positional constraints by introducing the MFFD as an extension to free-form-deformation. In that paper, the bivariate cubic B-spline tensor product was used to define the FFD function. **A** new direct manipulation technique for FFD, based on 2D B-spline approximation, was applied to a hierarchy of control lattices to exactly satisfy the positional constraints. To guarantee the one-to-one property of a warp, a sufficient condition for a cubic B-spline surface to be one-to-one was presented. The MFFD generates C2-continuous and one-to-one warps which yield fluid image distortions. The

MFFD algorithm was combined with the energy minimization method of in a hybrid approach. An example of MFFD-based morphing **is** given in Figure.-4**.**

Notice that the morph sequence shown in the middle row of the figure is virtually identical to that produced using mesh warping in Figure.-2. The benefit of this approach, however, is that feature specification is more expressive and less cumbersome. Rather then editing **a** mesh, a small set of feature primitives are specified. To further assist the user, snakes are introduced to reduce the burden of feature specification. Snakes are energy minimizing splines that move under the influence of image and constraint forces. They were first adopted in computer vision as an active contour model. Snakes streamline feature specification because primitives must only be positioned near the features. Image forces push snakes toward salient edges, thereby refining their final positions and making It possible to capture the exact position of a feature easily and precisely.

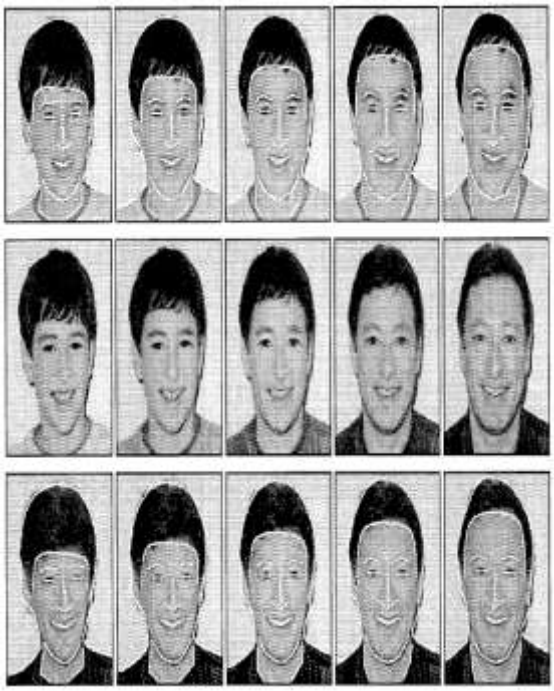


Figure-4. MFFD-based morphing[1]

4. COMPARISON

When we compared the three algorithms on a scale of computational speed, we found the Mesh Warping algorithm to be the best[2,8]. This results from the fact that the region is divided into a mesh and each mesh patch essentially has a local region of influence. Hence the computation is localized and independent, thus allowing for high level of parallelism. But a word of caution is in place. The computational advantage of the Mesh Warping algorithm is greatly offset by the huge amount of time overhead required to select mesh nodes all over the image. The main disadvantage of the Feature-based and Thin Plate Spline algorithms is speed. As the warping here is global the entire set of feature lines/control pixels that are specified need to be referenced for each pixel. As a result amount of time taken for each frame is proportional to the product of the number of pixels in the image and the number of control lines/pixels used. Table-1 gives the average warping time for each of our algorithms.

Table-1: Table showing the Comparison of different warping techniques[2]

Algorithm Name	**Computation Time**
Mesh Warping	0.15 s with a 10X10 mesh
Feature-based Warping	0.75 s with 11 feature lines
Thin Plate Spline Warping	0.45 s with 5 control points

Finally we wish to put in a word on the individual advantages and disadvantages of the three algorithms. The mesh warping algorithm requires that all four edges of the source and destination image be frozen. But this seemingly limiting constraint provides the mesh warping algorithm with its simplicity of implementation. The mesh warping algorithm also requires that the source and destination meshes be topologically equivalent i.e. no folding or discontinuities. This all adds to the problem of selecting mesh nodes spread through out the image. In case of the feature-based warping algorithm, sometimes unexpected and unwanted interpolations are generated due to some line combinations. Additional image processing efforts are required to fix these distortions and improve the quality of results.

5. FUTURE WORK

The traditional formulation for image morphing considers only two input images at a time, i.e., the source and target images. In that case, morphing among multiple images is understood to mean a series of transformations from one image to another. This limits any morphed image to take on the features and colors blended from just two input images.

Given the success of morphing using this paradigm, it is reasonable to consider the benefits possible from a blend of more than two images at a time. For instance, consider the generation of a facial image that is to have its eyes, ears, nose, and profile derived from four different input images. In this case, morphing among multiple images is understood to mean a seamless blend of several images at once. Despite the explosive growth of morphing in recent years, the subject of morphing among multiple images has been neglected.

In ongoing work conducted by the author and his colleagues, a general framework is being developed that extends the traditional image morphing paradigm applied to two images.

We formulate each input image to be a vertex of a regular convex polyhedron in (n - 1)-dimensional space, where n is the number of input images. An in between (morphed) image is considered to be a point in the convex polyhedron. The barycentric coordinates of that point determine the weights used to blend the input images into the In between image. Morphing among multiple images is ideally suited for image composition applications where elements are seamlessly blended from two or more images. A composite image is treated as a metamorphosis of selected regions in several input images. The regions seamlessly blend together with respect to geometry and color.

In future work, we will determine the extent to which the technique produces high quality composites with considerably less effort than conventional image composition techniques. In this regard, the technique can bring to image composition what image warping has brought to cross-dissolve in deriving morphing: a richer and more sophisticated class of visual effects that are achieved with intuitive and minimal user interaction.

Future work in morphing will also address the automation of morphing among limited classes of images and video sequences. Consider a limited, but common, class of images such as facial images. It should be possible to use computer vision techniques to automatically register features between two images. Model-based vision should be able to exploit knowledge about the relative position of these features and automatically locate them for feature specification. Currently, is is an active area of research, particularly for compression schemes designed for videoconference applications. The same automation applies to morphing among two video sequences, where time varying features must be tracked[9,10,11].

6. CONCLUSION

The focus of this article has been to survey various morphing algorithms and provide the animator with sufficient information to make an informed choice suiting his particular needs. In doing so we have defined a few easily comparable attributes, such as visual quality of morph, the ease with which the animator can select control pixels and the computational complexity. We found that Mesh morphing gives the best result among the algorithms we implemented but it requires a significant amount of animator effort in selecting the control pixels. The Thin Plate Spline gives results, which are of comparable quality with very little effort required from the animator. The Feature based morphing algorithm requires the animator to select a significantly larger number of feature lines to give the same results.

In summary, we feel that the Thin Plate Spline warping based Image Morphing algorithm is the best choice since it produces good quality results for lest animator effort. There are a variety of Image Morphing algorithms such as Image Morphing with snakes and free formed deformations, Image morphing using deformable surfaces, Image morphing using Delaunay triangulation and many others besides. Due to paucity of resources and time, we are unable to provide a comprehensive comparison of these algorithms.

7. REFERENCES

[1] George Wolberg, “Recent Advances in Image Morphing”, Department of Computer Science City College of New York / CUNY New York, NY 1003 1

[2] Prashant K. Oswal and Prashanth Y. Govindaraju, “Image Morphing: A Comparative Study”, Department of Electrical and Computer Engineering, Clemson University, Clemson

[3 Alexandru Vlad FECIORESCU, “Image Morphing Techniques”, JUNE 2010 ½ NUMBER 5 JIDEG

[4] Md. Tajmilur Rahman*, Al-Amin, M. A. Jobayer Bin Bakkre, Ahsan Raja Chowdhury† and Md. Al-Amin Bhuiyan¥, “A Novel Approach of Image Morphing Based on Pixel Transformation”. 1-4244-1551-9/07/$25.00 ©2007 IEEE.

[5] Mu-Chun Su and I-Chen Liu, “Facial Image Morphing by Self-organizing Feature Maps”, Department of Electrical Engineering, Tamkang University, Taiwan, R.O.C., 0-7803-5529-6/99/$10.00 01999 IEEE.

[6] Stephen Mullens and Simon Notley, “An Introduction to image morphing”, 2006.

[7] T. Beier and S. Neely, “Feature-bssed image metmoxpiiosis”, Compter Graphics (Proc. SIGGHAPH '92), 26(2):35-42, 1992.

[8] S.-Y Lee, K.-E: Chwa, **S.** Y Shin, and *G.* Wolberg. Image metamorphosis using snakes and free-form deformations. Computer Graphics (Proc.SIGGRAPH'95),pages 439-448, 1995.

[9] Mu-Chun Su and I-Chen Liu, “Facial Image Morphing by Self-organizing Feature Maps”, Department of Electrical Engineering, Tamkang University, Taiwan, R.O.C. 0-7803-5529-6/99/$10.00 01999 IEEE.

[10] Henry Johant Yuichi Koisot Tomoyuki Nishitat, “Morphing Using Curves and Shape Interpolation Techniques”, Dept. of Information Science, Dept. of Complexity Science and Engineering University of Tokyo, 0-7695-0868-5/0$01 0.00 0 2000 IEEE.

[11] Stephen Karungaru, Minoru Fukumi and Norio Akamatsu, “MORPHING FACE IMAGES USING AUTOMATICALLY SPECIFIED FEATURES”, University of Tokushima, 2-1 Minami Josamjima 770-8506, Tokushima, Japan., 0-7803-8294-3/04/$20.00 @2004 IEEE 741.

International Journal of Computer Applications Technology and Research
Volume 3– Issue 11, 706 - 710, 2014

Feature Selection Algorithm for Supervised and Semisupervised Clustering

S. Gunasekaran
Department of Computer Science and Engineering
V.S.B.Engineering College,
Karur, India

I. Vasudevan
Department of Computer Science and Engineering
V.S.B.Engineering College,
Karur, India

Abstract −In clustering process, semi-supervised learning is a tutorial of contrivance learning methods that make usage of both labeled and unlabeled data for training - characteristically a trifling quantity of labeled data with a great quantity of unlabeled data. Semi-supervised learning cascades in the middle of unsupervised learning (without any labeled training data) and supervised learning (with completely labeled training data). Feature selection encompasses pinpointing a subsection of the most beneficial features that yields well-suited results as the inventive entire set of features. A feature selection algorithm may be appraised from both the good organization and usefulness points of view. Although the good organization concerns the time necessary to discover a subsection of features, the usefulness is related to the excellence of the subsection of features. Traditional methodologies for clustering data are based on metric resemblances, i.e., non-negative, symmetric, and satisfying the triangle unfairness measures using graph-based algorithm to replace this process in this project using more recent approaches, like Affinity Propagation (AP) algorithm can take as input also general non metric similarities.

Keywords*:* Data mining, Feature selection, Feature clustering, Semi-supervised, Affinity propagation

1. INTRODUCTION

Clustering algorithms can be categorized based on their cluster model. The most appropriate clustering algorithm for a particular problem often needs to be chosen experimentally. It should be designed for one kind of models has no chance on a dataset that contains a radically different kind of models. For example, k-means cannot find non-convex clusters. Difference between classification and clustering are two common data mining techniques for finding hidden patterns in data. While the classification and clustering is often mentioned in the equal sniff, and dissimilar analytical approaches.

There is diversity of algorithms rummage-sale for clustering, but all the share belongings of

Iteratively assigning records to a cluster, manipulative a quantity and re-assigning records to clusters until the designed procedures don't modification much demonstrating that the process has converged to firm sections. Records within a cluster are more comparable to every one other, and added different from records that are in other clusters. Contingent on the precise implementation, there are a diversity of procedures of resemblance that are rummage-sale to over all aim is for the attitude to converge to collections of correlated records. Classification is a dissimilar method than clustering. Classification is correlated to clustering in that it also segments customer records into distinctive segments called classes. But dissimilar clustering, a classification inquiry requires that the end-user/analyst know ahead of time how classes are demarcated.

For instance, classes can be demarcated to represent the probability that a customer nonpayment on a loan (Yes/No). It is essential that every record in the dataset rummage-sale to physique the classifier before now have a value for the trait rummage-sale to describe classes. Because every record has a value for the trait rummage-sale to describe the classes, and because the end-user resolves on the trait to use, classification is much less investigative than clustering. The impartial of a classifier is not to search the data to ascertain interesting segments, but relatively to select how new records should be classified i.e. is this new customer likely to default on the loan?

With the aim of selecting a subsection of good features with high opinion to the impartial perceptions, feature subsection selection is a real way for reducing dimensionality, rejecting unrelated data, inflammation learning accurateness, and purifying result unambiguous. Feature subsection selection can be observed as the progression of ascertaining and confiscating as various unrelated and redundant features as possible. This is because 1) unrelated features do not subsidize to the extrapolation exactitude and 2) redundant features do not redound to receiving an enhanced analyst for that they deliver generally information which is previously contemporary in other feature(s). Unrelated features, beside with redundant features, strictly affect the exactness of the learning technologies.

Thus, feature subsection selection should be able to identify and remove as much of the unrelated and redundant information as possible. It develops a novel algorithm which can efficiently and effectively deal with both un related and redundant features, and obtain a good feature subsection. We achieve this through a new feature selection framework which composed of the two connected components of unrelated feature removal and redundant feature removal. The previous acquires features relevant to

the target concept by eliminating unrelated ones, and the latter removes redundant features from relevant ones via choosing denotative from different feature clusters, and thus produces the final subsection.

A fast clustering-based feature selection algorithm (FAST) works in two steps. In the first step, by using graph-theoretic clustering methods the features are separated into clusters. In the second step, the most typical feature that is powerfully associated to target classes is designated from every cluster to form a subsection of features. Features in different clusters are comparatively independent; the clustering-based approach of FAST has a high probability of producing a subsection of useful and sovereign features. To make sure the effectiveness of FAST, assume the well-organized minimum-spanning tree (MST) clustering method.

The unrelated feature removal is straightforward once the right relevance measure is demarcated or selected, while the redundant feature elimination is a bit of refined. In the FAST algorithm, it encompasses 1) the structure of the minimum spanning tree from a weighted complete graph; 2) the partitioning of the MST into a forest with every tree denoting a cluster; and 3) the selection of denotative features from the clusters. Feature selection encompasses detecting a subsection of the most useful features that produces compatible results as the original entire set of features.

2. RELATED WORK

The proposed method [2] provides the number of features in numerous applications where data has hundreds or thousands of features. Existing feature selection approaches predominantly focus on verdict relevant features. In this feature selection display that feature relevance alone is inadequate for well-organized feature selection of high-dimensional data. We define feature redundancy and propose to perform explicit redundancy analysis in feature selection. A new framework is introduced that decouples relevance analysis and redundancy analysis. We develop a correlation-based method for relevance and redundancy analysis, and conduct an empirical study of its efficiency and effectiveness comparing with representative methods.

The novel algorithm for discovery non-redundant discarded feature subsections based on the PRBF[5]has only one consideration, numerical meaning or the likelihood that the assumption that disseminations of two features are comparable is true. In the first step directories have been rummage-sale for ranking, and in the second step terminated features are detached in an unsupervised way, because during decrease of terminated features data about the modules is not used.

The primary tests are promising: on the reproduction data perfect ranking has been re-formed and terminated features rejected, while on the real data, with relatively modest number of features selected outcomes are regularly the superlative, or close to the superlative, associating with four state-of-the-art feature selection algorithms. The novel algorithm appears to work especially well with the direct SVM classifier. Computational anxieties of PRBF algorithm are related to other correlation-based filters, and lower than Relief.

The searching for interacting features in subsection selection [9] developing and acclimatizing abilities of robust intellect are superlative established in its aptitude to learn. Mechanism learning facilitates computer systems to learn, and recover presentation. Feature selection facilitates mechanism learning by targeting to eliminate irrelevant features .Feature interaction presents a dare to feature subsection selection for cataloging. This is because a feature by itself might have little relationship with the objective concept, but when it is combined with some other features, it can be strongly interrelated with the objective concept.

Thus, the in advertent elimination of these features may effect in poor cataloging presentation. It is computationally inflexible to switch feature exchanges in general. Nevertheless, the attendance of feature interaction in an extensive range of real-world requests demands applied solutions that can decrease high-dimensional data although perpetuating feature exchanges. In this paper, it ups the contest to design a special data structure for feature quality evaluation, and to employ an information-theoretic feature ranking mechanism to efficiently handle feature interaction in subset selection.

We conduct experiments to evaluate our approach by comparing with some representative methods, perform a lesion study to examine the critical components of the proposed algorithm to gain insights, and investigate related issues such as data structure, ranking, time complexity, and scalability in search of interacting features.

The success of many feature selection algorithms allows us to tackle challenging real-world problems. Many applications inherently demand the selection of interacting features.

An Evaluation on feature selection for text clustering is first demonstrated that feature selection can improve the text clustering efficiency and performance in ideal case, in which features are selected based on class information. But in real case the class information is unknown, so only unsupervised feature selection can be exploited. In many cases, unsupervised feature selection are much worse than supervised feature selection, not only less terms they can remove, but also much worse clustering performance they yield.

3. PROPOSED SYSTEM

Traditional approaches for clustering data are based on metric resemblances, i.e., nonnegative, symmetric and filling the triangle disparity measures. More recent approaches, like Affinity Propagation (AP) algorithm can take as input also general non metric similarities. AP can use as input metric selected segments of images' pairs. Accordingly, AP has been rummage-sale to solve a wide

range of clustering problems, such as image processing tasks gene detection tasks, and individual preferences predictions.

Affinity Propagation is derived as an application of the max-sum algorithm in issue graph; it is used to explorations for the smallest amount of dynamism function on the basis of message passing between data points. In this system implements the semi supervised learning has taken a great deal of considerations. It is a mechanism learning paradigm in which the model is constructed using both labeled and unlabeled data for training set.

It retrieve the data from training data or labeled data and extract the feature of the data and compare with labeled data and unlabeled data .In clustering process, semi-supervised learning is a class of machine learning techniques that make use of both labeled and unlabeled data for training - typically a small amount of labeled data with a large amount of unlabeled data.

Semi-supervised learning cascades among unsupervised learning (without any labeled training data) and supervised learning. Various mechanism-learning investigators have found that unlabeled data, when rummage-sale in conjunction with a small amount of categorized data, can yield substantial development in learning accuracy.

3.1 Irrelevant Based Feature Selection

A feature selection algorithm may be appraised from together the proficiency and usefulness point of view. Although the effectiveness concerns the time requisite to find a subsection of features, the efficiency is associated to the excellence of the subsection of features.

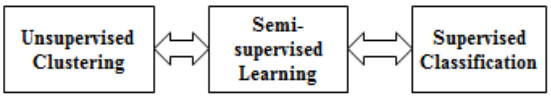


Fig 1: Semi-Supervised Learning

Many feature subsection selection algorithms, some can successfully remove irrelevant features but fail to handle redundant features yet some of the others can eliminate the irrelevant while taking care of the redundant features. In this system the FAST algorithm cascades into the subsequent group. The previous obtains features pertinent to the target concept by eliminating unrelated ones, and then removes redundant features from pertinent ones via choosing denotative from different feature clusters.

3.2 Redundant Based Feature Selection

The hybrid methods are combination of filter and wrapper methods by using a filter method to reduce search space that will be considered by the succeeding wrapper. It focuses on coalescing filter and wrapper approaches to achieve the best possible performance with a particular learning algorithm with similar time complexity of the filter methods. Redundant features do not redound to getting a better predictor for that they provide mostly information which is already present in other feature(s).

3.3 Graph Based Cluster

An algorithm to systematically add instance-level constraints to the graph based clustering algorithm. Unlike other algorithms which use a given static modeling parameters to find clusters, Graph based cluster algorithm finds clusters by dynamic modeling. Graph based cluster algorithm uses both Closeness and interconnectivity while identifying the most similar pair of clusters to be merged.

3.4 Affinity Propagation Algorithm

The affinity propagation (AP) is a clustering algorithm established on the notion of "message passing" among data points. For example of clustering algorithm is k-means. It does not need the quantity of clusters to be determined or estimated before running the algorithm.

Let x_1 and x be a set of data points, with no expectations ready around their internal structure, and the function that measures the resemblance among any two points, that is $s(x_i, x) > s(x_i, x)$ if x is further related to x_i than x.

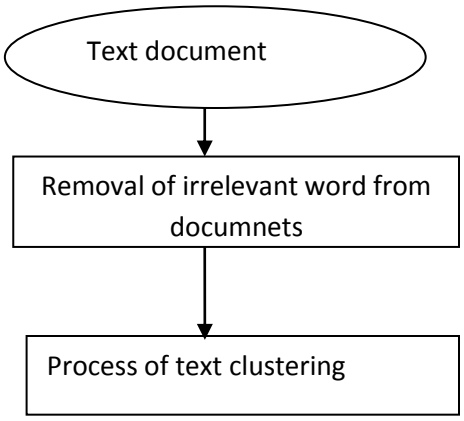


Fig 2: Process of clustering

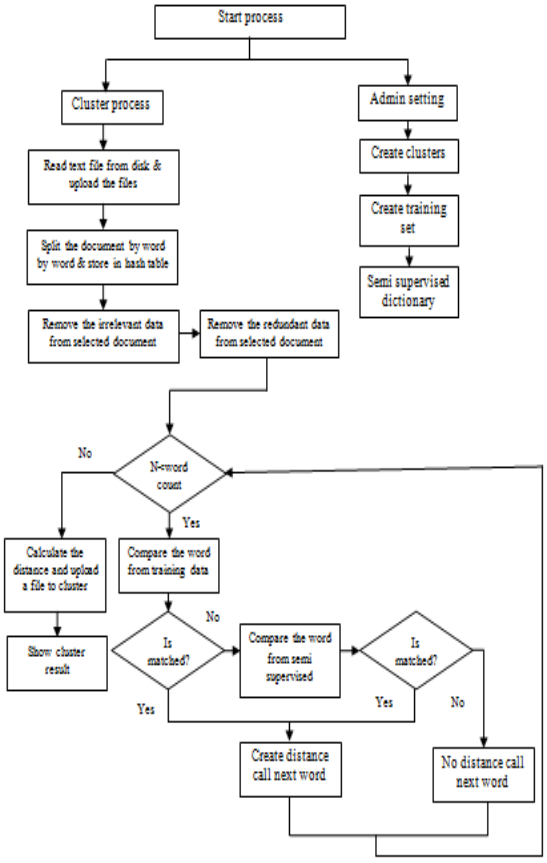


Fig 3: system flow diagram for proposed system

The algorithm ensues by flashing two message passing steps, it modernize by using the subsequent two conditions:

- The "responsibility" conditions *R* has values *r*(j, n) that measure how well-matched *x* is to aid as the exemplar for *x*, comparative to other candidate exemplars for *x*.
- The "availability" conditions *A* contains values *a*(j, n) characterizes how "applicable" it would be for *x* to pick *x* as its exemplar, taking into interpretation other points' favorite for *x* as an exemplar.

Together conditions are reset to all zeroes, and can be regarded as probability counters. The following updates are iteratively used to perform the algorithm:

First, responsibility updates are sent around:

$$r(j,n) \leftarrow s(j,n) - \max_{n' \neq n}\{a(j,n') + s(j,n')\}$$

Then, availability is updated per

$$a(j,n) \leftarrow \min\left(0, r(n,n) + \sum_{j' \in \{j,n\}} \max(0, r(j',n))\right)$$

$$for\ ^{j \neq n}\ and$$

$$a(n,n) \leftarrow \sum_{j' \neq n} max(0, r(j',n))$$

4. EXPERIMENTAL RESULTS

The performance of the proposed algorithm is compared with the two well-known feature selection algorithms FCBF and CFS of text data from the aspects of the proportion of selected features and runtime analysis.

TABLE 1 Runtime (in ms) of the Feature Selection Algorithms

Data set	FAST (Affinity Propagation)	FAST (Graph Based)	FCBF	CFS
Chess	90.1	94.02	94.02	90.43
Elephant	95.35	98.09	99.94	99.97
Wap.wc	69.01	71.25	75.74	77.8
Colon	87.4	90.45	90.76	89.14
GCM	55.69	58.73	59.16	60.92
AR10P	74.05	77.69	75.54	79.54
B-cell1	79.21	81.01	82.94	87.33

The affinity propagation algorithm is used to reduce the runtime compare with the graph based algorithm of FAST. It reduces the error and simplicity of performance. The semi-supervised learning is a tutorial of contrivance learning methods that make usage of both labeled and unlabeled data for training - characteristically a trifling quantity of labeled data with a great quantity of unlabeled data.

It is used to improve the efficiency of feature selection of FAST algorithm. Affinity propagation algorithm is used to achieve good performance of processing time. It provides better results with less amount of time compare with graph based algorithm.

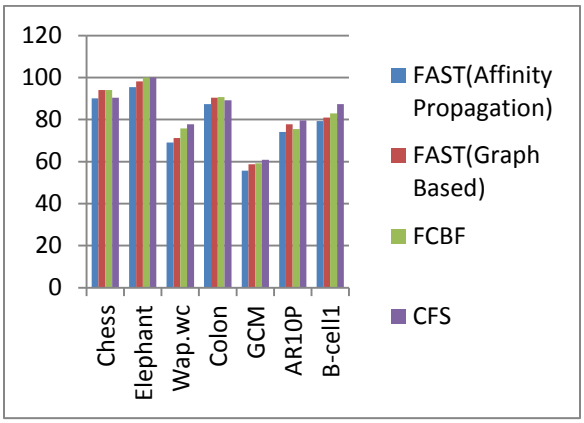


Fig 3: Runtime (in ms) of the Feature Selection Algorithms

5. CONCLUSION

In this paper, the semi supervised learning retrieve the data from training data or labeled data and extracts the feature of the data and compare with labeled data and unlabeled data. Feature selection encompasses pinpointing a subsection of the most beneficial features that yields well-suited results as the inventive entire set of features. A feature selection algorithm may be appraised from both the good organization and usefulness points of view. Then we use Affinity propagation algorithm for low error, high speed, flexible, and remarkably simple clustering algorithm that may be rummage-sale in forming teams of participants for business simulations and experiential exercises, and in organizing participants' preferences for the parameters of simulations.

5. REFERENCES

[1] Qinbao Song, Jingjie Ni, and Guangtao Wang, "A Fast Clustering-Based Feature Subset Selection Algorithm for High-Dimensional Data"*IEEE Transactions on knowledge and data engineering* vol. 25, no. 1, January 2013.

[2]L. Yu and H. Liu, "Efficient Feature Selection via Analysis ofRelevance and Redundancy," *J. Machine Learning Research*, vol. 10,no. 5, pp. 1205-1224, 2004.

[3]C.Sha, X.Qiu, and A.Zhou, "Feature Selection Based on a NewDependency Measure," *Proc. Fifth Int'l Conf. Fuzzy Systems and KnowledgeDiscovery*, vol.1,2008..

[4] I.S.Dhillon, S.Mallela, and R.Kumar, "A Divisive Information Theoretic Feature Clustering Algorithm for Text Classification,"*Machine Learning Research*, vol. 3, 2003.

[5] J.Biesiada and W.Duch, "Features selection for High-Dimensional data a Pearson Redundancy Based Filter," *Advances in Soft Computing*, vol. 45, 2008.

[6] P.Chanda, Y.Cho, A.Zhang, and M.Ramanathan, "Mining of Trait Interactions Using Information Theoretic Metrics," *Proc. IEEE Int'l Conf. Data Mining Workshops*, 2009.

[7] S.Chikhi and S.Benhammada, "ReliefMSS: A Variation on a Feature Ranking Relief Algorithm," *Int'l J. Business Intelligence and Data Mining*, vol. 4, nos. 3/4, 2009.

[8] S.Garcia and F.Herrera, "An Extension on Statistical Comparisonsof Classifiers over Multiple Data Sets for All PairwiseComparisons," *J. Machine Learning Res.*, vol. 9, 2008.

[9] Z.Zhao and H.Liu, "Searching for Interacting Features in Subset Selection," *J. Intelligent Data Analysis*, vol. 13, no. 2, 2009.

[10] Z. Zhao and H. Liu, "Searching for Interacting Features," Proc.20th Int'l Joint Conf. *Artificial Intelligence*, 2007.

International Journal of Computer Applications Technology and Research
Volume 3– Issue 11, 711 - 717, 2014

Rule Based Automatic Generation of Query Terms for SMS Based Retrieval Systems

Aarti Kumar
Department of Computer Applications
Maulana Azad National Institute of Technology
Bhopal, India

Sujoy Das
Department of Mathematics and Computer Applications,
Maulana Azad National Institute of Technology
Bhopal, India

Abstract : Every big and small need is fulfilled through the small hand held device called mobile. But matching the text standard of a mobile having limited space and of users' varying moods or limited capacity and knowledge, makes it difficult to comprehend what the user is actually seeking when it comes to processing strings sent through SMS text. This paper presents an overview of how strings sent through SMS can be processed in the simplest possible way and how they can be then used for matching best possible word from a standardized collection. In this paper we have presented an entirely different approach to handle the noise in the queries and have tried to bring forth a Rule Based Approach for automatic generation of query terms which converts a syntactically incorrect query to a semantically fruitful one.

Keywords: Domain dictionary; Synonym dictionary; phonetic replacement; rule based

1. INTRODUCTION

The advent of mobiles with all facilities like net connection, mobile banking, Bluetooth and wi-fi has brought the whole world into the palm of our hands. Every big and small need is fulfilled through this small hand held device. Blogs, Twitter, socializing sites and SMS are the most common approach now-a-days for all kinds of communication. These have limited space to convey a message. But all these are being used not only to communicate but also to seek information from various sources to help decision making. These sources, which are generally some organizations, government agencies or educational institutions, receive such strings and try to answer the query sent through any of such information seekers. Mostly when it comes to SMS text, the user behavior is not consistent and how they will frame their SMS depends solely upon their, attitude, mood, age and nature. In general it has been observed that the younger generation has started using somewhat cryptic text for sending their messages and communicating. The words that they use are non-standard and are not found in any of the standard dictionaries. But at the same time the users within themselves are very comfortable with that and comprehend such kind of text very well. Problem arises when the same has to be understood and analyzed by an online system which relies only on a standard dictionary and refuses to recognize such words or texts. These systems expect the query in a proper standard language format. The challenge is to process such deformed strings, find out meanings from such words which otherwise grammatically appear meaningless, match them with the original query and supply the answer. This involves a lot of steps and lots of calculations.

The approaches that are generally adopted to handle such queries are either cognitive which exploits the human brains to answer questions or they simply use the principles of Natural language processing or else they are IR based which treats the question-answering as a problem of Information Retrieval and employs various rules to search the corpora of text and find the correct match to help answer the question in the best possible manner.
In this paper we have tried to bring forth a Rule Based Approach for automatic generation of query terms. This approach for finding the best question answer pair for a given query, from a list of FAQs, is easy to understand, handles the noisy SMSs efficiently and is simple to incorporate.

The rest of the paper is structured as follows: In Section 2 work done by different authors on SMS based FAQ retrieval are discussed. Section 3 discusses the proposed approach. Section 4 and 5 discuss the experiment performed and the observations respectively. Section 6 discusses the intricacies involved and the rules formulated and finally Section 7 presents conclusion.

2. RELATED WORK

Aw et al., 2006[14, Choudhury et al., 2007[15] and Kobus et al., 2008[13] have worked towards removing noise from SMS. An aligned SMS corpus and conventional language is required for training by the techniques employed by them. As reported by [4], Acharya et al., 2008 worked towards mapping non-standard words to their corresponding conformist recurrent form through an unsupervised technique. The algorithm proposed by Govind Kothari et al.[4] takes care of the noise in a SMS query by formulating query similarity over FAQ questions along with handling semantic variations in question formulation. As his approach considers it as a combinatorial search problem, therefore, the search space consists of combinations of all possible dictionary variations of tokens in the SMS query.

Deirdre Hogan et al.[5] presented a paper on SMS based FAQ retrieval in FIRE 2011. Their approach consists of first transforming the noisy SMS queries into a normalized, corrected form. The combined results of three different retrieval mechanisms are then used to retrieve a ranked list of FAQ results from the normalized

queries. The information gathered from retrieval results are then used for classifying and tagging out-of-domain (OOD) queries.
V. M. Pathak and M. R. Joshi[6] have worked on Marathi language and showed their results for Marathi language retrieval using SMS based query. They have used Vector space model and Cosine Similarity on ITRANS Marathi Literature documents to rank the documents as per their relevance for each selected query.

Paul Cook and Suzanne Stevenson in their work An Unsupervised Model for Text Message Normalization [7] have also given an unsupervised noisy-channel model for normalization of SMS text with 59% accuracy

Deana L. Pennell and Yang Liu [8] have given a system for normalizing text for Text-To-Speech engine. A classifier is used to form rules and to transform standard text to texting abbreviations. A reversal of the mappings gives the English words from these abbreviations. The intervention of human annotators is needed for the task of abbreviating.

Fei Liu et al.[9] have proposed a unified letter transformation approach where human supervision and pre-categorization of non standard words are not required. Nonstandard tokens under a sequence labeling framework have been generated from the dictionary words performed character-level alignment on a large set of noisy training pairs. They have reported absolute accuracy gain of 21.69% over deletion-based abbreviation system and of 18.16% over jazzy spell checker

3.PROPOSED APPROACH

Most the work that has been done towards processing such strings focuses on the SMS queries that are received and tries to solve the problem by processing these noisy queries using various methods and by adopting complicated processes. This involves quite a lot number of steps to solve a problem. But based on the fact that the number of SMSs received by any organization is, in majority of cases, manifolds the number of questions in the FAQ corpora, if instead of trying to mould the new generation language into standard language, it would be simpler if we do something which adapts to this language and moulds the standard language to harmonize with the current language in trend.

Although the works done by Deana L. Pennell and Yang Liu[8] and Fei Liu et al.[9] use the similar concept of processing the dictionary terms, but the work done in [8] requires human intervention, does not deal with substitutions of text which is very frequently seen in SMS text, does not deal with synonyms and is basically an interpretation of text only for text to speech conversion and for query formulation.

Again the proposed system by Fei Liu et al. [9] is very complicated involving many steps and complex calculations.

The proposed work is a step towards the same and uses very simple but efficient procedure to solve the problem. No human intervention is involved in normalizing the text and no complex procedures have been used. The idea is that instead of processing the umpteen numbers of SMSs received, process the terms of the standard query, which is limited in number, to match the terms of SMSs text. Through this approach it will be less time consuming, less intricate and easier to resolve the queries and will also require lesser number of steps.

4. EXPERIMENT AND ANALYSIS

To come out with the rules and verify it an experiment was conducted on three batches of MCA students with 90 students per batch of our institute and on a group of middle aged people of officers club. They all were given to write on a piece of paper any message of their choice that they would like to send their family and friends keeping in mind the restriction of 150 characters imposed by mobile SMS service. They were asked to write it in the way they would write it in an SMS. Not restricting them to a domain made it easy for us to get SMS terms on a variety of topic and helped us in forming the rules. Further data was collected from comments of Face Book.

After forming the rule we applied the rules on dataset provided to us by FIRE 2012 for SMS based FAQ retrieval. The dataset consisted FAQs in three languages – English, Hindi and Malyalam that were collected from online sites - both government and private. They included domains like Railway Enquiry, Telecom, Health and Banking .The SMSs for FIRE were generated by asking college students to write down their information need using a mobile phone. We used the English dataset of 999 KB of SMSs for our study to generate the original FAQs and to retrieve the answer. 610 SMS terms of FIRE were also analyzed. Table 1 and Figure 1 show the analysis of rules incorporated in SMSs of FIRE 2012 English SMS dataset.

Windows was the platform used for testing algorithm. Java (jdk1.7.0_07) was used to implement the algorithm through program and test the results for original FAQs. Rule numbers 5.1 to 5.6 were incorporated in the programs to generate terms and to retrieve the queries to get the results. The testing is still in progress and is giving convincing results.

Table 1. Analysis of rules incorporated in SMSs of FIRE 2012 English SMS dataset

Rule Applied	No. of instances	Percentage out of 610 words
Acronym	27	4.43
Repeating letter dropped	1	0.16
H following w dropped	5	0.82
Digit replacement	4	0.66
Vowels completely dropped	154	25.25
Partial dropping of vowel	171	28.03
First few letters to represent word	40	6.56
Combination of rules	51	8.36
Last g dropped	2	0.33
Stylistic variation	70	11.48
Phonetic replacement of word	10	1.64
Phonetic replacement of substring	19	3.12
Repeating letter dropped	7	1.15
Spelling mistake	39	6.39
Complete standard words	10	1.64

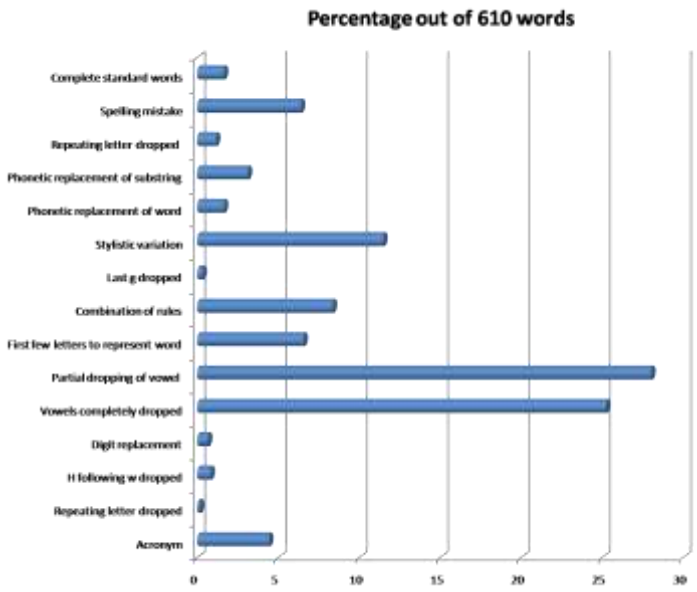


Figure 1: Graph showing percentagewise analysis of Rules incorporated in SMSs of FIRE 2012 English SMS dataset

5. OBSERVATIONS

After going through many SMSs it was observed that although the users are of varied backgrounds, behaviors, likings, moods and many a times also unsure of spellings and sentence formations, yet they are aware of one thing and that is phonetics and limited space. They try to convey their message with their full meanings to the ones they wish to communicate. For this they have to distort, shorten the words and use phonetic or digit substitutions more often. Still there are some general rules that are followed while creating SMSs. Eight such rules have been recognized which are as follows:

5.1 Omitting Vowels Partially or Retaining Vowels Partially (Generally the First or the Last Vowel)

If space allows, and the standard words contain more than one vowel, then only the first vowel from the words is removed to write the SMS term. Table 2 shows some common SMS terms conforming to this rule.

Table 2. SMS terms created by partially retaining or omitting vowels

SMS text	Standard word	SMS text	Standard word
ntion	nation	evaluation	valuation
bettr	better	xpect	expect
unending	nending	gmes	games
inactive	nactive	alwys	always
bke	bike	anarchy	narchy
latr	later	lbow	elbow

5.2 Omitting Vowels Completely

The SMS term is actually the consonant frame which is obtained by removing all the vowels from the standard term (Table 3).

Table 3. SMS terms created by fully omitting vowels

SMS text	Standard word	SMS text	Standard word
plc	place	wrst	wrist
strng	Stong, string	frm	from
fr	for	strtd	started
f	of	wht	what
bst	best	wrld	world
I	eye	cn	can
u	you	X	axe
whr	where	bt	But, bet
cn	can	nt	Not, net
fnd	find	rqts	raquets
hw	how	whch	which
s	is	rsdnt	resident
p	Pea	R	are
m	am	knw	Know, knew
srv	serve	gt	Get, got
srvc	service	B	Bee, be
wrn	warn	t	Tea, tee
thnk	thank		

5.3 Omitting Consecutive Repeated Alphabets

As per this rule, the letters appearing more than once in succession, are removed from the standard term to get the SMS term (Table 4)

Table 4. SMS terms created by omitting consecutive repeated alphabets

SMS text	Standard word	SMS text
Tenis	tennis	committee
comite	running	runing

5.4 Dropping Last 'g', Last 't', Last 'e' and also Dropping 'h' Associated with 'i' and 'w'

In most cases the last 'g' and't' are dropped if that does not affect the meaning of the word. The 'h' which follows 'w' or precedes 'i' is also dropped to form the SMS term. Table 5 shows some examples of SMS terms which are created in this manner.

Table 5. SMS terms created by 'g', last 't', last 'e' and also dropping 'h' associated with 'i' and 'w'

SMS	Standard	SMS	Standard

text	word	text	word
carin	caring	goin	going
jus	just	wat	what
usn	using	wch	which
comin	coming	wite	white
warin	wearing	hav	have

5.5 Representing Words by Digits, Single Alphabets or Combination of Alphabets

One or more alphabets, digits, special characters or symbols are used to create a full word with the same phonetics (Table 6).

Table 6. SMS terms created by representing words by digits, symbols, single alphabets or combination of alphabets

SMS text	Standard word	SMS text	Standard word
a	Answer,	n	An, and
b	Be, bee	o	Owe,oh, ough(tho)
c	See, sea,she	q	Queue, question
d	the	u	you
i	Eye	v	we
mt	empty	ne	any
y	why	5	five
1	one	6	Six
2	To, two, too	7	Seven
3	Three	8	Eight
4	For,four	9	nine
10	ten	+	plus
&	and	ur	your
@	at		

5.6 Using Alphabets, Symbols and Digits to Replace Substring Character, Substring Bi-gram, Substring Trigram and Substring Quad-gram Instead of the Whole Word

This rule is like the previous rule but instead of replacing the whole standard word, its substring is replaced. The single character, bigrams, trigrams and quad grams which are part of a string(standard word) and sound like single alphabets, symbols and digits, are replaced by the corresponding alphabet, symbol and digit to get the SMS term (Table 7).

Table 7. SMS terms created by replacing Substring character, substring Bi-gram, substring Trigram and substring quad-gram by alphabets, symbols and digits

Substring	Single Alphabet/ symbol/digit	Examples
si	c	cmple
di, th,de	d	dat, der, d@, dtel, d,dm,dem
gee, gi	g	
ck	k	quik
oh,ow	o	ro, o
et, eat, eight	8	gr8, p8, 8y,
ks	X(thanx)	
que(st)	q	qst
oo,o	u	u, gud, cum
wee	v	vd,vp
whi	y	yl
se, s, st,is	z	uz, juz, balz,whatz
ine,in,line	9	f9, f9d, on9(online)
an	n	ny
and	&	gr&, b&,br&
at	@	h@, w@
one, on	1	1s,1c, 1ce,up1
to,	2	2maro
fore	4	b4, der4
ha	a	av

5.7 Represent words using combination of the above rules

The same person at different time can frame the same word in a different form. This mood based generation of words generally applies the combination of two or more of the above mentioned rules. This variation may also depend upon the age of the users. Table 8-13show some examples of SMS created combining more than one rule.

Table 8. SMS words created using rule A and F

SMS text	Standard words	Explanation
Wrstb&	wristband	1. Partial vowel dropped 2. 'and' replaced by symbol '&'
B4	before	1. Vowels dropped 2. 'fore' represented by '4'

Table 9. SMS words created using rules B and D

SMS text	Standard words	Explanation
wch	which	1. Vowel dropped 2. 'h' associated with 'i' dropped
wt	what	1. Vowel dropped 2. 'h' following 'w' dropped

Table 10. SMS words created using rules B and F

SMS text	Standard words	Explanation
frndz	friends	1. Omitting vowels 2. Replacing 's' with 'z'
plz	please	1. Vowel removed 2. 's' replaced by 'z'

Table 11. SMS words created using rules B and C & also rules C and F

SMS text	Standard words	Explanation
clg	college	1. Dropping vowels 2. Dropping repeated 'i'
balz	balls	1. Repeating letter dropped 2. 's' replaced by 'z'

Table 12. SMS words created using rules D and F

SMS text	Standard words	Explanation
watz	whats	1. Dropping 'h ' associated with 'w' 2. Replacing 's' with 'z'
w@	what	1. 'h' associated with 'w' removed 2. 'at' replaced by symbol @

Table 13. SMS words created using 3 rules. First 3 columns show the example which uses rule A, C and D and the last 3 columns show the example which uses rules B, C and F

SMS text	Standard words	Explanation
caln	calling	1. Partial vowel removal 2. Removing repeated letter 3. Dropping last 'g'
10s	tennis	1. Vowel dropped 2. Repeating letter dropped 3. Phonetic replacement by digit

5.8 Abbreviations as SMS terms

Many standard and custom made abbreviations of the standard words are used to create the SMS (Table 14).

Table 14. Standard and custom made abbreviations as SMS terms

SMS text	Standard Forms	SMS text	Standard Forms
Comfy	comfortable	Btw,	between
		b/w	
lab	laboratory	audi	auditorium
motivatn	motivation	std	standard
no	number	envt	environment
Tomm, morrow	tomorrow	hol	holiday
mgmt	management	govt	government
nite	night	cum	come
id	identity	Bcoz, cuz	because
Diff/diffce	difference	pic	picture
Bday, b/day	birthday	ello	hello
exam	examination	chap	chapter
2maro	tomorrow		

5.9 Stylistic variation

This is the trend among the youngsters who use any style of writing a SMS term and these cannot be predicted. Table XV shows some examples of such stylistic variations.

Table 15. Stylistic variations used for SMS terms

SMS text	Standard word
Mah, ma	my
betta	better

6. GENERAL RULES FOLLOWED FOR CREATING AN SMS

It was also observed that code for the same word varied from person to person. Where one coded tomorrow as '2maro, the other coded it as '2morrow' and yet another as 'tomorrow'. Yet the variations followed one or the other rules from rule number 1-8. So for obvious reasons a rule based system, which is developed on the basis of the above rules, will certainly take care of all the morphological variations of the query terms.

It was observed that the dropping of partial vowels(the first one generally) when a vowel starts a word in many cases gives a totally mismatched reduced structure of word which does not match the standard word at all and does not convey the phonetics as well. For example, on one hand where 'awful', 'own', 'idle' etc will give totally meaningless word, on the other 'ideal' will give a totally different word with a different meaning. Also dropping the vowels completely sometimes poses problems and gives the same consonant skeleton for different words. For e.g. 'Quiet' and 'quite' and 'quit' in such a case will give the same term 'qt' which naturally will not be coded as same in the SMS terms. Likewise, 'form', 'from' and 'forum' also be coded as the same term 'frm' which is actually a SMS term for 'from'. For such terms the proximity phrase search or context searching needs to be done.

Each SMS S is a collection of tokens S = t1, t2, t3…., tn. Let Q denote the set of questions in any organization's FAQ corpus. Each question Q* ϵ Q a also a collection of tokens. The algorithm below

aims at finding the question Q* from corpus Q which is the best equivalent for SMS S.

The proposed approach takes into account the above mentioned rules to develop a rule based approach for query expansion and proceeds through the following steps for automatic generation of query Q*:

1. Developing a Domain dictionary consisting of all terms that appear in standard collection of queries in the FAQs of the organization.
2. Creating a synonym dictionary for all the terms of the domain dictionary and mapping them to the terms in the domain dictionary.
3. Processing the terms of the domain dictionary and their synonyms, using the above mentioned rules, for creating a rule based list of variants that could match the SMS text and arranging them along with the standard term in alphabetical order
4. Searching the SMS terms in the list of generated variants
5. If a match is found, mapping the matched term to the domain dictionary term
6. Retrieving the actual query term
7. Retrieving all the queries which contain that particular term
8. Repeating the process for all terms of SMS and generating a query list for each
9. Applying 'project' operation to find the query which is common in all the query lists
10. This will give the required query.

Figure 2 describes the steps for query expansion.

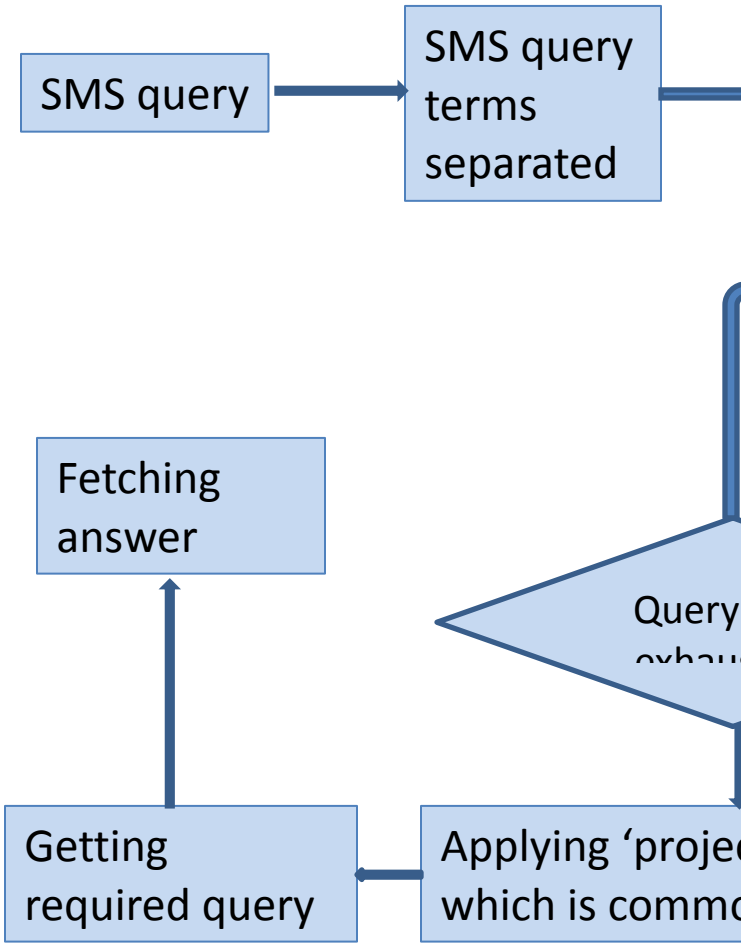


Figure 2. Steps for Rule Based Expansion of Query Terms

Also taking into account the problems with dropping of vowels and after carefully analyzing a long list of words, it was observed that the following conditions have to fulfilled before removing vowels either partially or completely to avoid generation of totally junk

words. In all these cases if after removing the vowel if the reduced word sounds the same, then the rule can be relaxed.

1. If two lettered word, vowel should not be removed unless the removal does not affect the phonetics. . E.g. *to, no, of* should be retained as it is but in *in* it can be removed to give the same sound even with *n.*
2. If three lettered word with only one vowel e and that too as the last letter, vowel should not be removed. E.g. *the* should remain as it is or the whole word should be replaced by d
3. If three or five lettered with single vowel (a,i,o) as the middle alphabet
4. If four lettered word and last letter s, vowel should not be removed. E.g. tabs
5. If four lettered word and last letter is the second vowel, last vowel should not be dropped
6. If four lettered word and last two letters same, vowel should not be removed. E.g. call, tall (removal gives cll, tll which will also be obtained in case of the words cell and tell)
7. If I and e appear in a word with an intervening consonant, then i is replaced by y and e is dropped e.g. Bike->byk, like->lyk, time->tym, life->lyf
8. Same way if o and e appear in a word with an intervening constant, then o is replaced by u and e removed e.g. some-> sum, come->cum
9. If the word starts with a vowel then first vowel should not be removed. E.g. if not followed, idle will give dle which is a junk word and our will become ur which is the abbreviated form of your
10. Two vowels appearing together in succession (except for a and u appearing with o or e appearing with u) vowel should not be removed.
11. If a and o or u and o appear together in succession and a follows o or u follows o then a and u can be removed but o has to be retained. E.g. fought(foght), goal(gol)
12. If u and e appear together and e follows u then u can be removed. Eg. Guess
13. If u comes after o with a consonant in between then u has to be retained, o can be removed. E.g. forum-> frum
14. If ou come together and are the only two vowels of the word followed by l, o and l can be removed e.g. should ->shud, could->cud
15. S occurring in between the words should not be replaced by z
16. If word with single vowel and last letter is g, g should not be removed.
17. If word is a standard abbreviation it should be preserved as it is.
18. The abbreviated months and week days should be retained as it is.
19. Last two letters same and single vowels before that, vowels should not be removed. Eg still, stall, wall, mess
20. If vowels alternate with consonant and there are only two vowels in the word, then the initial vowel can be removed. Eg forum-> frum, daring->dring
21. If applying two rules ie of vowel removal and of removal of one of the two consecutive repeated character, if the word after the first rule gives the ending as nng then the rule for removal of last g should not be applied as the third rule to generate abbreviations e.g. training-> trainng-> traing-> train×

7. CONCLUSION

It has been observed that dropping a vowel is the most obvious and used rule for creating an SMS term. The reason being its presence in every word more than once and dropping it considerably saves space where space is a constraint. As the proposed system takes into account the inadvertent but unanimously accepted vocabulary of the cryptic terms used in the SMS and tries to form rules from the same, it is able to devise a very easy and less time consuming method for automatic generation of expanded query terms for SMS based retrieval system. It does not involve any complex calculation and uses only table look ups and mappings to expand the query terms. Also it uses lesser number of steps to do the same. The unordered, unplanned and non standard format of the SMS will take the standard form automatically when this Rule Based system will be applied and will certainly prove a step forward in this direction. However, this approach does take into account the typographical errors and spelling mistakes. The experimentation is still in its progress stage. Once this proves successful, it can be deployed on a larger corpus of FAQs.

8. ACKNOWLEDGEMENT

Authors are grateful to FIRE for providing corpus of FIRE 2012 for conducting the experiment

One of the authors, Aarti Kumar, is thankful to Maulana Azad National Institute of Technology, Bhopal, India for providing her the financial support to pursue her Doctoral work as a full time research scholar.

9. REFERENCES

[1] Manning Christopher D., Raghavan P. and Schulz H. An Introduction to Information Retrieval, Cambridge University Press.

[2] Baeza-Yates R. and Ribeiro-Neto B. Modern Information Retrieval, Pearson education.

[3] Joel S. and Samuel W. Information Retrieval System Design for Very High Effectiveness.

[4] Kothari G. et al. SMS based interface for FAQ retrieval.

[5] Hogan D. et al. SMS Based FAQ Retrieval.

[6] Pathak V. M. and Joshi M. R. Itransed Marathi Literature Retrieval Using SMS Based Natural Language Query.

[7] Cook P. and Stevenson S. An Unsupervised Model for Text Message Normalization

[8] Pennell Deana L. and Liu Y. Normalization Of Text Messages for Text-To-Speech.

[9] Liu F. et al. Insertion, Deletion, or Substitution? Normalizing Text Messages without Pre-categorization nor Supervision.

[10] Frakes W.B. and Baeza-Yates R. editors. 1992. Information Retrieval: Data Structures and Algorithms. Prentice-Hall.

[11] Salton G. 1989. Automatic Text Processing: The Transformation, Analysis, and Retrieval of Information by Computer. Addison-Wesley, Reading, Massachusetts.

[12] Ravino B. and Boll R. 1993. A Natural Semantics for Information Retrieval. In East Pacific Rim Symposium on Applied Linguistics, pages 161–163.

[13] Kobus C., Yvon F. and Damnati G. 2008. Normalizing SMS: are two metaphors better than one? In Proc. of the 22nd Int. Conf. on Computational Linguistics, pp. 441–448. Manchester.

[14] AiTi Aw et al. 2006. A phrase based Statistical model for SMS text normalization. In Proc. of the COLING/ACL 2006 Main Conference Poster sessions, pages 33-40, Sydney.

[15] Choudhary M. et al. 2007. Investigations and modeling of the structure of texting language. International Journal of Document analysis and Recognition, 10(3/4):157-174.

[16] Rebecca E. et al. 2001. Y do tngrs luv 2 txt msg. In Proceedings of 7th European Conference on Computer Supported Cooperative Work, pages 219-238, Bonn, Germany.

[17] Sproat R. et al. 2001. Normalization of Non-standard words. Computer Speech and language, 15: 287-333.

International Journal of Computer Applications Technology and Research
Volume 3– Issue 11, 718 - 720, 2014

Knowledge Management in the Cloud: Benefits and Risks

Mehmet Sabih AKSOY
College of Computer and Information Sciences
Department of Information Systems,
King Saud University
Kingdom of Saudi Arabia

Danah Algawiaz
Information Systems Department
Shaqra University
Kingdom of Saudi Arabia

Abstract: The success of organizations largely depends on continual investment in learning and acquiring new knowledge that creates new businesses and improve existing performance. So, using Knowledge management must result in better achieving, or even exceeding, organizations objectives. The purpose of knowledge management must not be to just become more knowledgeable, but to be able to create, transfer and apply knowledge with the purpose of better achieving objectives. As new technologies and paradigms emerge, businesses have to make new efforts to properly get aligned with them, especially in knowledge management area. Today the Cloud Computing paradigm is becoming more and more popular, due to the vast decrease in time, cost and effort for meeting software development needs. It also provides a great means for gathering and redistributing knowledge. In this paper, we will discuss the benefits and risks of using cloud computing in knowledge management systems.

Keywords: Knowledge, Cloud Computing, Knowledge Management, Service Oriented Architecture, Grid computing, Knowledge Management Systems.

1. INTRODUCTION

Knowledge is an understanding of someone or something, such as facts, information, descriptions, or skills, which is acquired through experience or education by perceiving, discovering, or learning [1]. Also, knowledge can refer to a theoretical or practical understanding of a subject. Furthermore, it can be implicit or explicit [2]. Explicit knowledge is knowledge that has been articulated, codified, and stored in certain media. Moreover, it can be readily transmitted to others. However, tacit knowledge is the kind of knowledge that is difficult to transfer [3]. A knowledge management system is most often used in business in applications such as information systems, business administration, computer science, public policy and general management. Organizations need Knowledge Management for finding, mapping, gathering, filtering information, developing new knowledge, converting personal knowledge into shared knowledge resources, understanding and learning, and adding value to information to create knowledge. The three fundamental processes of knowledge management are knowledge acquisition, knowledge sharing, and knowledge utilization [4]. However, Knowledge management is not a static process, it is dynamic from two dimensions: the business and the technology [5]. So, for the success of knowledge management, it should be kept aligned with the business and the technology, which is fast upgrading. One of the new popular technological paradigms is cloud computing (CC) that is an extension to grid computing and the service-oriented architecture (SOA) [6]. As [6] articulates, CC has five key characteristics: providing on demand self-service, based on broad network access, making advantage of resource pooling, rapid elasticity based on cloud consumers' resource needs, and providing the ability to measure the provided services. In this paper, we aim to discuss the benefits and risks of using cloud computing in knowledge management systems. The reminder of this article is organized as follows: section 2 is devoted to explain knowledge Management Systems. However section 3 will explain cloud computing. Benefits of Using Cloud Computing in Knowledge Management systems are detailed in section 4. Then section 5 will explain Risks of Using Cloud Computing in Knowledge Management Systems. Finally we conclude in section 6.

2. KNOWLEDGE MANAGEMENT SYSTEMS

It is not easy to define the term "knowledge" as it has different meanings depending on context. In the context of the business enterprise or the personal computer user, knowledge tends to connote possession of experienced "know-how" as well as possession of factual information or where to get it [1]. In philosophy, the theory of knowledge is called epistemology and deals with such questions as how much knowledge comes from experience or from innate reasoning ability; whether knowledge needs to be believed or can simply be used; and how knowledge changes as new ideas about the same set of facts arise [1]. Knowledge management is A method for the improvement of business process performance [3]. In addition, a knowledge management system is most often used in business in applications such as information systems, business administration, computer science, public policy and general management. Also, common company departments for knowledge management systems include human resources, business strategy and information technology. Moreover, knowledge management systems consist of processes to capture, distribute, and effectively use knowledge [7]. Knowledge acquisition is the process of development and creation of insights, skills, and relationships [4]. On the other hand, Knowledge sharing is disseminating and making available what is already known. However, Knowledge utilization includes research, scholarly, and programmatic intervention activities aimed at increasing the use of knowledge to solve problems [8]. The knowledge Management functions are finding, mapping, gathering, filtering information, developing new knowledge, converting personal knowledge into shared knowledge resources, understanding and learning, adding value to information to create knowledge, enabling action through knowledge, processing shared knowledge resources, delivering explicit

knowledge, and building adequate technical infrastructures [9].

3. CLOUD COMPUTING

Cloud Computing is an extension to grid computing and the Service-Oriented Architecture [6]. And Grid computing is the collection of computer resources from multiple locations to reach a common goal. Also, Grid computing is applying the resources of many computers in a network to a single problem at the same time - usually to a scientific or technical problem that requires a great number of computer processing cycles or access to large amounts of data [10]. Service-oriented architecture (SOA) is a software design and software architecture design pattern based on distinct pieces of software providing application functionality as services to other applications [6]. Moreover, this is known as service-orientation. In addition, it is independent of any vendor, product or technology [10]. Service-Oriented Architecture makes it easy for computers connected over a network to cooperate [6]. Besides, every computer can run an arbitrary number of services, and each service is built in a way that ensures that the service can exchange information with any other service in the network without human interaction and without the need to make changes to the underlying program itself [6]. Cloud computing is internet-based computing in which large groups of remote servers are networked to allow the centralized data storage, and online access to computer services or resources. Furthermore, clouds can be classified as public, private, community or hybrid [9]. Private cloud is accessible from an intranet, internally hosted, and used by a single organization [11]. Community cloud has infrastructure accessible to a specific community. And public cloud is accessible from the internet, externally hosted, and used by the general public [12]. Finally, hybrid cloud is a combination of two or more clouds [13]. Moreover, there are five essential characteristics of cloud computing: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service [14]. Users of On-demand self-service are able to provision cloud computing resources without requiring human interaction, mostly done though a web-based self-service portal (management console) [15]. In contrast, broad network access means that cloud computing resources are accessible over the network, supporting heterogeneous client platforms such as mobile devices and workstations [15]. But resource pooling is the service multiple customers from the same physical resources, by securely separating the resourceson logical level [15]. And rapid elasticity is the resources that provisioned and released on-demand and/or automated based on triggers or parameters [15]. Resource usage are monitored, measured, and reported (billed) transparently based on utilization by measured service [16]. Furthermore, cloud computing is much more than just virtualization. It's really about utilizing technology "as a service". There are three Service models of cloud computing: Infrastructure as a service, Platform as a service, and Software as a service [17]. Infrastructure as a service (IaaS) provides access to server hardware, storage, network capacity, and other fundamental computing resources [17]. And Platform as a service (PaaS) provides access to basic operating software and services to develop and use customer-created software applications [18]. Finally, Software as a service (SaaS) provides integrated access to a provider's software applications [17].

4. BENEFITS OF USING CLOUD COMPUTING IN KNOWLEDGE MANAGEMENT SYSTEMS

Cloud computing provides a scalable online environment that makes it possible to handle an increased volume of work without impacting system performance. Cloud computing also offers significant computing capability and economy of scale that might not otherwise be affordable, particularly for small and medium-sized organizations, without the IT infrastructure investment [19]. Organizations can provide unique services using large-scale computing resources from cloud service providers, and then nimbly add or remove IT capacity to meet peak and fluctuating service demands while only paying for actual capacity used. Moreover, organizations can rent added server space for a few hours at a time rather than maintain proprietary servers without worrying about upgrading their resources whenever a new application version is available [20]. They also have the flexibility to host their virtual IT infrastructure in locations offering the lowest cost. Optimized IT infrastructure provides quick access to needed computing services. In addition, providing the right level of security for knowledge management system is a challenging that can be solved by using cloud computing. Also, cloud computing can keep knowledge management up with technology. By using private cloud sensitive information should be shielded from most users, while allowing easy access to those with the proper credentials. Furthermore, community and hybrid cloud can motivated people and overcoming organizational culture challenges by developing a culture that embraces learning, sharing, changing, and improving knowledge sharing [19].

5. RISKS OF USING CLOUD COMPUTING IN KNOWLEDGE MANAGEMENT SYSTEMS

Depending on the cloud solution used (SaaS, PaaS, or IaaS), users of knowledge management system may be unable to obtain and review network operations or security incident logs. A multi-tenant cloud environment in which users of knowledge management system and applications share resources presents a risk of data leakage that does not exist when dedicated servers and resources are used exclusively by one organization [21]. Also, if cloud computing is adopted to a significant degree, an organization needs fewer internal IT personnel in the areas of infrastructure management, technology deployment, application development, and maintenance. So, the morale and dedication of remaining IT staff members could be at risk as a result. Many cloud service providers are relatively young companies, or the cloud computing business line is a new one for a well-established company. Hence the projected longevity and profitability of cloud services are unknown. At the time of publication, some Cloud Service Providers are curtailing their cloud service offerings because they are not profitable. And cloud computing service providers might eventually go through a consolidation period. As a result, Cloud Service Provider customers might face operational disruptions or incur the time and expense of researching and adopting an alternative solution, such as converting back to in-house hosted solutions [21].

6. CONCLUSION

Using Knowledge management systems must result in better achieving, or even exceeding, organizations objectives. However, Knowledge management is not a static process; it is dynamic from two dimensions: the business and the technology. And as new technologies and paradigms emerge, businesses have to make new efforts to properly get aligned with them, especially in knowledge management area. Today the Cloud Computing paradigm is becoming more and more popular, due to the vast decrease in time, cost and effort for meeting software development needs. It also provides a great means for gathering and redistributing knowledge. But using cloud computing in Knowledge management system has some risks like risk of data leakage, IT organizational changes and cloud service provider viability. Our future work will be a bout decrease risks of using cloud computing in knowledge management systems by reducing likelihood and impact of risks in cloud computing.

7. REFERENCES

[1] Stanley Cavell, "Knowing and Acknowledging", Must We Mean What We Say? (Cambridge University Press, 2002), 238–266.

[2] Drucker, P., The age of discontinuity: guidelines for our changing society. New York: Harper & Row, 1969.

[3] Davenport, Thomas H. (1994). "Saving IT's Soul: Human Centered Information Management". Harvard Business Review 72 (2): 119–131.

[4] Alavi, M. and Leidner, D., Review: knowledge management and knowledge management systems: conceptual foundations and research issues, MIS Quarterly, Vol. 25 No. 1, pp. 107-36, 2001.

[5] Gupta, Jatinder; Sharma, Sushil (2004). Creating Knowledge Based Organizations. Boston: Idea Group Publishing. ISBN 1-59140-163-1.

[6] P. Mell, and T. Grance, Draft NIST Working Definition of Cloud Computing, 2009.

[7] Wong, K.Y. and E. Aspinwall; Characterizing knowledge management in the small business environment, Journal of Knowledge Management, vol. 8, pp. 44-61, 2004.

[8] Jay Liebowitz, Strategic Intelligence: Business Intelligence, Competitive Intelligence, and Knowledge Management, Auerbach Publications, 2006.

[9] Maier, R., Knowledge management systems, 3rd edition, Springer, 2007.

[10] I. Sriram and A. Khajeh-hosseini, Research Agenda in Cloud Technologies, Methodology abs/1001.3, 2010.

[11] Foley, John. "Private Clouds Take Shape". InformationWeek. Retrieved 2010-08-22

[12] Rouse, Margaret. "What is public cloud?". Definition from Whatis.com. Retrieved 12 October 2014.

[13] Rouse, Margaret. "What is a multi-cloud strategy". SearchCloudApplications. Retrieved 3 July 2014.

[14] "What is Cloud Computing?". Amazon Web Services. 2013-03-19. Retrieved 2013-03-20.

[15] "Defining 'Cloud Services' and "Cloud Computing"". IDC. 2008-09-23. Retrieved 2010-08-22.

[16] Danielson, Krissi (2008-03-26). "Distinguishing Cloud Computing from Utility Computing". Ebizq.net. Retrieved 2010-08-22.

[17] Keep an eye on cloud computing, Amy Schurr, Network World, 2008-07-08, citing the Gartner report, "Cloud Computing Confusion Leads to Opportunity". Retrieved 2009-09-11.

[18] Boniface, M. et al. (2010), Platform-as-a-Service Architecture for Real-Time Quality of Service Management in Clouds, 5th International Conference on Internet and Web Applications and Services (ICIW), Barcelona, Spain: IEEE, pp. 155–160, doi:10.1109/ICIW.2010.91

[19] "Towards Continuous Cloud Service Assurance for Critical Infrastructure IT". The 2nd International Conference on Future Internet of Things and Cloud (IEEE FiCloud-2014). Retrieved 2014-08-15.

[20] Kemal A. Delic, Jeff A. Riley , Enterprise Knowledge Clouds: Next Generation KM Systems?, International Conference on Information, Process, and Knowledge Management, 2009.

[21] Albena Antonova, Roumen Nikolov, Conceptual KMS Architecture within Enterprise 2.0 and Cloud Computing, Computing, 2005.

International Journal of Computer Applications Technology and Research
Volume 3– Issue 11, 721 - 724, 2014

Assistive System Using Eye Gaze Estimation for Amyotrophic Lateral Sclerosis Patients

Cheng-Chieh Chiang
Department of Information Technology
Takming University of Science and Technology
Taipei, Taiwan

Abstract: Amyotrophic lateral sclerosis (ALS) patients cannot control their muscle except eyes in the later stage of the disease progress. This paper aims to develop an eye-based assistive system that is controlled by the eye gaze to help ALS patients improve their life quality. Two main functions are proposed in this paper. The first one is called HelpCall that can detect the users' eye gaze to active the corresponding events. ALS patients can "talk" with other people more easily by looking at specific buttons in the HelpCall system. The second one is an eye-control browser that allows the users browsing web pages in Internet. We design an interface that embeds the IE browser into several buttons controlled by the user eye gaze. ALS patients can visit the Internet only using their eyes in our proposed system. This paper discusses our ideas for the assistive system and then describes the design and implementation of our proposed system in details.

Keywords: Amyotrophic Lateral Sclerosis; eye-based assistive system; eye gaze; HelpCall; eye-control browser.

1. INTRODUCTION

Amyotrophic lateral sclerosis (ALS) is a neurodegenerative disease that patients gradually lose the control for their muscle in the whole body. Eventually, patients cannot move their any part of bodies, except eyes, in the end of the disease progress. In the last stage of their life, ALS patients are locked in the frozen body and lose the ability to communicate with other people. The rough description about the ALS disease can be found in the Wikipedia site [1].

Eye is the only one part that most of ALS patients can control in the last stage of the ALS. It has much potential to improve the life quality if ALS patients can "do something" using their eyes. Hence, an assistive system that can be controlled by the eye gaze should be helpful for ALS patients. Now there have been some products called Eye Tracker [2][7][9][10] that can estimate what target the user looks at. In current many eye tracker system have been released for different goals that are introduced in Section 2.

This paper aims to design an eye-based assistive system for ALS patients to build a communication bridge. What kinds of applications do ALS patients need? The assistive system does not need complex or rich of functions. Instead, we try to design a simple but helpful user interface for patients. In this paper two applications to help ALS patients in their life are provided. First, we design an assistive function called HelpCall, which allows the patients can easily "talk" with other people by looking at specific buttons in screen. For example, a caregiver may ask whether the patient wants to watch TV or not, and then the patient only need to stare at a "Yes" button to answer it. Second, an eye-control browser is proposed to allow the patients browsing webpages in Internet. Using this eye-control browser, the patients can determine by themselves what pages they want to view.

Figure 1 draws the brief flowchart of our system. When a video frame is captured, we first employ a face detection method to detect the face region in image. In general, a human face contains a fixed layout consisting of eyes, nose, and mouth. Hence, a method for eye detection is performed on a rough eye-area in face to determine the eye regions. Moreover, we design the horizontal and vertical projection for pupil localization due to the high contrast between the pupil and the surrounding area. The pupil localization can define the coordinate of pupil in eye, and then we construct a mixture of Gaussian Models to estimate the corresponding eye gaze. Finally, the eye gaze can drive the mouse control in the two applications, HelpCall and the eye-control browser, proposed in this paper.

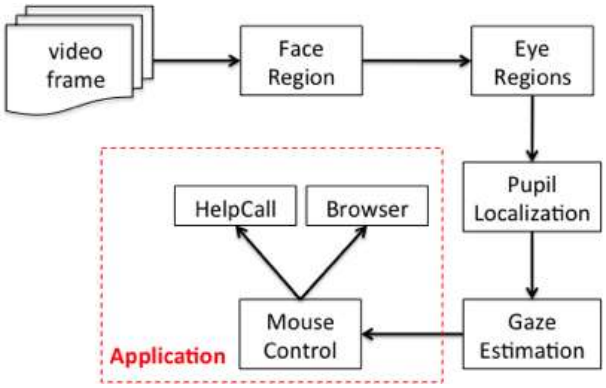


Figure 1. Example of an image with acceptable resolution

The rest of this paper is organized as the follows. Section 2 reviews previous works related to this paper. Section 3 describes how to localize the pupil position in eye, and then Section 4 presents our approach to estimate the user eye gaze. The design and implementation of the proposed assistive system are shown in Section 5. Finally, Section 6 draws our conclusions and discusses potential extensions for this work.

2. RELATED WORKS

Many eye tracking systems have been released in the market for different goals, such as EyeLink [2], MangoldVision [7], SMI iView [9], and Tobii [10]. Most of eye tracking systems request to fix the head position in order to simplify the pupil localization. For example, both EyeLink and SMI iView need to construct a "head holder" in Figure 2(a) and 2(b) to keep the accurate estimation for eye gaze estimation. This case of

eye tracking system is not appropriate for ALS patients who need to lie on a bed.

(a) EyeLink (b) SMI iView

Figure 2. Both EyeLink in (a) and SMI iView in (b) need to construct a "head holder" to keep the head position.

Another type of eye tracking systems is to embed a camera into a glasses to track the pupil position, such as MangoldVision [7] and Tobii [10] shown in Figire 3. These two systems are wearable, hence ALS patients can wear the camera-glasses on bed to control the computer system. In fact, Tobii is somewhat widely used for ALS patients. Unfortunately, the prices of Tobii systems are also a little high. Our work in this paper tries to employ a common camera to reduce the cost of the whole system. Moreover, we design two specific functions to help ALS patients to improve their inconvenient life.

(a) MangoldVision (b) Tobii

Figure 3. MangoldVision in (a) and Tobii in (b) designs wearable glasses that appends a camera to estimate the pupil position.

3. PUPIL LOCALIZATION

Pupil is one of the most significant features in eye. Given a video frame, this section presents our procedures to locate the pupil position in eye, including the face detection to separate the face region, eye region detection on the face region, and determining the pupil coordinate in eye.

3.1 Face Detection

Face detection is a key technology to locate or identify human in image. Many state-of-the-art approaches have been proposed to treat the face detection in either image or video under different conditions of the real world [5][6].

This work adopted the adaboosting approach [11], which was first proposed by Viola and Jones in 1999, to automatically detect face regions in a video frame. This approach collects a large number of Haar-like features that are fast computed by the integral image. Then, an adaboosting approach [3] is employed to select most significant Haar-like features of face regions. In general, many Haar-like features may be contained to construct an efficient classifier in the adaboosting approach, but that should also need more computational time for face detection. In order to achieve the real-time requirement, Viola and Jones designed a cascading structure, the basic concept is shown in Figure 4, to fast filter most of trivial non-face regions out using fewer Haar-like features in the several starting stages and then accurately to detect face regions using more features in the ending stages.

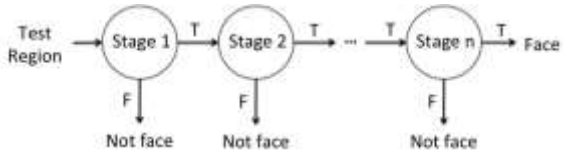


Figure 4. The cascade structure to speed up the face detection

The adaboosting approach of face detection has been implemented in the openCV library [8] and was widely used in many applications. Although this approach may be failed if the orientation of face regions is skew, it is still appropriated for our framework due to skewed human faces can be simply ignored in eye-related applications such as the eye state monitoring for car drivers.

3.2 Eye Region

The eye region in face contains a strong characteristic that there is high contrast between the eyes and the surrounding areas. Thus, the gray channel is more appropriate than color channels in representing eye regions. Hence, the first step to detect the eye region is to convert the face image from color to gray. We adopt the simplest averaged method for the gray conversion: gray = (R+G+B)/3, where R, G, and B are the pixel values in the red, green, and blue channels, respectively.

Next, we employ the adaptive thresholding method [4] to make a binary image from the gray image of face. In the traditional thresholding method for binarization, it is difficult to choose a proper threshold globally for a whole image. Instead a global threshold, the adaptive thresholding method computes the average of pixel values in a slide window to be a local threshold value associated with the center pixel of the slide window. The adaptive thresholding method can make a better binarization by adapting the intensity various locally. The details of the adaptive thresholding method can be found in [4].

Now a binary image of face can be available from a video frame. Our next step is to determine the accurate position of the pupil in eye. Since our goal of this work is to design a practical system for ALS patients, the computation in our methods must be simple such that the system can have fast responses in work. Thus, we employ the horizontal and vertical projection method [12] to fast but efficiently capture the eye regions. Assume that $I(x, y)$ is the pixel value at (x, y) in a candidate of eye region with size m by n pixels. Because the image is converted to binary, the pixel values have to be either 0 or 1. The horizontal (H_{porj}) and vertical (V_{proj}) projection on the binary image can be defined as the follow,

$$H_{proj}(x) = \sum_{x=1}^{n} I(x, y), \text{ where } x = 1 \text{ to } m$$
$$V_{proj}(y) = \sum_{x=1}^{m} I(x, y), \text{ where } y = 1 \text{ to } n. \quad (1)$$

Figure 5 presents an illustration that performs the horizontal and the vertical projections in a binary eye image. Due to the low intensity of the pupil, the maximal peaks in the projections can indicate the center in the two coordinates. That is to say, the center coordinate of the pupil can be located according to the two maximal peaks.

(a) (b) (c)

Figure 5. An illustration for eye region decision. (a) and (c) are the results of the horizontal and the vertical projections in the binary eye image (b), respectively. Thus, the intersection of maximal peaks in the two projections can locate the eye region drawn in the red circle of (b).

4. GAZE ESTIMATION

In order to understand what target the user is looking at, we have to construct the mapping between the coordinate in screen and the pupil position in eye. Unfortunately, the coordinate scales of screen and eye region are very different. Assume that an image is 640x480 captured from a common webcam, and hence we cannot expect to get an eye region with high resolution. In our implementation, the width of an eye region is often less than 100 pixels in our system. In contrast to pupil, the resolution is often very high in the current screen. Hence, the coordinate mapping from pupil to screen could be very sensitive to the accuracy of the pupil localization.

The whole screen are divided into 3x3=9 grids instead of high-resolution coordinates to reduce the sensitivity of the gaze estimation. Let $L = \{L_i | i=1, \ldots, 9\}$ be the nine areas in the screen, and then our task is to convert the coordinate of pupil position in eye to the nine grid. To this end, we construct nine Gaussian distributions, denoted G_i with mean μ_i and variance σ_i^2, associated with the nine grids $L = \{L_i | i=1, \ldots, 9\}$. Given a pupil position (x, y), the gaze can be assigned to the screen grid L_{i^*}, where

$$i^* = \arg\max_i G_i(x, y) \quad (2)$$

The mean μ_i and variance σ_i^2 of Gaussian distribution G_i can be computed by the training images that are captured by asking for the patient looking at the grid L_i. When the proposed assistive system starts, the screen first shows a circular point in a grid and then asks for the patient watching this point. Repeating nine times with changing grids, the system can capture a lot of training images that the patient looks at each of grids. Therefore, the mean and variance of the pupil coordinates associated with a grid can be computed to determine the Gaussian distribution.

5. DESIGN AND IMPLEMENTATION

This section presents our design of the assistive system that is controlled by the user gaze. Two systems are proposed in this paper. The first one is called HelpCall that can help ALS patients communicate with people. The second one is an eye-control browser to help the patient does not need a mouse but use the eye gaze to control the browser in Internet.

5.1 HelpCall

The idea of HelpCall system is intuitive: one button presents one meaning. The users can look at a specific button to present their opinions without any talks. Figure 6 shows the interface of this system that contains four dedicated and five user-defined functions. The four dedicated functions are:

- TV: ask for watching TV
- CALL: trigger an alarm to call the caregiver.
- YES/NO: a simple answer in talk.

This system preserves five functions that patients can define them according to their needs. All of nine functions can be edited by the users if necessary.

Figure 6. The user interface of HelpCall system, containing four dedicated (blue) and five user-defined functions.

5.2 Eye-Controlled Browser

ALS patients have been imprisoned in body, hence our idea is to design an eye-controlled browser that can allow them contact rich contents of Internet. The most challenging issue of this system is to design an appropriate interface that cannot only provide a simple way browsing a web page for ALS patients but also cover the complex functions of a browser.

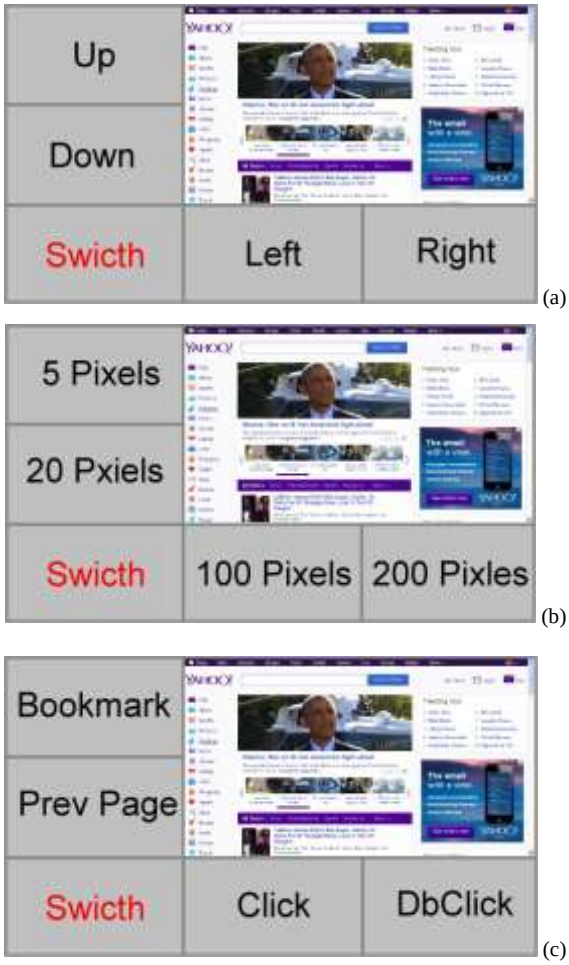


Figure 7. The user interface of our proposed eye-controlled browser system. Buttons in three pages can help ALS patients to control the IE browser without mouse.

The interface of the proposed system is shown in Figure 7 that embeds several buttons in order to control the cursor by eye gaze instead of moving mouse. The interface is also based on the layout of 9x9 grids, where the browser covers four right-upper grids and functional buttons are on the other five grids. The "Switch" button can change functions such that 4x3=12 functional buttons are provided to control the browser. In the first page of Figure 7(a), buttons are used for moving the cursor with the directions. The buttons of Figure 7(b) can determine the step size of cursor moving. Figure 7(c) provides four important functions, containing "Click" and "DbClcik" for mouse click and double click, respectively, "Bookmark" for opening the bookmark page, and "Pre Page" for returning the previous page.

ALS patients can completely control the browser using our proposed interface by their eye gaze. First, the users can look at "Switch" button to change the page of Figure 7(a), and then enable the four directional buttons to move the cursor in the browser. If the users want to change the moving step of cursor, they just need to switch to the second page in Figure 7(b). When the cursor stays at a link of interest in the web page, the users can switch the page again to Figure 7(c) and enable the "Click" function to enter the hyperlink.

6. CONCLUSION AND FUTURE WORK

ALS patients should be difficult to control their body muscle in the late stage of life. This paper proposes an assistive system with two functions, HelpCall and an eye-controlled browser, to help ALS patients based on the computer vision technologies. The HelpCall system provides nine buttons of grids to present nine responses for ALS patients by using eye gaze. The eye-controlled browser embeds additional buttons to allow ALS patients moving the cursor in the browser using their eyes. These two assistive functions can definitely improve the quality in life for ALS patients.

Two main extensions are included in our future works. Using eye gaze to control the interface is not an easy way for users in a practical system. Hence, we plan to develop the blink detection for the proposed assistive system and then to perform a user study of this system controlled by the eye gaze and blink. The second potential extension for this work is to design an eye-controlled keyboard, either eye gaze or blink, that users can enter words in the browser such that the functions in the proposed assistive system can be more complete.

7. REFERENCES

[1] Amyotrophic lateral sclerosis, http://en.wikipedia.org/wiki/Amyotrophic_lateral_sclerosis

[2] EyeLink, http://www.sr-research.com/

[3] Freund, Y., Schapire, R., and Abe, N., A short introduction to boosting. Journal-Japanese Society For Artificial Intelligence, 1999. 14: p. 771-780.

[4] Gonzalez, R. C. and Woods, R. E., Digital Image Processing, 3rd Edition. Prentice Hall, 2007.

[5] Hsu R.-L., Abdel-Mottaleb M., and Jain A. K., Face detection in color images. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2002. 24(5): p. 696-706.

[6] Liao S., Jain A. K., Li S. Z., Partial face recognition: alignment-free approach. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2013. 35(5): p. 1193-1205.

[7] MangoldVision, http://www.mangold-international.com/home.html

[8] OpenCV, http://opencv.org/

[9] SMI, http://www.smivision.com/en.html

[10] Tobii, http://www.tobii.com/

[11] Viola P. and Jones M. J., Robust real-time face detection. International journal of computer vision, 2004. 57(2): p. 137-154.

[12] Zhou Z.-H. and Geng X., Projection functions for eye detection. Pattern recognition, 2004. 37(5): p. 1049-1056.

International Journal of Computer Applications Technology and Research
Volume 3– Issue 11, 725 - 728, 2014

A Survey on the Classification Techniques In Educational Data Mining

Nitya Upadhyay
RITM
Lucknow, India

Vinodini Katiyar
Shri Ramswaroop Memorial University
Lucknow, India

Abstract: Due to increasing interest in data mining and educational system, educational data mining is the emerging topic for research community. educational data mining means to extract the hidden knowledge from large repositories of data with the use of technique and tools. educational data mining develops new methods to discover knowledge from educational database and used for decision making in educational system. The various techniques of data mining like classification. clustering can be applied to bring out hidden knowledge from the educational data.
In this paper, we focus on the educational data mining and classification techniques. In this study we analyze attributes for the prediction of student's behavior and academic performance by using WEKA open source data mining tool and various classification methods like decision trees, C4.5 algorithm, ID3 algorithm etc.

Keywords: Educational data mining; Classification; Analysis; WEKA,

1. INTRODUCTION:

The examination and study of student's academic performance is not a new exercise but computer based learning environment increases more interest towards student's analysis. The concepts and techniques of data mining can be implemented in education to predict the academic performance of student. On the basis of these kind of predictions the academic performance of student can be improved. EDM is applied to large amount of data accumulated by surveys and various classification techniques are implemented for better performance. The prediction of student's performance has become one of most important needs in order to improve the quality of performance. There is a need of data mining in educational system for the students as well as academic's responsible. Educational data mining is an arising regulation that promote the new techniques for extracting the new data that come from educational settings and by using those techniques, a better prediction can be done for student's behavior, academic performance, subject interest etc.

2. WHAT IS EDUCATIONAL DATA MINING?

Data mining originate a new technique known as educational data mining. In educational data mining, data mining concepts are applied to data that is related to field of education. EDM is the process of transforming the raw data aggregated by education systems.
Educational data mining means exploring hidden data that originated from educational settings by using new methods for better interpretation of students and settings they learnt. Educational data mining promote distinct tools and algorithms for analyze the data patterns. In EDM, data is accumulated during learning process and then study can be done with the techniques from statistics, machine learning and other data mining concepts. To extract the hidden knowledge from data came from educational system, the various data mining techniques like classification, clustering, rule mining etc.

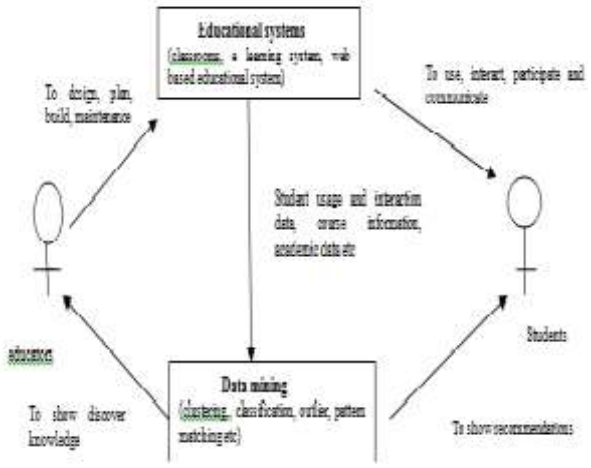


Figure 1

In figure 1 we represent the need of educational data mining. The Academics' responsible and educators worked upon the educational system to enhance the performance of students. In this diagram it is shown that educators want to design the educational system then plan to build that system and most important maintain that educational system. Educational systems include traditional classrooms and some innovative learning methods like e learning system, intelligent and adaptive web based educational system etc. The data set can be extracted from students as students are directly connected with educational system. Now the data is given as input to data mining process and in result it gives recommendations to students and to extract new knowledge to the educators by using various data mining techniques like clustering, classification, pattern matching etc.

2.1 Goals of Educational data mining:

Some of the goals of educational data mining are as follows:

1. Prediction of student's learning behavior by building student models that integrate all definite information of

students like student's knowledge, behavior, academic information etc.

2. Exploring or upgrading domain models that discriminate the content to be learnt and perfect pedagogical sequences.
3. Analysis of all the effects of various types of instructional support given by learning.
4. Advancing scientific knowledge.

2.2 Phases of Educational data mining:

Educational data mining is concerned with translation of new hidden information from the raw data collected from educational systems. EDM generally consist of four phases:

1. The first phase of educational data mining is to find the relationships between data of educational environment. The aim of establishing these relationships is to utilize these relationships in various data mining techniques like classification, clustering, regression etc.
2. The second phase of educational data mining is validation of discovered relationships between data so that over fitting can be avoided.
3. The third phase is to make predictions for future on the basis of validated relationships in learning environment.
4. The fourth phase is supporting decision making process with the help of predictions.

2.3 Methods of Educational data mining

There are so many promoted methods of educational data mining but all kind of methods lie in one of following specified categories:

1. **Prediction**: Ryan S. J. d. Baker has given a detail explanation of prediction in his paper. He mentioned that " In prediction, the goal is to develop a model which can infer a single aspect of data(predicted variable) from some combination of other aspects of data (predictor variables).if we study prediction extensively then we get three types of prediction: classification, regression and density estimation. In any category of prediction the input variables will be either categorical or continuous. In case of classification, the categorical or binary variables are used, but in regression continuous input variables are used. Density estimation can be done with the help of various kernel functions.

2. **Clustering**: In clustering technique, the data set is divided in various groups, known as clusters. When data set is already specified, then the clustering is more useful. As per clustering phenomenon, the data point of one cluster and should be more similar to other data points of same cluster and more dissimilar to data points of another cluster. There are two ways of initiation of clustering algorithm. Firstly, start the clustering algorithm with no prior assumption and second is to start clustering algorithm with a prior postulate.

3. **Relationship Mining**: Relationship mining generally refers to contrive new relationships between variables. It can be done on a large data set, having a no of variables. Relationship mining is an attempt to discover the variable which is most closely associated with the specified variable. There are four types of relationship mining: association rule mining, correlation mining, sequential pattern mining and causal data mining. Association data mining is based on if- then rule that is if some particular set of variable value appears then it generally have a specified value. In correlation mining, the linear correlations are discovered between variables. The aim of sequential pattern mining is to extract temporal relationships between variables.

4. **Discovery with Models:** it includes the designing of model based on some concepts like prediction, clustering and knowledge engineering etc. This newly created model's predictions are used to discover a new predicted variable.

5. **Distillation of Data for Human Judgment**: There are two objectives for human judgment for which distillation of data can be done: Identification and Classification. As per phenomenon of identification, data is represented in a way that human can easily recognize the well specified patterns.

3. LITERATURE SURVEY

3.1. Efficiency of decision trees in predicting student's academic performance

In this paper, S. Anupama Kumar et.al has suggested an approach for predicting the student's performance in examination. They have used C4.5 (J48 in WEKA) to do the prediction analysis. In data collection, a slight modification has been done in defining the nominal values for the analysis of accuracy. As per need of system, data is preprocessed, and integer values are converted into nominal values and stored in .CSV format. After that it is converted to .ARFF format that is accessible to WEKA.

In this paper, the implementation of decision trees rules can be done by dividing the data into two groups. J48 made decision trees by using a set of training data and ID3does the same with the concept of information entropy. In decision tree the attribute for splitting at each node of tree is normalized information gain. The attribute having highest normalized information gain is chosen to make decision. This paper analyzes the accuracy of algorithm in two ways, the first is by comparing the result of tree with the original marks obtained by student and the second is comparing the ID3 and C4.5 algorithm in terms of efficiency.

3.2. Classification model of prediction for placement of students

In paper Ajay Kumar Pal has presented a new approach of classification to predict the placement of students. This approach provides the relations between academic records and placement of students. In this analysis, various classification algorithms are employed by using data mining tools like WEKA for study of student's academic records. In this approach the training algorithm uses a set of predefined attributes. The most widely used classification algorithms are, naïve Bayesian classification algorithm, multilayer perceptron and C4.5 tree. For the high dimensional inputs the naïve Bayesian classification is best technique. Multilayer perceptron is most suitable for vector attribute values for more than one class. Nowadays C4.5 is most popularly used

algorithms due its added features like supervising missing values, categorization of continuous attributes, pruning of decision trees etc.
For testing, the 10 fold cross validation is selected as this evaluation approach. Here, a no of tests are regulated for estimation of input variables: chi square test, information gain test and gain ratio test. Each of the tests makes the concernment of variable in another way. According to this analysis, among three selected best algorithms, the best algorithm is Naïve Bayes classification.

3.3. Study of factors analysis affecting academic achievement of undergraduate students in international program

In this paper, Pimpa Cheewaprakobkit has done analysis to identify the weak students so that the academic performance of those weak students can be improved. In this study, WEKA open source data mining tool is used to estimate aspects for predicting the student's academic performance. In this study , data set to characterize classifier(decision tree, neural network). To predict the accuracy, a cross validation with 10 folds is used.
In this study, to explore the proposal, two classification algorithms have been accepted and distinguished: The Neural Network and C4.5 decision tree algorithm. The investigation process consists of three main steps: data preprocessing, attribute filtering and classification rules. According to this analysis, it is suggested the decision tree model is more accurate than the neural network model. It can be concluded that the decision tree technique has better efficiency data classification for this data set.

3.4. Predicting student's performance using modified ID3 algorithm

Ramanathan L. has overcome the shortcoming of famous algorithm ID3. This algorithm is used to generate the decision trees. In this analysis, instead of information gain, the gain ratio is used. One additional aspect of this study is assignment of weights to each attribute at every decision point. In this paper, in place of traditional ID3 algorithm, a modified ID3 algorithm is used. This modified ID3 algorithm is known as weighted ID3 algorithm. To enhance the normalization, gain ration is more beneficial as compared to information gain. To get a new value, gain ratio is multiplied with the weight and among these new values, the attribute having maximum gain ratio will be elected as node of the tree. Here, WEKA tool is used to analyze the J48 and naïve Bayes algorithm. The modified weighted ID3 algorithm is based on gain ratio and the attributes should be converted by accounting its weight. As per analysis, it is concluded that WID3 algorithm is more efficient than other two algorithms J48 and Naïve Bayes algorithm.

3.5. Analysis and predictions on student's behavior using decision trees in WEKA environment

In this paper, Vasile Paul Bresfelean has worked on data accumulated by different surveys. it is necessary to identify the different conducts of the student's belonging to different specializations. In this paper, the author develops a progression of decision trees based on WEKA's implemented J48 algorithm. In this effort, to discriminate and predict the student's choice in continuing their education. WEKA workbenches applied in this research two of the most common decision tree algorithms are implemented: ID3 and C4.5 (called version J48). In this study, author used J48 because as compared to ID3, J48 gives better result in any circumstances.

Comparison Table

Paper	Author	Technology used	Accuracy	Advantage	Disadvantage
Analysis and predictions on students behavior using decision trees in WEKA envirnment	Vasile Paul Bresfelean	Decision tree construction algorithm: ID3 and C4.5	In IE: 88.68% In CIG: 71.74%	-	-
Classification model of prediction for placement of students	Ajay kumar pal	Classification algorithm: 1.Naive Bayesian classification 2.Multilayer perceptron 3. C4.5 tree Tool: WEKA	1.Naïve Bayesian classification: 86.15 2.Multilayer perceptron: 80.00 J48: 75.38	-	-
Predicting student's performance using modified ID3 algorithm	Ramnathan L., Sakhsham Dhandha, Suresh kumar	J48 and Naïve Bayesian classification algorithms Tool:WEKA	ID3: 93% J48: 78.6% Naïve bayes classifiers: 75%	Shortcoming of ID3 is removed. Gain ration is used instead of information gain	It is inclined towards the attributes with more vales.
Efficiency of decision trees in predicting student's academic	S. Anupama kumar Dr. vijaylaxmi	ID3 and C4.5 algorithm J48	ID3: PASS: 103 FAIL: 12	-	-

performance			J48: PASS: 103 FAIL: 13		
Study of factors analysis affecting academic achievement of undergraduate students in international program	Pimpa cheewaprakobkit	Classifiers: Decision tree Neural network	Decision tree model: 85.188% Neural network model: 83.875%	-	-

5. CONCLUSION:

This paper described about the Educational data mining, goals of educational data mining and phases of educational data mining and existing classification techniques. Various classification techniques can be implemented on the data set but which classification technique will be applied on the data to improve the academic performance of students, it is important. In this paper, we made a comparison analysis on different existing approaches and methods of classification of data sets. We did the comparative analysis on the basis of accuracy percentage on the application of various classification techniques like Naïve Bayesian Classification, Multilayer Perceptron, J48 and ID3 etc. we also analyzed the advantages and shortcomings of each algorithm applied to data set. So we can say that this paper will provide a beneficial glance of existing solution for classification with their advantages and shortcomings.

6. REFERENCES

[1] Kumar S. Anupama and N. vijaylaxmi M.2011 Efficiency of Decision trees in predicting Student's Acedemic performance.

[2] L. Ramanathan, Dhanda S. and D. S. kumar 2013 Predicting Student's Performance using Modified ID3 Algorithm

[3] Pal A. kumar and Pal S. 2013 Classification Model of Prediction for Placement of Students

[4] Cheewaprakobkit P.2013 Study of Factors Analysis Affecting Academic Achievement of Undergraduate Students in International Program

[5] Bresfelean V. Paul 2007 Analysis and Predictions on Student's Behaviour using Decision Trees in Weka Environment Babes Bolyai University

[6] Baker Ryan S.J.d. Data mining for education Carnegie Mellon University

International Journal of Computer Applications Technology and Research
Volume 3– Issue 11, 729 - 733, 2014

Application of a Novel Software Algorithm for Information Reduction in High Frame Rate Ultrasonography

J. Jean Rossario Raj
Centre in Bio-Medical Engineering, Indian Institute of Technology –Delhi
India

S.M.K Rahman
Centre in Bio-Medical Engineering, Indian Institute of Technology –Delhi
India

Sneh Anand
Centre in Bio-Medical Engineering, Indian Institute of Technology –Delhi
India

Abstract: Ultrasonography is a non invasive method in medical field and is generally used for imaging the abnormal tissue growth. The tissue growth can be benign or malignant and to diagnose the quality of the tissue growth based on the stiffness is a challenge. Orthogonal wave velocity is computed by observing the orthogonal wave propagation in determining the stiffness of a tissue in Ultrasound Transient Elasticity. This requires an ultra-fast scanner which works at frame rates more than 1000 fps. The major difficulty is in collecting huge amount of scanner information and process in the processing system. Hence the designs are very complex and costly. Sliding rectangle algorithm is an innovative approach used in extracting the needed information in measuring the orthogonal wave velocity from successive matrix arrays. In this approach, one image matrix array is integrated into multiple rectangles and in a multi matrix array period, only one rectangle is sent and balance rectangles are discarded. This rectangle is moved multi matrix array to multi matrix array. This information is super imposed on full matrix array information. The orthogonal wave speed is calculated rectangle by rectangle. This algorithm reduces the amount of information sent to the processing system. This will enable the information from the scanner to be ported to Laptops in processing through standard interfaces such as USB or Ethernet in DICOM format. This makes the transient elasticity technology viable to be used in tele-medical field applications.

Keywords: Transient Elasticity, Orthogonal modulus, orthogonal wave velocity, Ultra-fast Scanner, Sliding Rectangle Algorithm, Ethernet, DICOM, Tele-medical field

1. INTRODUCTION

Elasticity measurement is a method used in the computation of tissue stiffness. Elasticity is the natural characteristic of a solid substance which comes back to its original contour after the stress caused by the external forces which caused it distort is taken out. The strain is the relative amount of deformation. The application of ultrasound elasticity in clinical applications is given in [1].

Orthogonal modulus computation using orthogonal wave velocity is given by the equation, $E = 3\rho c^2$where ρ is the density of the tissue. If orthogonal wave velocity is measured, elasticity can be evaluated.

In transient elasticity, low frequency orthogonal waves are induced. The orthogonal wave velocity is measured by cross correlation of the orthogonal wave propagation between the adjacent matrix arrays. Such a method is able to diagnose the tissue growths in a qualitative manner. However in such a qualitative measurement, the precision of the instrument depends upon the distance between adjacent matrix arrays. Though low-frequency orthogonal waves propagate at a low speed of a few m/s in soft tissues, the matrix array rate of the detection system must be higher than 1000 frames/sec to be able to follow their propagation on mm scale [3]. With a frame rate of 800fps and orthogonal wave velocity of 5m/s, a precision of the order of 1mm can be achieved.

Matrix array Rate (FR) is calculated using the equation $\frac{C}{2 \times D \times N}$where C is the ultrasound speed (1540m/s in normal tissues), N is the No. of Scan Lines per frame and D is the Depth of Penetration of the ultrasound waves. Maximum frame Rate is achieved by making N = 1 i.e. all crystals are excited simultaneously.

In an ultrasound machine operating at an ultrasound frequency of 8MHz and a receiver sampling rate of say 24MSPS (Mega Samples Per Second) and an ADC resolution of 8bits, the per sensor channel information rate would be of the order of 192Mbps. The machine has to transfer all the information from all the matrix arrays of all the sensor channels. An ultrasound machine with 64 crystals probe would require around 12Gbps information rate to be transferred from the ultrasound scanner to the processing system. Moreover, receiving such huge amount of information and processing is also a challenge in portable low cost ultrasound machines.

The important considerations in a portable transient elasticity ultrasound machine are as follows. The information / image processing is done in a laptop. The interfacing of the machine with laptop is using standard interfaces such as USB or Ethernet. Standard DICOM interface is used. The scanned information sent from the ultrasound scanner to the laptop is of the order of around 50Mbps in reasonable processing and display in the laptop.

Tele-medical field applications require portable low cost machines which can be taken to remote village locations. The raw information with the selected information size and format or the retrieved video is possible to be sent to a remote location in tele-medical field applications. Peak throughput and TCP rectangle sizes are needed to be evaluated in optimum use of the resources [5]in a Tele-medical field application.

In resolving the above limitations, the output information rates are reduced. Gigabit Ethernet interface, makes it easy to

transfer and to view the images immediately on a laptop at a distance away [7]. But the maximum throughput from GE interface is only of the order of 650Mbps. Moreover the Ethernet interface of the Laptop also is needed to process the complete information. The sliding rectangle algorithm approach presented in this paper is in reducing the information rates without affecting the transient elasticity requirement of measurement of inter matrix array movements.

2. Materials &Methods

2.1 Information Transfer Requirements

In the experimental setup, 32 sensor channels of Transmitter and Receiver are used. The information received from the ADC's are temporarily stored in the RAM available in the field programmable gated array. In the planned ultrasound scanner working at 8MHz, sampling frequency of 24MSPS, ADC resolution of 8bits per sample and PRF of 8 kHz, 3000 bytes of information is to be written per sensor channel. This corresponds to an information rate of 6144 Mbps. In order to reduce the information rates, first an information compression method of peak detection of consecutive 8 samples is carried out. This achieves a compression level of 8 i.e. 375 bytes of information are stored per sensor channel. The information compression reduces the per sensor channel information rates to 24Mbps.Thus in 32 sensor channels, 768Mbps of information is to be transferred. With the additional Ethernet, IP and UDP overheads, the information rates would become around 1Gbps. The planned Sliding Rectangle Algorithm in this paper further reduces the information rates to 45Mbps. This requires 32 Blocks of 375 Bytes RAM storage in the field programmable gated array. With a bus width of 16 Bits, one Block RAM can simultaneously store two sensor channels. Thus 16 Block RAM's of 375 Bytes length would be needed in storing one matrix array of information.

Two separate RAM areas are planned in the read and write operations such that while one matrix array is written into one RAM area, previous matrix array will be read and transferred via Ethernet from the second RAM area. The Ethernet Matrix array is created by the field programmable gated array by multiplexing the information sensor channels and the matrix array bytes of the Ethernet Matrix array, IP/UDP packets. The UDP Source/destination port 104 – Digital Imaging and Communication in Medicine [DICOM] is used as a standard interface protocol.

2.2 Choosing the field programmable gated array

In logic emulation systems the Field Programmable Gate Array (FPGA) provides faster computation as compared to software model. The logic designs are customized in high performance in different types of applications. In multimode system, the field programmable gated array yield significant hardware savings and provides generic hardware in [13]. In order to meet such requirements, Xilinx field programmable gated array with the following specifications is chosen. This device has 172 input/output(I/O Pins), 216K Block RAM, LVDS (Low Voltage Differential Signaling) interface is used in interfacing with High voltage pulsar and the Receiver chips, 622Mbps speed of the IO Bus and EEPROM/Master-Slave/JTAG Programming Headers.

2.3 Sliding Rectangle Algorithm

Even though the transient elasticity ultrasound scanner do not possess any limitations in sending the information at these high information rates, the laptops available do not have enough processing capacity in wire rate reception of information at these rates. The main motivation of development of this technique is to reduce the information rate throughput in processing so that the processing can be done in standard hardware such as Laptops. With an ultrasound frequency of f, sampling rate of S, bits per sample as b and number of sensor channels as n, the output information rates typically shall be s*b*n. This information rate is of the order of 1Gbps in the planned system.

Hence an information/image matrix array is integrated into multiple rectangles say 'w' using an algorithm planned in this paper as sliding rectangle algorithm. In this case a w of 23 is taken i.e. the information matrix array matrix is integrated into 23 rectangles and selective rectangles are only transmitted. However in practical implementations, these values and requirements can vary and sufficient flexibility in the methodology can be achieved in choosing the right combinations. Thus the effective information rate is reduced to around 45Mbps. The Sliding rectangle Algorithm is executed in the field programmable gated array.

In the first time, in few matrix arrays, each rectangle is sent one after the other in the low matrix array rate in the MATLAB video reconstruction algorithm to synchronize and reconstruct the full image. Subsequently, the field programmable gated array repeats the first matrix array in 'm' times and discards the balance rectangles before sliding to the second rectangle and so on. This method of repeating the same rectangle 'm' times at the requisite high matrix array rate ensures the measurement of matrix array to matrix array displacement and orthogonal wave velocity without any difficulty. The bottom line is that the used techniques should not hammer the matrix array to matrix array displacement and velocity measurements. In the experimental setup the value of m is taken as 256.

2.4 Sliding Rectangle Algorithm Flow Chart

The flow chart of the receive field programmable gated array in the implementation of Sliding Rectangle Algorithm is shown in the figure-1 below.

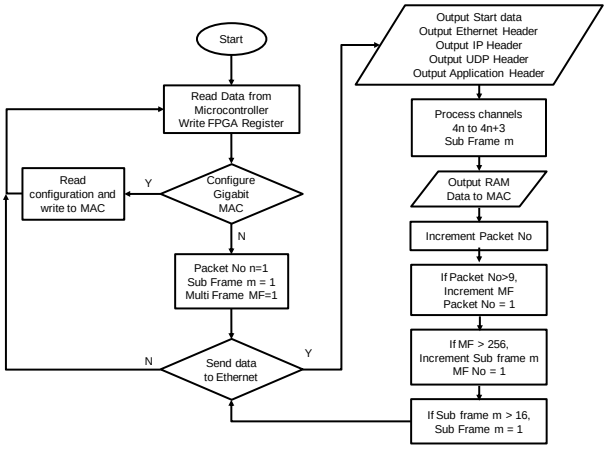


Figure-1: Receive field programmable gated array software algorithm flow chart

In the experimental setup described in this paper, 368 Bytes of information per sensor channel is read out of the field programmable gated array through the Ethernet port. The 368 Bytes are integrated into 23 rectangles. I.e. each rectangle comprises of 16 bytes per sensor channel or 16 x 32 Bytes per ultrasound matrix array. During one write sequence to the

field programmable gated array, only one rectangle of 16 x 32 bytes is transferred to the laptop and balance information is discarded. A multi matrix array consists of 256 such sub matrix arrays where in only the first matrix array is only read. Once one multi matrix array is read, it moves on to read the next rectangle and so on. This algorithm reduced the effective output information rate by 23. This also ensured that the high matrix array rate is retained so that the measurement of matrix array to matrix array displacement and hence the transient wave velocity is not affected.

Video reconstruction algorithm in MATLAB does intelligent algorithm. Based on the initial consecutive rectangles, the first image is reconstructed. Subsequent matrix arrays are superimposed on the initial matrix array. In enabling this arrangement of rectangles and matrix arrays, the rectangle id and matrix array id are sent along with the packet in the UDP payload. The rectangle matrix is superimposed on the complete matrix array matrix and image is displayed. Since motion detection calculates the difference between the matrix arrays, orthogonal wave motion is detected in the sliding sector.

3. IMPLEMENTATION & MODEL

3.1 General Working Procedure

The Tx field programmable gated array generates the Transmit pulses at 8MHz and at a PRF of 8kHz in all the sensor channels.8 Sensor channel High Voltage Pulser consists of logic interfaces and amplifies the digital pulses generated by the field programmable gated array in exciting the piezo electric crystals located in the Ultrasound transducer probe. The 8 sensor channel receiver has LNA to amplify the low level receive data received from the piezoelectric crystals, TGC in Time Gain Compensation, AAF – the Anti Aliasing Filter and the ADC which performs the Analog to Digital Conversion. TGC implementation in ultrasound, see [18].

The Receive field programmable gated array has sufficient I/O Buses in interfacing with the ADC's, Ethernet MAC and the Microcontroller as given in the Figure-2 below. Serial Peripheral Interface [SPI] programming infield programmable gated array, see [9]

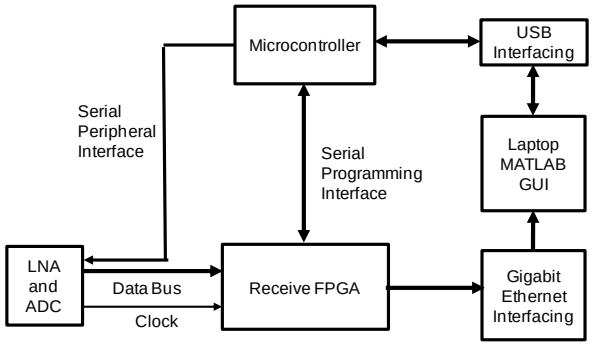


Figure-2: Block schematic of the Receive portion of Ultrasound Scanner

3.2 Storing the receive information in the field programmable gated array RAM using two information banks

The LNA supplies two clocks FCO and DCO in synchronizing and reading the information by the field programmable gated array LVDS Receiver. Various clocks needed in receiving and processing of the information is generated in the field programmable gated array. The internal RAM of the field programmable gated array acts as the temporary storage of the scanned information. The receive information is converted into serial to parallel stream and stored in the field programmable gated array Block RAM. Two Block RAMs of the field programmable gated array are used in writing the alternate matrix array of information. Thus the field programmable gated array requires two information banks, which will be switched between the write and read operations. The interface logic is embedded in Field Programmable Gate Array and therefore the field programmable gated array includes both user logic and interface logic [11].

Likewise all the 32 sensor channels of receive information are written into the information banks. 375 Bytes per sensor channel is stored in the field programmable gated array information bank.

3.3 Storing Overhead information infield programmable gated array Registers

The overhead information in the Ethernet Matrix array, IP Packet and UDP information are stored in the field programmable gated array Registers. Some of these information values are fixed values where as some of the values like source, destination IP addresses etc are assigned by the Microcontroller. The Microcontroller in turn is programmed from the MATLAB graphical user interface through the USB interface as shown in Figure-2.

3.4 Field programmable gated array Receive Packet Information Architecture

The field programmable gated array receive packet formation system architecture uses the Sliding rectangle algorithm. The information header generated by the field programmable gated array contains the MAC Information write start bytes, Ethernet header Information, IP Header Information and the UDP Header Information. After sending the information headers, the information from any one of the field programmable gated array RAM information bank is read using the Sliding Rectangle Algorithm. On completion of the information read, the MAC information write stop bytes are sent which will enable the MAC to send the complete packet to the Ethernet interface. This is given in Figure-3 below.

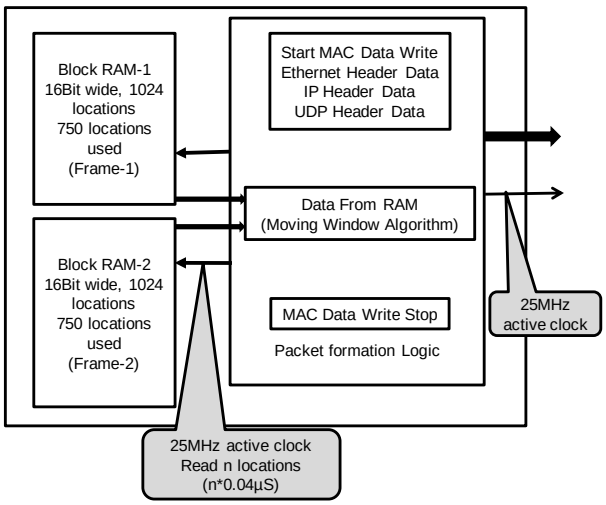


Figure-3: Receive field programmable gated array logical block schematic

The pipelined architecture of the Field Programmable Gate Array and the distributed Random Access Memory in high

I/O resources of an image classifier implementing object classification stages in object detection system is discussed in [15].

Some of the header bytes like the checksum etc are written into the Ethernet matrix array by the Gigabit Ethernet MAC chip. All other headers are written through the microcontroller into the field programmable gated array registers. The Gigabit MAC chip also requires the start and stop bytes from the field programmable gated array. A counter is used in sending the information sequentially in the order of start bits, Ethernet header, IP header, UDP header, Application header, Information from the block RAM, Ethernet end of matrix array and stop bits. The information is transferred at very high speeds to the Gigabit Ethernet MAC chip.

Gigabit Ethernet controller maintains full duplex operation with 1000Mbps information Rate, High-performance non-PCI local bus, EEPROM interface and 16/32-bit SRAM-like host interface. It does the Ethernet framing of the information and inserts the IP and UDP header checksums. Physical Layer (PHY) devices maintain 1000BASE-T standards in full-duplex mode, and maintain the RGMII interface operating at 125MHz towards the Gigabit Ethernet controller. It carries out the Physical layer level translations and conversions to Gigabit Ethernet speeds over copper interface.

The information processing and image processing is carried out in the MATLAB based graphical user interface. The device configurations are controlled from the graphical user interface through a microcontroller in the Ultrasound board.

3.5 Model Results

The model results of various waveforms of host clock, RAM enable clocks etc can be seen in the figure-4 below. The various clocks generated by the field programmable gated array including the RAM read clocks from different information banks are seen in the figure.

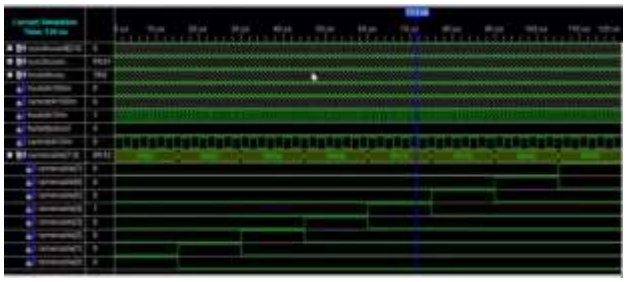
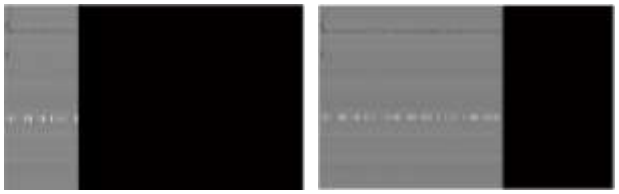


Figure-4: Model results during the design phase using field programmable gated array

4. RESULTS

The image reconstruction using the sliding rectangle in a MATLAB graphical user interface is given in the Figure-5. The image is progressively getting reconstructed in this method. The final image can be seen in Figure-6.



(a) (b)

Figure-5: Sliding rectangle Algorithm display in MATLAB graphical user interface with (a) 4 and (b) 10 Rectangles

Figure-6: Final acquired image after the sliding rectangle algorithm on a homogeneous medium used as phantom

Further, the displacement of the propagating orthogonal wave is measured as a function of time and space in [18] using MATLAB based algorithms.

Transient elasticity measurements require the cross correlation measurements between successive matrix arrays which are sliding at matrix array rates of the order of 1000fps.In this method, one rectangle is continuously transmitted in say256 matrix arrays. Hence the velocity of propagation of the orthogonal waves can be measured within the rectangle using the existing methods. This method is repeated in successive rectangles and the resultant velocity graph is combined to get expected results. The arrival time envelope satisfies the Eikonal equation. The distance method is used to solve the inverse Eikonal equation given the arrival times of a propagating wave, to find the wave speed [17].

5. DISCUSSION AND CONCLUSION

In observing the orthogonal wave propagation and to compute the orthogonal modulus, an ultrafast scanner is needed which works at matrix array rates more than 1000 fps. Such ultrasound machines are needed to collect huge amount of scanner information and process the same in the processing system. This makes their design very complicate and expensive. Hence the algorithm helps.

Through this paper, a new algorithm named Sliding rectangle algorithm is introduced which is found to be an innovative approach by extracting the needed information in measuring the orthogonal wave velocity from successive matrix arrays.

In this approach, one image matrix array is integrated into multiple rectangles say 16 and in a multi matrix array period, only one rectangle is sent and balance rectangles are discarded. This rectangle is moved multi matrix array to multi matrix array. This information is super imposed on full matrix array information. The orthogonal wave speed is calculated rectangle by rectangle. This algorithm reduces the amount of information sent to the processing system. This will enable the information from the scanner could be ported to Laptops in processing through standard interfaces such as USB or Ethernet. This makes the transient elasticity technology viable to be used in tele-medical field applications.

6. ACKNOWLEDGEMENTS

This work was maintained in part by the Department of Science and Technology, Government of India.

7. REFERENCES

[1] Elisa E. Konofagou, Jonathan Ophir, Thomas A. Krouskop and Brian S. “Elastography: from theory to clinical applications Garra”, Focused Ultrasound Laboratory, Department of Radiology, Brigham and Women's Hospital - Harvard Medical School, Boston, MA, 2003 Summer Bioengineering Conference, June 25-29, Sonesta Beach Resort in Key Biscayne, Florida

[2] S. Park, S. R. Aglyamov, and S. Y. Emelianov, "Beam forming for photo acoustic imaging using linear array transducer," Proceedings of IEEE Ultrasonic Symposium, pp. 856-859, 2007

[3] J. Bercoff,* S. Chaffai,* M. Tanter,* L. Sandrin,* S. Catheline,* M. Fink*, J. L. Gennisson* And M. Meunier†, In Vivo Breast tumor Detection Using Transient Elastography, *LaboratoireOndes et Acoustique, E.S.P.C.I., Universite´ Paris VII, U.M.R. 7587 C.N.R.S 1503, Paris, France; and †Institut Curie, Service de Radio diagnostique, Paris, France, Ultrasound in Med. & Biol., Vol. 29, No. 10, pp. 1387–1396, 2003

[4] R. J. Zemp, R. Bitton, M. L. Li, K. K. Shung, G. Stoica, and L. V. Wang,"Photoacoustic imaging of the microvasculature with a high-frequency ultrasound array transducer," JBO Letters, vol. 12, pp. 0105011-3, 2007.

[5] Optimization of wide-area ATM and local-Area Ethernet/FDDI network configurations for high-speed telemedicine communications employing NASA's ACTS McDermott, W.R. ; Maya Found., USA ; Tri, J.L. ; Mitchell, M.P. ; Levens, S.P. Published in: Network, IEEE (Volume:13 , Issue: 4) doi: 10.1109/65.777439

[6] C. K. Liao, M. L. Li, and P. C. Li, "Optoacoustic imaging with synthetic aperture focusing and cohehrence weighting," Optics Letters, vol. 29, pp. 2506-2508,2004.

[7] Zentai, G.; Partain, L., "Development of a high resolution, portable x-ray imager for security applications," Imaging Systems and Techniques, 2007. IST '07. IEEE International Workshop on , vol., no., pp.1,5, 5-5 May 2007 doi: 10.1109/IST.2007.379590

[8] K. W. Hollman, K. W. Rigby, and M. O'Donnell, "Coherence factor of speckle from a multi-row probe," Proceedings of IEEE Ultrasononic Symposium, pp.1257-1260, 1999

[9] Trupti D. Shingare, R. T. Patil, “SPI Implementation on FPGA”, International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075, Volume-2, Issue-2, January 2013

[10] K. E. Thomenius, "Evolution of ultrasound beamformers," Proceedings of IEEE Ultrasonic Symposium, pp. 1615-1622, 1996

[11] A design of embedded Gigabit Ethernet interface, Li Mingwei Electron. Eng. Dept., Dalian Univ. of Technol., Dalian, China, Li Yanxia ; HuYanguo; IEEE International Conference on Mechanic Automation and Control Engineering (MACE), 2010; IEEE 10.1109/MACE.2010.5535339

[12] S. Krishnan, K. W. Rigby, and M. O'Donnell, "Efficient parallel adaptive aberration correction," IEEE Transactions on Ultrasonics, Ferroelectrics, andFrequency Control, vol. 45, pp. 691-703, 1998

[13] Hauck, S., "The roles of FPGAs in reprogrammable systems," Proceedings of the IEEE , vol.86, no.4, pp.615,638, Apr 1998 doi: 10.1109/5.663540

[14] P. C. Li and M. L. Li, "Adaptive imaging using the generalized coherence factor,"IEEE Transactions on Ultrasonics, Ferroelectrics, and Frequency Control, vol.50, pp. 128-141, 2003

[15] McCurry, P.; Morgan, F.; Kilmartin, L., "Xilinx FPGA implementation of an image classifier for object detection applications," Image Processing, 2001. Proceedings. 2001 International Conference on , vol.3, no., pp.346,349 vol.3, 2001, doi: 10.1109/ICIP.2001.958122

[16] M. L. Li, H. F. Zhang, and K. Maslov, "Improved in vivo photoacoustic microscopy based on a virtual-detector concept," Optics Letters, vol. 31, pp. 474-476, 2006.

[17] Joyce McLaughlin and Daniel Renzi; “Shear wave speed recovery in transient Elastography and supersonic imaging using propagating fronts”; Institute of Physics Publishing; Published 27 March 2006 Online atstacks.iop.org/IP/22/681

[18] Mingwang Tang; FeiLuo; Dong Liu, "Automatic Time Gain Compensation in Ultrasound Imaging System," Bioininmatics and Biomedical Engineering, 2009. ICBBE 2009. 3rd International Conference on , vol., no., pp.1,4, 11-13 June 2009 doi: 10.1109/ICBBE.2009.5162432

[19] M. Xu and L. V. Wang, "Photo acoustic imaging in biomedicine," Review of Scientific Instruments, vol. 77, pp. 0411011-22, 2006.

[20] T. J. Shan and T. Kailath, "Adaptive beam forming for coherent signals and interferences," IEEE Transactions on Acoustics, Speech, and Signal Processing vol. 33, pp. 527-536, 1985.

International Journal of Computer Applications Technology and Research
Volume 3– Issue 11, 734 - 736, 2014

Authenticating Location Based Skyline Queries in Mobile Environment

A.Sethupathi
Computer Science and Engineering
V.S.B Engineering College
Karur, India

A.P.V Raghavendra
Computer Science and Engineering
V.S.B Engineering College
Karur, India

Abstract: With the booming of Smartphone's and mobile devices, location-based services have experienced massive escalation in nowadays. The outsourcing data processing services to cloud service provider becomes very trending in recent years, which provides solution to the clients instead of data owner. However, we cannot expect real solutions from the data processing services; it may give dishonest results to the clients. Therefore, to provide the correct results some authentication techniques are requiring. In this paper, we learn the authentication techniques for location-based arbitrary-subspace skyline queries (LASQs), which signify an essential class of LBS applications. We suggest a basic Merkle Skyline R-tree method and a novel Partial S4-tree method to authenticate LASQs. For authentication process using this LASQ, the client can contact server frequently during movement and also verify the results by client itself.

Keywords: location based services, outsourcing data management, cloud service provider, Merkle Skyline R-tree, novel Partial S4-tree

1 INTRODUCTION

With the rapid development of mobile handset devices (such as smartphones and tablet computers), wireless communication, and positioning technologies in the past decade, Location-based services (LBSs) have prospered. Users carrying location-aware mobile devices are able to query LBSs for surrounding points of interest (POIs) anywhere and at any time. Among the many types of location-based queries, one important class is *location-based skyline queries*. These queries take into account both the spatial and non-spatial attributes of the POIs A representative example is finding nearby restaurants with good food, where the distance to the querying user is a spatial attribute and the goodness of the food is a non spatial attribute. The query returns a set of restaurants that are closer to the querying user and/or have better food than those not returned. In general, while spatial objects can have a long list of non-spatial attributes—such as food quality, service, hygiene, environment, and price—only *a small subset* of these attributes (termed *a subspace*) is of interest to a particular user in a single query. Moreover, different users may have different preferences—e.g., Mary prefers taste, whereas Tom is concerned about hygiene, environment, and price. In this paper, we call these skyline queries location-based arbitrary-subspace skyline queries (LASQs).To scale up LBSs along with their ever-growing popularity, a rising trend is to outsource data management and service provisioning to Cloud service providers (CSPs) such as Amazon EC2 and Google App Engine .More specifically, a data owner delegates its data to a CSP, which in turn provides query services to clients on behalf of the data owner. While such an outsourcing model is advantageous in terms of cost, performance, and flexibility in resource management, it brings a great challenge to query integrity assurance If the CSP is untrustworthy or compromised, it may return incorrect or incomplete query results to clients (intentionally or not) for various reasons:

The CSP may return incorrect results unintentionally because of bugs in the implementation of query processing algorithms.

• The CSP (or the adversary who compromised it) may intentionally tamper with the query results. For example, in the restaurant-finding scenario mentioned above, a restaurant may be ranked higher than other restaurants just because the CSP is sponsored by that restaurant.
• To cut costs or avoid performance bottlenecks in peak hours, the CSP may return incomplete results by carrying out the query evaluation process partially.

Therefore, in the data-outsourcing model, there is a need for clients to authenticate the *soundness* and *completeness* of query results,1 where *soundness* means that the original data is not tampered with by any third party (including the CSP), and *completeness* means that no valid result is missing. This leads to a problem known as *authenticated query processing* which has been studied for various spatial queries, including range queries top-*k* queries *k*NN queries and shortest-path queries .

Fig. 1. Authenticated query processing.

Fig. 1 shows a general framework of authenticated query processing. The data owner obtains, through a certificate authority (e.g., VeriSign), a pair of private and public keys of digital signatures. Before delegating a spatial dataset to the CSP, the data owner builds an authenticated data structure (ADS) of the dataset. To support efficient query processing, the ADS is often a tree-like index structure, where the root is signed by the

data owner using his/her private key. The CSP keeps the spatial dataset, as well as the ADS and its root signature. Upon receiving a query from the client, the CSP returns the query results, the root signature, and a verification object (VO), which is constructed based on the ADS. The client can authenticate the correctness of the query results using the returned VO, the root signature, and the data owner's public key.

In a preliminary study we have investigated the authentication problem for location-based skyline queries in a fixed space of attributes. In this paper, we extend this study to the general problem of authenticating location based skyline queries in arbitrary subspaces of attributes (*i.e.*, LASQs). Because a basic solution that returns all results in the full space is inefficient, we propose a new authentication method based on the notion of *signed subspace skyline scope (S4)*. We devise a data structure, called *Partial-S4-tree*, which pre-computes, signs, and stores the skyline scopes of some subspaces, so that many redundant objects can be easily identified and safely removed from the VO, thereby minimizing its size and saving the server processing time. To improve the filtering effects, we further propose a storage-budget allocation policy to construct the Partial-S4-tree for each spatial object. For continuous LASQs, the concept of *clear area* is introduced to enable a moving client to re-evaluate new results locally. Moreover, we propose an approach to prolong the client's residence time inside a clear area.

In summary, our contributions in this paper are four-fold:
• We identify the problem of authenticating LASQs in outsourced databases. To the best of our knowledge, this study is the first attempt to investigate this problem.
• For a one-shot LASQ authentication, we propose a basic Merkle Skyline R-tree method and a Partial-S4-tree method, aiming to reduce the server processing time and minimize the VO size.
• We develop a prefetching-based approach for authenticating continuous LASQs. This approach enables the clients to re-evaluate new LASQ results locally during movement, thus reducing both communication and computation costs.
• We conduct extensive experiments to evaluate the performance of the proposed methods and algorithms.

2.RELATED WORK

In this section, we review the related work on query authentication and skyline query processing.

2.1 Query Authentication

Authenticated query processing has been studied extensively. Most studies on query authentication are based on an AD called Merkle Hash Tree (MH-tree) In MH-tree, the digests of index nodes are recursively computed from the leaf nodes to the root. After that, the root digest is signed by the data owner's private key and stored on the outsourced database server. For each user query, this signature is returned to the client along with the query results and a VO for result verification. In contrast, an alternative method is to employ signature aggregation, which signs every object in the dataset and generates a VO by aggregating the signatures of the result objects along with some non-result objects (*e.g.*, the objects immediately beyond a query range). However, as the aggregate signature is generated on-the-fly, this method incurs high overhead in query processing and client-side verification. Therefore, in this paper, we focus on authentication methods based on MH-tree.

Following the concept of MH-tree, the query authentication problem has been studied for relational databases data streams and text search engines Yang *et al*. first introduced this problem to the spatial database domain and studied the authentication of spatial range queries. They proposed an authenticated index structure called MR-tree, which combines the ideas of MB-tree and R*-tree Yiu *et al*. investigated how to efficiently authenticate kNN queries and shortest-path queries . In Hu *et al*. proposed a novel approach that authenticates spatial queries based on neighborhood information. More recently, in we developed new schemes for range and top-*k* query authentication that preserves the location privacy of queried objects.

In our preliminary studies, we investigated the authentication of location-based skyline queries in *fixed* subspaces. A new authenticated index structure called MRSky- tree (or MSR-tree) was proposed in . The main difference between MR-tree and MSR-tree is that the former indexes the spatial objects while the latter indexes the solution space of spatial objects (in form of a notion called skyline scope.

2.2 Skyline Query Processing

Skyline query processing was first introduced into the database community by Borzonyi *et al.*[4]. A number of algorithms have been developed since then. These algorithms can be divided into two categories. The first category is non-index-based algorithms. The representatives are Black-Nested-Loop (BNL) and Divide-and-Conquer (D&C). BNL scans the dataset sequentially and compares each new object to the skyline candidates obtained so far. D&C partitions the dataset into several parts, processes them part by part, and finally merges all partial skylines.SFS improves BNL by pre-sorting the dataset. In the Bitmap approach , each data point is encoded in a bit string and the skyline is computed on the bit matrix of all data points.

3. LASQ AUTHENTICATION METHOD

In this section, we propose a basic LASQ authentication method. We start with the authentication problem in a fixed subspace, and then extend it to arbitrary subspaces

3.1 LASQ Authentication

3.1.1 Design of Authenticated Index Structure. To expedite query processing, we index all the objects' subspace skyline scopes by an R*-tree , where the subspace skyline scopes are stored in the leaf nodes as data entries. Additionally, to support query authentication, we follow similar ideas of MB-tree and MR-tree to maintain a series of digests for all index nodes in the tree structure.

3.1.2 Server Query Processing and VO Construction. With the help of MSR-tree, an LASQ is reduced to a point-location

query on the indexed subspace skyline scopes. Specifically, starting from the root and going all the way down to the leaf nodes, the server checks whether any child of a node covers the query point. If it does, the node is *unfolded* and inserted into the VO for further checking; otherwise, the node is *pruned* and only its MBR and digest are inserted into the final VO. When visiting a leaf entry associated with an object *o*, if the corresponding S_o does not cover the query point, both S_o and H_o should be inserted into the VO; otherwise, *o* is an LASQ result and only S_o is inserted into the VO (H_o can be computed locally by the client based on the received result). It is noteworthy that as the nodes in the VO also form a tree structure, we call it a *VO-tree*. In general, a VO-tree contains four types of data:

1) the subspace skyline scopes of all objects in the visited leaf nodes;
2) the digests of non-result objects in the visited leaf nodes;
3) the MBRs of all visited non-leaf entries;
4)the digests of the pruned index nodes.

3.1.3 Client Result Verification. The VO-tree and the root signature ($Sig(H_{root})$), along with the skyline results, are sent to the client after query processing. To verify the correctness of the results, the client checks the following three conditions:

1) the subspace skyline scopes of all result objects should cover the query point *q*;
2) no MBRs of the pruned index nodes and no subspace skyline scopes of the non-result objects cover *q*;
3) the root signature matches the root digest computed from the VO-tree.

4 CONCLUSION

In this paper, we have studied the problem of authenticating location-based skyline queries in arbitrary subspaces (LASQs). We have proposed a basic MSR-tree authentication method by extending our previous work on skyline query authentication. To enable authentication for large scale datasets and subspaces, we have further proposed a Partial-S4-tree method, in which most of the redundant objects can be easily identified and filtered out from the VO. For authenticating continuous LASQs, we have proposed a prefetching-based solution to avoid frequent query issuances and VO transmissions. Extensive experimental results demonstrate the efficiency of our proposed methods and algorithms under various system settings. In particular, our proposed Partial-S4-tree method outperforms the basic authentication method by up to 69% in terms of the overall query latency and up to 74% in terms of the VO size.

5. FUTURE WORK

As for the future work, we will extend this work to road network environments. Since the query distance is defined by network distance in a road network, the skyline scope defined in this paper no longer works, which calls for new authentication methods. Moreover, we are also interested in studying the authentication problem for dynamic objects, where how to guarantee the freshness of query results is a very challenging issue .

6. REFERENCES

[1] (2011) AT&T to Launch Cloud-Based LBS Mobility Data Offering [Online]. Available:http://www.mobilecommercedaily.com/2011/01/06/att-to-launch-cloud-based-lbs-mobility-data-offering.

[2] N. Beckmann, H.-P. Kriegel, R. Schneider, and B. Seeger, "The R*-tree: An efficient and robust access method for points and rectangles,"in *SIGMOD*, Atlantic City, NJ, USA, 1990, pp. 322–331.

[3] M. Berg, O. Cheong, and M. Kreveld, "*Computational Geometry: Algorithms and Applications*," 3rd ed., Berlin,Germany:Springer,2008, ch. 7.

[4] S. Borzonyi, D. Kossmann, and K. Stocker, "The Skyline operator,"in *Proc. ICDE*, Heidelberg, Germany, 2001, pp. 421–430.

[5] Q. Chen, H. Hu, and J. Xu, "Authenticating Top-k queries in location-based services with confidentiality," in *PVLDB*, Hangzhou, China, 2014.

[6] J. Chomicki, P. Godfrey, J. Gryz, and D. Liang, "Skyline with presorting," in *Proc. ICDE*, 2003.

[7] H. Hu, J. Xu, and D. L. Lee, "A generic framework for monitoring continuous spatial queries over moving objects," in SIGMOD, Baltimore, MD, USA, 2005.

[8] H. Hu, J. Xu, Q. Chen, and Z. Yang, "Authenticating locationbased services without compromising location privacy,"in SIGMOD, 2012.

[9] H. Hu, Q. Chen, and J. Xu. "VERDICT: Privacy-preserving authentication of range queries in location-based services," in ICDE, Brisbane, QLD, Australia, 2013 (Demo).

International Journal of Computer Applications Technology and Research
Volume 3– Issue 11, 737 - 744, 2014

Evasion Streamline Intruders Using Graph Based Attacker model Analysis and Counter measures In Cloud Environment

D.Usha Sree
Chiranjeevi Reddy Institute of Technology
Anantapuramu-51500,
Andhra Pradesh. India

S. Sravani
Chiranjeevi Reddy Institute of Technology
Anantapuramu-51500,
Andhra Pradesh.India

Abstract: Network Intrusion detection and Countermeasure Election in virtual network systems (NICE) are used to establish a defense-in-depth intrusion detection framework. For better attack detection, NICE incorporates attack graph analytical procedures into the intrusion detection processes. We must note that the design of NICE does not intend to improve any of the existing intrusion detection algorithms; indeed, NICE employs a reconfigurable virtual networking approach to detect and counter the attempts to compromise VMs, thus preventing zombie VMs. NICE includes two main phases: deploy a lightweight mirroring-based network intrusion detection agent (NICE-A) on each cloud server to capture and analyze cloud traffic. A NICE-A periodically scans the virtual system vulnerabilities within a cloud server to establish Scenario Attack Graph (SAGs), and then based on the severity of identified vulnerability toward the collaborative attack goals, NICE will decide whether or not to put a VM in network inspection state. Once a VM enters inspection state, Deep Packet Inspection (DPI) is applied, and/or virtual network reconfigurations can be deployed to the inspecting VM to make the potential attack behaviors prominent.

Keywords: NICE, Compromised Machines, spam zombies, Compromised Machine detection Algorithms Scenario Attack Grapg(SAGs)

1. INTRODUCTION

RECENT studies have shown that users migrating to the cloud consider security as the most important factor. A recent Cloud Security Alliance (CSA) [1] .Survey shows that among all security issues, abuse and nefarious use of cloud computing [2] is considered as the top security threat, in which attackers can exploit vulnerabilities in clouds and utilize cloud system resources to deploy attacks. In traditional data centers, where system administrators have full control over the host machines, vulnerabilities can be detected and patched by the system administrator in a centralized manner. However, patching known security [3] holes in cloud data centers, where cloud users usually have the privilege to control software installed on their managed VMs, may not work effectively and can violate the service level agreement (SLA). Furthermore, cloud users can install vulnerable software on their VMs, which essentially contributes to loopholes in cloud security [4]. The challenge is to establish an effective vulnerability/attack detection and response system for accurately identifying attacks and minimizing the impact of security breach to cloud users. Addressed that protecting "Business continuity and services availability" from service outages is one of the top concerns in cloud computing systems.

1.1 Motivation

NICE significantly advances the current network IDS/ IPS solutions by employing programmable virtual networking approach that allows the system to construct a dynamic reconfigurable IDS system. By using software switching techniques, NICE constructs a mirroring-based traffic capturing framework to minimize the interference on users' traffic compared to traditional bump-in-the-wire (i.e., proxy-based) IDS/IPS. The programmable virtual networking architecture of NICE enables the cloud to establish inspection and quarantine modes for suspicious VMs according to their current vulnerability state in the current SAG. Based on the collective behavior of VMs in the SAG, NICE can decide appropriate actions, for example, DPI or traffic filtering, on the suspicious VMs. Using this approach, NICE does not need to block traffic flows of a suspicious VM in its early attack stage.

1.2 Definitions

NICE is a new multiphase distributed network intrusion detection and prevention framework in a virtual networking environment that captures and inspects suspicious cloud traffic without interrupting users' applications and cloud services.

NICE incorporates a software switching solution to quarantine and inspect suspicious VMs for further investigation and protection. Through programmable network approaches, NICE can improve the attack detection probability and improve the resiliency to VM exploitation attack without interrupting existing normal cloud services.

NICE employs a novel attack graph approach for attack detection and prevention by correlating attack behavior and also suggests effective countermeasures.

NICE optimizes the implementation on cloud servers to minimize resource consumption. Our study shows that NICE consumes less computational overhead compared to proxy-based network intrusion detection solutions.

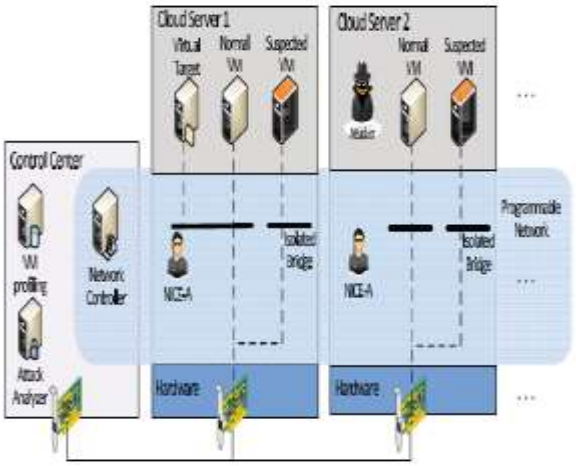


Figure 1.1: Architecture of intruders

2. PROBLEM STATEMENT

2.1 Existing System

Every day in data repositories many number of knowledgeable people are update the data. Data is increases here. Already existing data it can add in two or more number of databases. These kinds of data repositories are come under dirty repositories. Any user it can forward the query, extract and display the results here. Extraction results are contains useless data. Query shows much number of problems like high response amount of time, availability, quality assurance and security. Websites are not providing any useful services in extraction. These services are showing the problems in performance, quality and operational cost.

Previous existing system applies the data integration, data cleaning under record linkage and record matching. In record matching time and record linkage any duplicates are present removed here. Next previous approach near duplicate detection also remove some duplicates of data. These approaches are not gives any efficient solution in implementation. It cannot provide high quality data.

2.2 Proposed System

A recent Cloud Security Alliance (CSA) survey shows that among all security issues, abuse and nefarious use of cloud computing is considered as the top security threat, in which attackers can exploit vulnerabilities in clouds and utilize cloud system resources to deploy attacks. In traditional data centers, where system administrators have full control over the host machines, vulnerabilities can be detected and patched by the system administrator in a centralized manner. However, patching known security holes in cloud data centers, where cloud users usually have the privilege to control software installed on their managed VMs, may not work effectively and can violate the service level agreement (SLA). Furthermore, cloud users can install vulnerable software on their VMs, which essentially contributes to loopholes in cloud security.

In a cloud system, where the infrastructure is shared by potentially millions of users, abuse and nefarious use of the shared infrastructure benefits attackers to exploit vulnerabilities of the cloud and use its resource to deploy attacks [5] in more efficient ways. Such attacks are more effective in the cloud environment because cloud users usually share computing resources, e.g., being connected through the same switch, sharing with the same data storage and file systems, even with potential attackers. The similar setup for VMs in the cloud, e.g., virtualization techniques, VM OS, installed vulnerable software, networking, and so on, attracts attackers to compromise multiple *VMs.*

The evaluation is done by assigning to an individual a value that measures how suitable that individual is to the proposed problem. In our GP experimental environment, individuals are evaluated on how well they learn to predict good answers to a given problem, using the set of functions and terminals available. The resulting value is also called raw fitness and the evaluation functions are called fitness functions. Notice that after the evaluation step, each solution has a fitness value that measures how good or bad it is to the given problem. Thus, by using this value, it is possible to select which individuals should be in the next generation. Strategies for this selection may involve very simple or complex techniques, varying from just selecting the best n individuals to randomly selecting the individuals proportionally to their fitness.

3. METHODOLOGY

3.1 Cloud Components

A Cloud system consists of 3 major components such as clients, datacenter, and distributed servers. Each element has a definite purpose and plays a specific role.

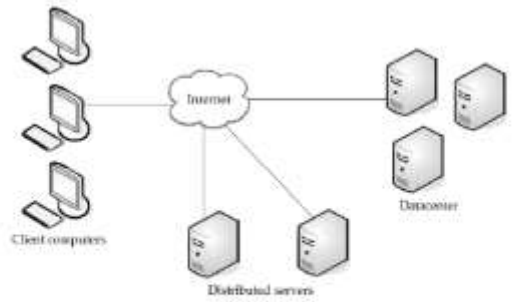


Figure 2: Three components make up a cloud computing solution(adopted from [1]).

Figure 3.1: Cloud components

Clients:

End users interact with the clients to manage information related to the cloud. Clients generally fall into three categories as given in:

- Mobile: Windows Mobile Smartphone, smartphones, like a Blackberry, or an iPhone.
- Thin: They don't do any computation work. They only display the information. Servers do all the works for them. Thin clients don't have any internal memory.

- Thick: These use different browsers like IE or Mozilla Firefox or Google Chrome to connect to the Internet cloud. Now-a-days thin clients are more popular as compared to other clients because of their low price, security, low consumption of power, less noise, easily replaceable and repairable etc. Datacenter.

Datacenter is nothing but a collection of servers hosting different applications. A end user connects to the datacenter to subscribe different applications. A datacenter may exist at a large distance from the clients.

Now-a-days a concept called virtualization is used to install a software that allow multiple instances of virtual server applications.

Distributed Servers:

Distributed servers are the parts of a cloud which are present throughout the Internet hosting different applications. But while using the application from the cloud, the user will feel that he is using this application from its own machine.

Services provided by Cloud computing:

Service means different types of applications provided by different servers across the cloud. It is generally given as "as a service". Services in a cloud are of 3 types as given:

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Hardware as a Service (HaaS) or Infrastructure as a Service (IaaS)

Software as a Service (SaaS)

In SaaS, the user uses different software applications from different servers through the Internet. The user uses the software as it is without any change and do not need to make lots of changes or doen't require integration to other systems. The provider does all the upgrades and patching while keeping the infrastructure running.

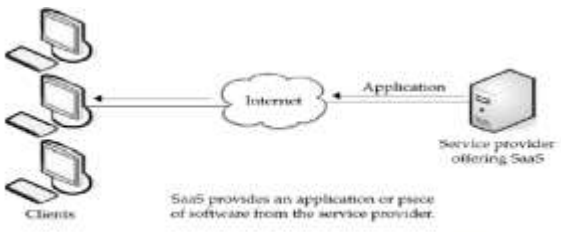


Figure 5: Software as a service (SaaS) (adopted from [1])

Figure 3.2: Software as a service

The client will have to pay for the time he uses the software. The software that does a simple task without any need to interact with other systems makes it an ideal candidate for Software as a Service. Customer who isn't inclined to perform software development but needs high-powered applications can also be benefitted from SaaS.

Customer resource management (CRM)

- Video conferencing
- IT service management
- Accounting
- Web analytics
- Web content management

Benefits: The biggest benefit of SaaS is costing less money than buying the whole application.

The service provider generally offers cheaper and more reliable applications as compared to the organization. Some other benefits include (given in): Familiarity with the Internet, Better marketing, smaller staff, reliability of the Internet, data Security[6], More bandwidth etc.

Obstacles:

- SaaS isn't of any help when the organization has a very specific computational need that doesn't match to the SaaS services
- While making the contract with a new vendor, there may be a problem. Because the old vendor may charge the moving fee. Thus it will increase the unnecessary costs.
- SaaS faces challenges from the availability of cheaper hardware's and open source applications.

Platform as a Service (PaaS):
PaaS provides all the resources that are required for building applications and services completely from the Internet, without downloading or installing a software.

PaaS services are software design, development, testing, deployment, and hosting. Other services can be team collaboration, database integration, web service integration, data security, storage and versioning etc.

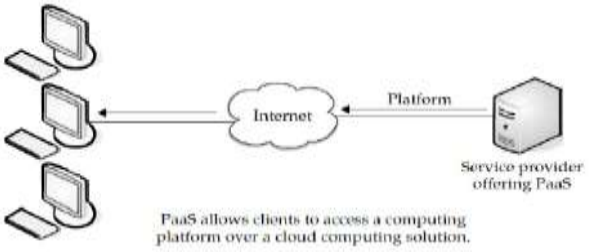


Figure 6: Platform as a service (PaaS) (adopted from [1])

Figure 3.3: Platform as a Service

Downfall:

- Lack of portability among different providers.

- if the service provider is out of business, the user's applications, data will be lost.

Hardware as a Service (HaaS):

It is also known as Infrastructure as a Service (IaaS). It offers the hardware as a service to a organization so that it can put anything into the hardware according to its will [1]. HaaS allows the user to "rent" resources (taken from [1]) as

- Server space
- Network equipment
- Memory
- CPU cycles
- Storage space

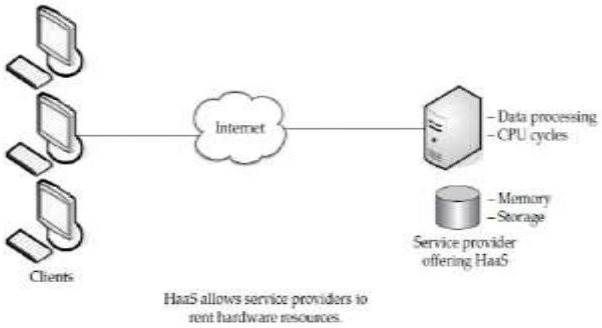


Figure 7: Hardware as a service (HaaS) (adopted from [1])

Figure 3.4: Hardware as a service

Cloud computing provides a Service Oriented Architecture (SOA) and Internet of Services (IoS) type applications, including fault tolerance, high scalability, availability, flexibility, reduced information technology overhead for the user, reduced cost of ownership, on demand services etc. Central to these issues lies the establishment of an effective load balancing algorithm.

4. IMPLEMENTATION

Design is concerned with identifying software components specifying relationships among components. Specifying software structure and providing blue print for the document phase. Modularity is one of the desirable properties of large systems. It implies that the system is divided into several parts. In such a manner, the interaction between parts is minimal clearly specified.
During the system design activities, Developers bridge the gap between the requirements specification, produced during requirements elicitation and analysis, and the system that is delivered to the user.
Design is the place where the quality is fostered in development. Software design is a process through which requirements are translated into a representation of software.

4.1 Use Case Model

Use case diagrams represent the functionality of the system from a user point of view. A Use case describes a function provided by the system that yields a visible result for an actor. an actor describe any entity that interacts with the system. The identification of actors and use cases results in the definition of the boundary of the system, which is , in differentiating the tasks accomplished by the system and the tasks accomplished by its environment. The actors outside the boundary of the system, whereas the use cases are inside the boundary of the system

A Use case contains all the events that can occur between an actor and a set of scenarios that explains the interactions as sequence of happenings.

4.2 Java Programming Language

Each of the preceding buzzwords is explained in The Java Language Environment , a white paper written by James Gosling and Henry McGilton.

In the Java programming language, all source code is first written in plain text files ending with the .java extension. Those source files are then compiled into .class files by the javac compiler. A .class file does not contain code that is native to your processor; it instead contains bytecodes — the machine language of the Java Virtual Machine1 (Java VM). The java launcher tool then runs your application with an instance of the Java Virtual Machine.

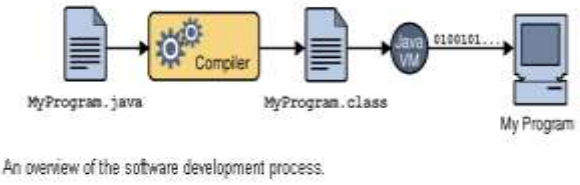


Figure 4.1: java software development process

An overview of the software development process.

Because the Java VM is available on many different operating systems, the same .class files are capable of running on Microsoft Windows, the Solaris Operating System (Solaris OS), Linux, or Mac OS. Some virtual machines, such as the Java HotSpot virtual machine, perform additional steps at runtime to give your application a performance boost. This include various tasks such as finding performance bottlenecks and recompiling (to native code) frequently used sections of code

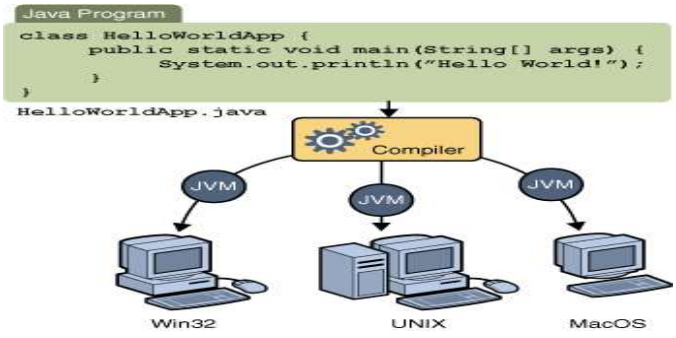


Figure 4.2: java compiler

Code Snippets (Logics) & Analysis

Logics

When using GP to solve a problem, there are some basic requirements that must be fulfilled, which are based on the data structure used to represent the solution. In our case, we have chosen a tree-based GP representation for the deduplication function, since it is a natural representation for this type of function. These requirements are the following:

1. All possible solutions to the problem must be represented by a tree, no matter its size.

2. The evolutionary operations applied over each individual tree must, at the end, result into a valid tree.

3. Each individual tree must be automatically evaluated.

For Requirement 1, it is necessary to take into consideration the kind of solution we intend to find. In the record reduplication problem, we look for a function that combines pieces of evidence.

In our approach, each piece of evidence (or simply "evidence") E is a pair <attribute; similarity function> that represents the use of a specific similarity function over the values of a specific attribute found in the data being analyzed. For example, if we want to reduplication a database table with four attributes (e.g., forename, surname, address, and postal code) using a specific similarity function.

To model such functions as a GP tree, each evidence is represented by a leaf in the tree. Each leaf (the similarity between two attributes) generates a normalized real number value (between 0.0 and 1.0). A leaf can also be a random number between 1.0 and 9.0, which is chosen at the moment that each tree is. Such leaves (random numbers) are used to allow the evolutionary process to find the most adequate weights for each evidence, when necessary. The internal nodes represent operations that are applied to the leaves. In our model, they are simple mathematical functions (e.g. *, % , /) that manipulate the leaf values.

To enforce Requirement 2, the trees are handled by sub tree atomic operations to avoid situations that could affect the integrity of the overall function, resulting an invalid tree. For a valid tree (or a valid function), there cannot be neither a case where the value of a leaf node is replaced by the value of an internal node nor one where the value of an internal node is replaced by the value of a leaf node.

According to Requirement 3, all trees generated during a GP evolutionary process is tested against pre evaluated data repositories where the replicas have been previously identified. This makes feasible to perform the whole process automatically, since it is possible to evaluate how the trees perform in the task of recognizing record pairs that are true replicas.

The tree input is a set of evidence instances, extracted from the data being handled, and its output is a real number value. This value is compared against a replica identification boundary value as follows: if it is above the boundary, the records are considered replicas, otherwise, the records are considered distinct entries. It is important to notice that this classification enables further analysis, especially regarding the transitive properties of the replicas.

4 This can improve the efficiency of clustering algorithms, since it provides not only an estimation of the similarity between the records being processed, but also a judgment of whether they are replicas or not.

After doing these comparisons for all candidate record pairs, the total number of correct and incorrect identified replicas is computed. This information is then used by the most important configuration component in our approach: the fitness function.

5. NICE OUTPUTS

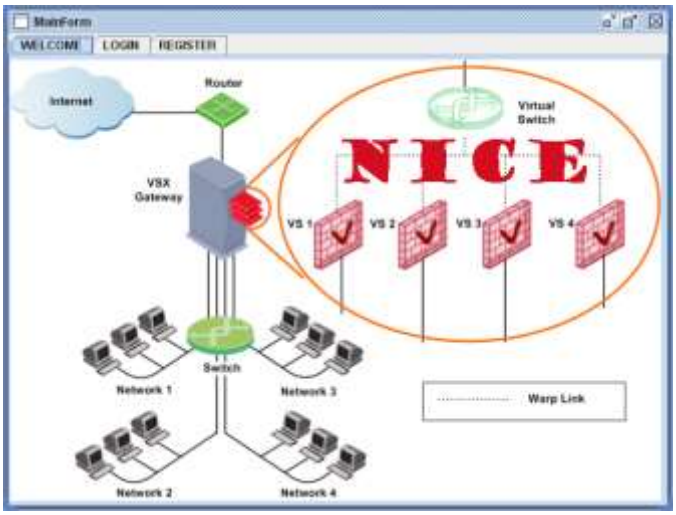


Figure 5.1:NICE

Login into NICE web-page

Figure 5.2:login page NICE

Figure 5.3:Registration page NICE

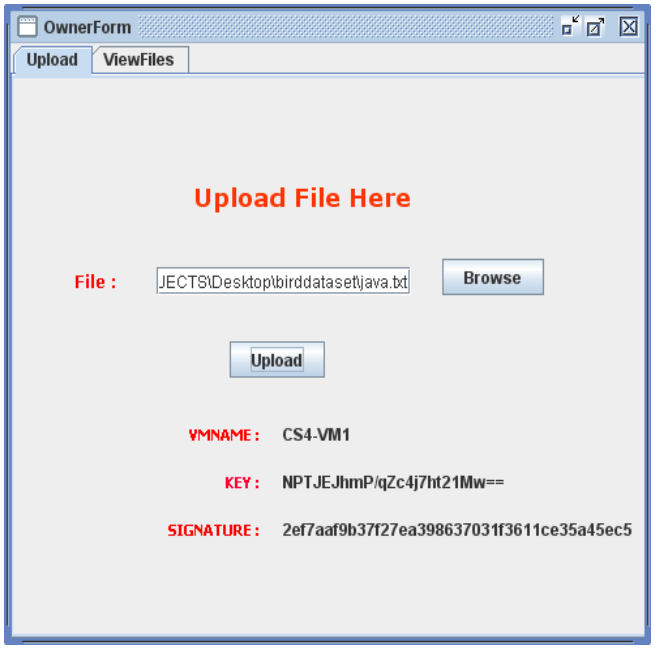


Figure 5.4:Upload file

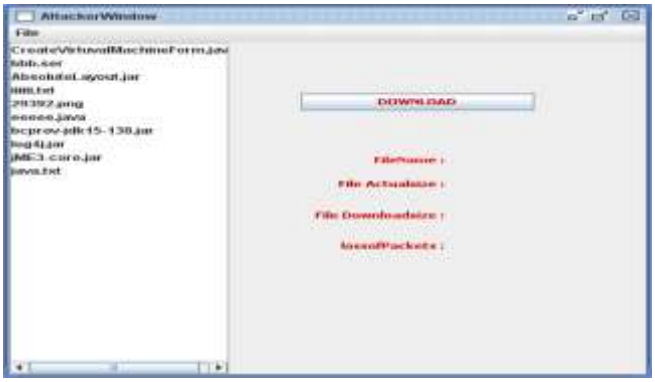


Figure 5.5:Downloading file

Figure 5.6: Intruder found the NICE

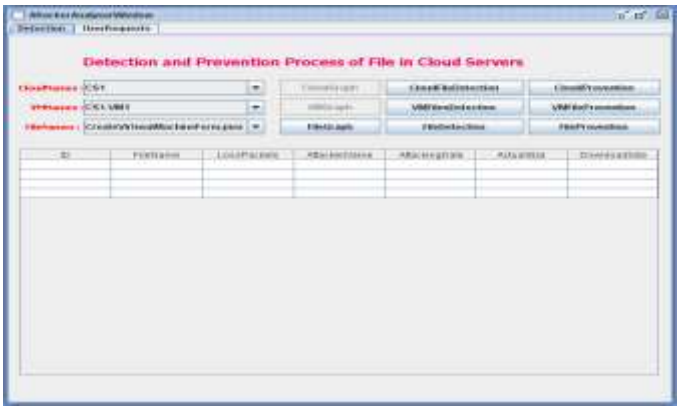


Figure 5.7: Detection and Prevention process of file in cloud services

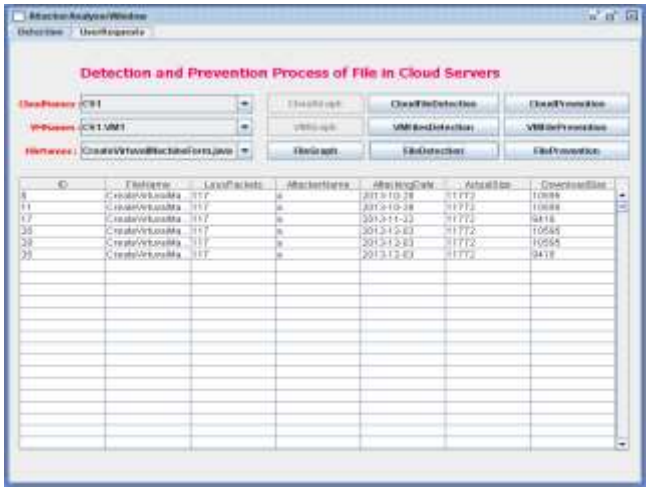


Figure 5.8: Output of cloud servers

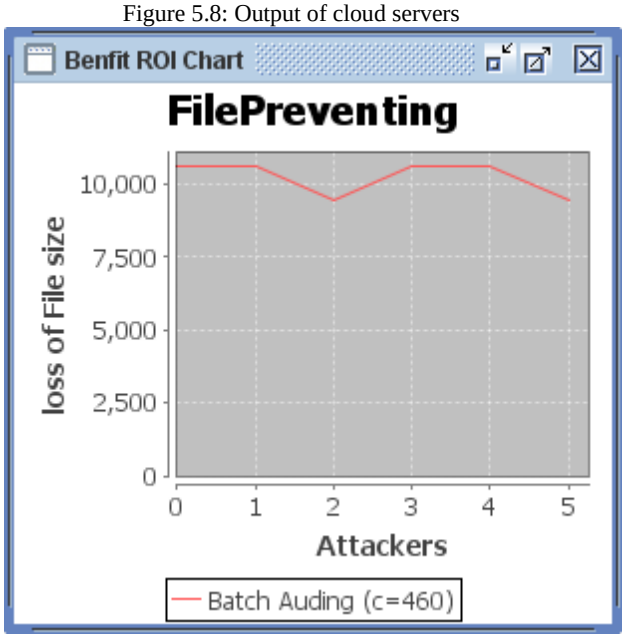


Figure 5.9: Benefit RIO chart

6. CONCLUSION

In this paper, we presented NICE, which is proposed to detect and mitigate collaborative attacks [9] in the cloud virtual networking environment. NICE utilizes the attack graph model to conduct attack detection and prediction. The proposed solution investigates how to use the programmability of software switches-based solutions to improve the detection accuracy and defeat victim exploitation phases of collaborative attacks. The system performance evaluation demonstrates the feasibility of NICE and shows that the proposed solution can significantly reduce the risk of the cloud system from being exploited and abused by internal and external attackers.

NICE only investigates the network IDS [7] approach to counter zombie explorative attacks. To improve the detection accuracy, host-based IDS solutions are needed to be incorporated and to cover the whole spectrum of IDS in the cloud system.

7. FUTURE ENHANCEMENT

This should be investigated in the future work. Additionally, as indicated in the paper, we will investigate the scalability of the proposed NICE solution by investigating the decentralized network control and attack analysis model based on current study.

8. ACKNOWLWDGEMENTS

We are grateful to express sincere thanks to our faculties who gave support and special thanks to our department for providing facilities that were offered to us for carrying out this project.

REFERENCES

[1] Coud SercurityAlliance,"Top Threats to Cloud Computing v1.0,"https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf, Mar. 2010.

[2] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," ACM Comm., vol. 53, no. 4, pp. 50-58, Apr. 2010.

[3] B. Joshi, A. Vijayan, and B. Joshi, "Securing Cloud Computing Environment Against DDoS Attacks," Proc. IEEE Int'l Conf. Computer Comm. and Informatics (ICCCI '12), Jan. 2012.

[4] H. Takabi, J.B. Joshi, and G. Ahn, "Security and PrivacyChallenges in Cloud Computing Environments," IEEE Security and Privacy, vol. 8, no. 6, pp. 24-31, Dec. 2010.

[5] "Open vSwitch Project," http://openvswitch.org, May 2012.

[6] Z. Duan, P. Chen, F. Sanchez, Y. Dong, M. Stephenson, and J. Barker, "Detecting Spam Zombies by Monitoring Outgoing Messages," IEEE Trans. Dependable and Secure Computing, vol. 9, no. 2, pp. 198-210, Apr. 2012.

[7] G. Gu, P. Porras, V. Yegneswaran, M. Fong, and W. Lee, "BotHunter: Detecting Malware Infection through IDS-driven Dialog Correlation," Proc. 16th USENIX Security Symp. (SS '07),pp. 12:1-12:16, Aug. 2007.

[8] G. Gu, J. Zhang, and W. Lee, "BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic,"

Proc. 15thAnn. Network and Distributed Sytem Security Symp. (NDSS'08), Feb. 2008.

[9] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J.M. Wing,"Automated Generation and Analysis of Attack Graphs," Proc.IEEE Symp. Security and Privacy, pp. 273-284, 2002,

[10] "NuSMV: A New Symbolic Model Checker," http://afrodite.itc. it:1024/nusmv. Aug. 2012.

International Journal of Computer Applications Technology and Research
Volume 3– Issue 11, 745 - 750, 2014

Integration of Bus Specific Clock Gating and Power Gating

M. Nagarjuna
Vardhaman College of Engineering
Hyderabad, Telangana
India

B. Narendra Reddy
Vardhaman College of Engineering
Hyderabad, Telangana
India

S. Rajendar
Vardhaman College of Engineering
Hyderabad, Telangana
India

Abstract: In integrated circuits a gargantuan portion of chip power is mostly consumed by clocking systems which comprises of flip-flops, latches and clock distribution networks. The two most widely used techniques for the reduction of dynamic and leakage power are clock gating (CG) and power gating (PG). The two techniques CG and PG are coupled in such a way that the clock enable signal is generated by CG used as sleep signal to drive the power gated cells for the reduction of leakage power. So here we first introduced bus specific clock gating (BSCG) technique which is traditional XOR based CG and it reduces the dynamic power, then the power gating (PG) technique is used for power gated cells for reduction of leakage power. All circuits are simulated in Cadence Virtuso Analog Design Environment using GPDK 45nm technology at different global clock frequencies and temperatures. The performance of proposed integrated technique is compared with power gating technique in terms of performance metrics like average power and leakage power. From simulation results, it is evident that as temperature increases both average and leakage powers is reduced and the sleepy stack technique outstands in its performance as compared with other techniques.

Keywords: Low Power, Flip-Flop, Power Gating, Clock Gating, Latches.

1. INTRODUCTION

With the small geometries in deep sub-micron technology the number of devices has to be integrated on a single chip, so the devices in a chip and the total power consumption had increases rapidly.

With the increasing popularity of battery driven portable electronics there is a growing demand for low-power circuit designs. With the progress of CMOS technology there is steady growth in clock frequency and chip capacity. So the low power techniques are highly appreciated in current VLSI design. In a CMOS circuit power consumption consists of dynamic and leakage power. Leakage power can be sub-divided into standby and active leakage. Dynamic power consumption occurs in a circuit when it's input toggles. Leakage power is dissipated in a circuit when it's input not toggles is known as standby leakage, so it is referred as the circuit is in sleep mode, while the leakage power consumed in operation mode (when the input toggles) is known as active leakage.

Clock gating (CG) [1]-[5] is the most widely used technique for the reduction of dynamic power in CMOS circuits. Power gating (PG) [6]-[9] is the dominant technique to reduce the standby leakage power. The active leakage power becomes more important, so it is differ from normal PG, the PG to minimize active leakage power in operation mode is referred as a run time power gating [10]-[12]. During the clock gated period there are some components that are performing redundant operations and run time power gating will put these components into sleep. Integration of CG and PG is achieved with simultaneous reduction of dynamic and active leakage power [12]-[16].

In this paper, integration of BSCG and PG will leads to the reduction of dynamic and active leakage power simultaneously. After the BGSC is applied to the design the components performing redundant operations during the clock gated period are determined by forward traversing the circuit from the gated flip-flop outputs. These components will be power gated using the clock enable signal generated by BSCG.

The rest of this paper is organized as follows. Section 2 gives an overview of CG and PG. BSCG is presented in Section 3. Integration of BSCG and PG is explained in Section 4. Simulation results are shown in Section 5 and concluded in Section 6.

2. PRELIMINARY CONCEPTS

2.1 Clock Gating (CG) Basics

As the operating speed increases of a chip then the dynamic power consumption increases dramatically.CG is a technique used to gate the unnecessary clock toggles of a registers. Clock gating is a technique that is used to control the power dissipated by a clock network and it reduces the dynamic power dissipation. In a synchronous circuits clock network is responsible for a power dissipation up to 40%..Clock gating reduces the unwanted switching on the parts of a clock network by disabling the clock signal. Clock gating saves the power by adding a more logic to a clock network. When the clock is not switched the switching (dynamic) power consumption goes to zero and there is only a leakage current is occurred. Clock gating shuts off the clock when the system is in current state so that the dynamic power consumption is reduced.

Fig.1 shows a CG architecture it consists of a signal called activation function (F_a), latch, AND gate and registers. Activation function is defined in order to selectively stop the clocking of the circuit then the activation signal is filtered by a latch when the global clock is high. The purpose of latch is to filter glitches of the activation signal that should not propagate when the global clock is low. When both of the

global clock is and the output of latch are high then the gated clock signal is applying as a clock signal for the registers i.e. when there is change in the input data of a register at that time the gated clock is applying. Activation signal is a combinational block that extracts the information from primary and state inputs of a circuit.

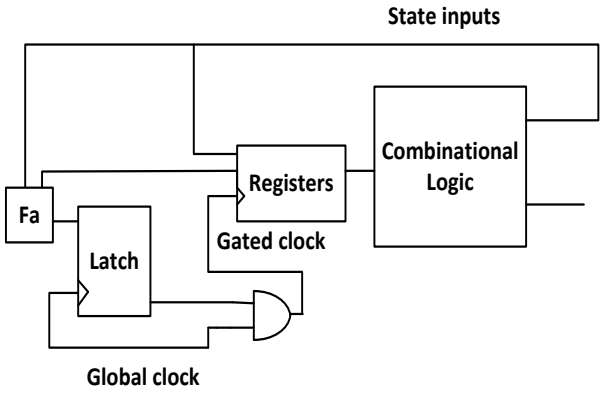


Fig.1. Clock Gating (CG) Architecture

2.2 Power Gating (PG) Basics

As the scaling of MOSFET proceeds leakage power of chip will increases dramatically. Leakage power is the major concern in portable devices because it wastes the energy in standby mode and leads to shortening of battery life. So one of the effective techniques to reduce the standby leakage is power gating in which power switches (sleep transistors) are inserted among logic circuits, power supply and ground. Power switch is turned off when the system is in standby mode so that the power is off for the system so the leakage current is reduced.

PG is also called as MTCMOS technique in which the header (PMOS) and/or footer (NMOS) transistor is inserted on the pull-up and/or pull-down network of a CMOS gate. The transistors are turned off when the circuit is in standby mode thus reducing the leakage current that flows from supply to ground path shown in fig.2. The power switches are normally referred as sleep transistors because they are driven by the same signal. In a power gated design sleep transistors controls the clusters of gates instead of individual gates.

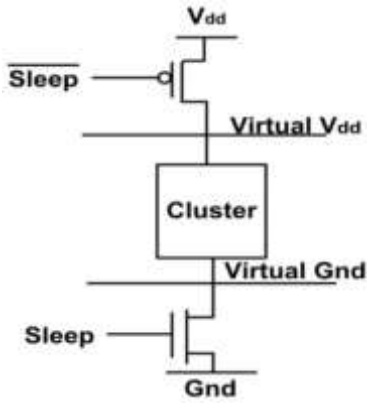


Fig.2. Power Gating (PG) Architecture

3. BUS SPECIFIC CLOCK GATING (BSCG)

It is used to reduce the dynamic power and it can be realized by D-flip-flops, AND, XOR and OR gates. BSCG circuit compares the inputs and outputs and gates the clock when they are equal i.e. when there is change in the input data of gated FFs then only the gated clock is applying for D-FFs otherwise the gated clock signal is not applying. Fig. 3(a) shows a non-clock gating circuit and fig b shows a BSCG circuit.

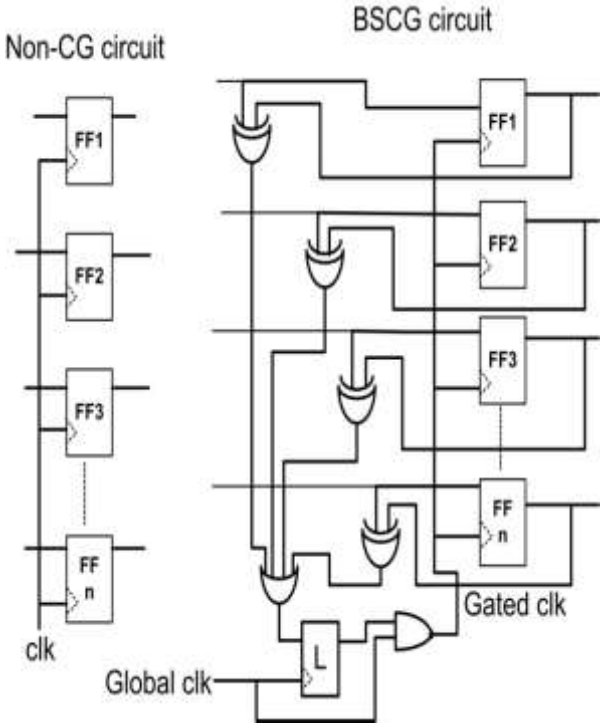


Fig. 3(a) Non-clock gating circuit (b) BSCG circuit

4. INTEGRATION OF BSCG AND PG

A footer power switch is inserted either in between actual ground and virtual ground of the power gated cells or a header switch is inserted in between power supply and the virtual power supply of power gated cells are shown in Fig. 4. The enable signal generated from BSCG is used as sleep signal for PG cells. PG cells are totally dependent on gated FF outputs. Holders are placed in between the power gated cells and the non-power gated cells so that non-power gated cells can function properly.

Integration of BSCG and PG can be explained in detail by considering an example of synchronous circuit as shown in Fig. 5. It consists of four out of five FFs are clock gated. For it first we had applied BSCG technique then four FFs are clock gated. The dashed lines are completely dependent on stable gated FFs outputs, so they are inactive and can be power gated into sleep. However, one input of the xor gate H is the output of un-gated FF1, since it may not be stable (active) during clock gated period. In order to avoid floating signal, holder logic is placed at the output of power gated cell if that output connects to non-power gated cells or primary outputs.

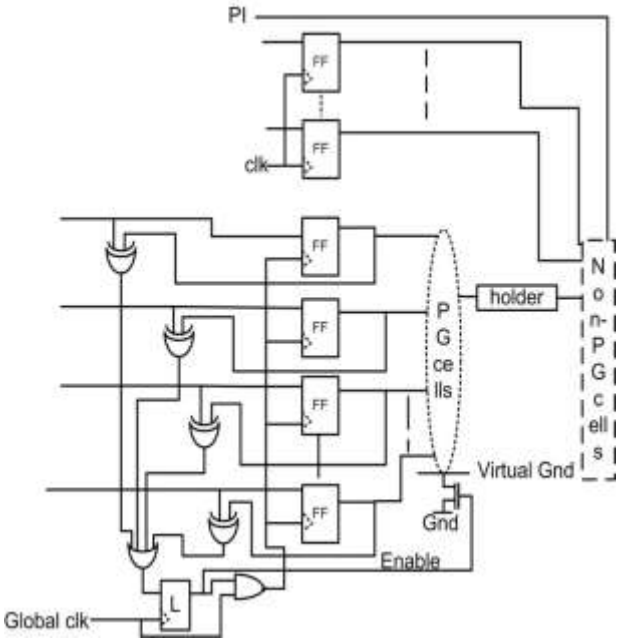


Fig. 4. Integration of BSCG and PG

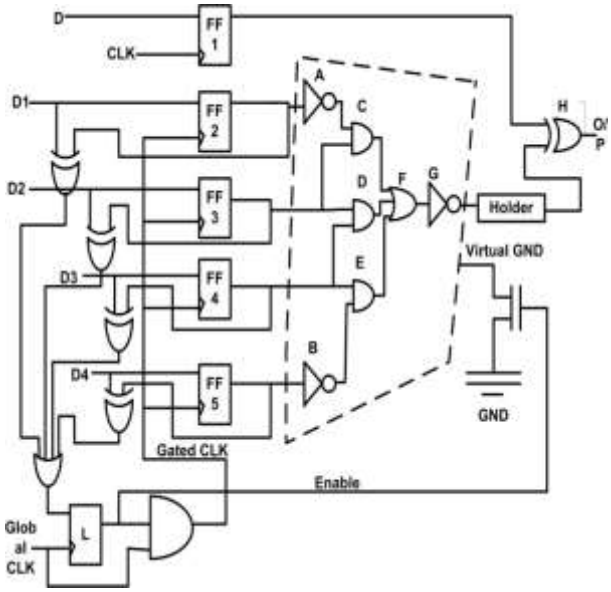


Fig. 5. Synchronous circuit example

5. RESULTS

The synchronous circuit is simulated in CADENCE 45nm technology. Average power and leakage power with different power gate techniques at different global clock frequencies and at different temperatures are shown in Table 1 and there variations with temperature are shown in the figures6 - 9 for average power and in figures 10 - 13 for leakage power.

Table 1: Average power and Leakage Power

Power Gating Schemes	Average and Leakage Powers (nW) at -27^{0}C			Average and Leakage Powers (nW) at 0^{0}C			Average and Leakage Powers (nW) at 27^{0}C			Average and Leakage Powers (nW) at 50^{0}C		
	Global Clock Frequencies			Global Clock Frequencies			Global Clock Frequencies			Global Clock Frequencies		
	20MHz	25MHz	50MHz	20MHz	25MHz	50M Hz	20MHz	25MHz	50MHz	20MHz	25MHz	50M Hz
Dual Sleep Technique	968.2	1008	990	888.6	927	914.6	823.4	860.3	852.8	778.4	814	810.6
	625.5	684.7	630.9	602.3	631.6	576.8	573.4	599.2	544.3	535.9	559.9	503.1
Sleep Technique	965.2	1005	987.3	883.1	921.4	909.6	821.9	858.9	850.4	776.8	812.7	808.2
	622.3	677.4	624.1	598.9	626.6	574.2	573.9	600	544.6	536.9	560.7	503.4
Stack Technique	960.9	1002	985.9	879.4	919.8	905.8	817.7	856.7	849.3	776.2	812.5	808
	618.5	668.3	622.2	595.2	624.5	570.6	570.5	598.2	543.2	533.7	557.8	501.1
Sleepy Stack Technique	958.7	999	981.5	876.5	914.9	902.2	816	852.3	844.3	771.7	808.4	803.6
	615.8	664.9	618.6	589.3	619.8	565.4	569	594	538.7	532.7	556.2	498.2

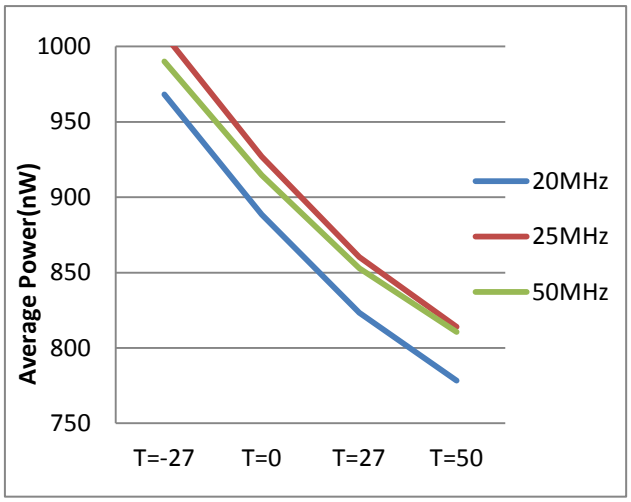


Figure6: Average power versus temperature for Dual Sleep Power Gating Technique

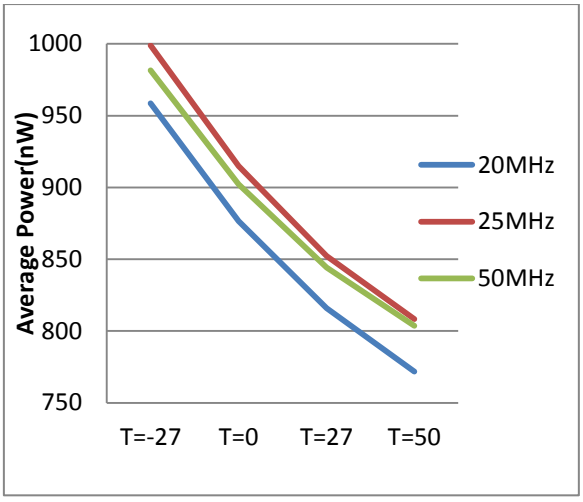


Figure9: Average power versus temperature for Sleepy Stack Power Gating Technique

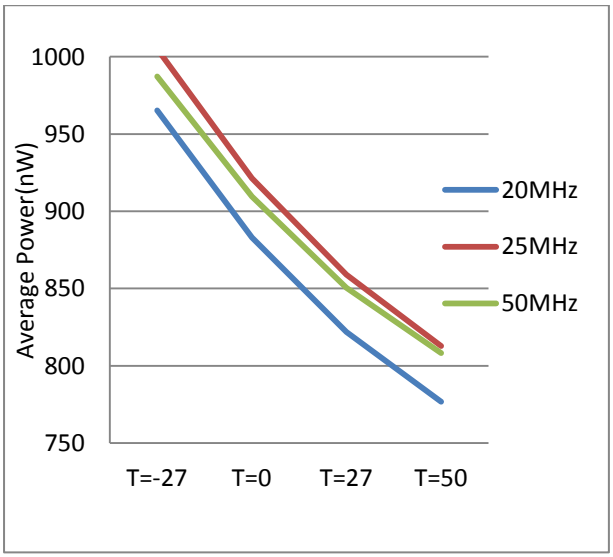


Figure7: Average power versus temperature for Sleep Power Gating Technique

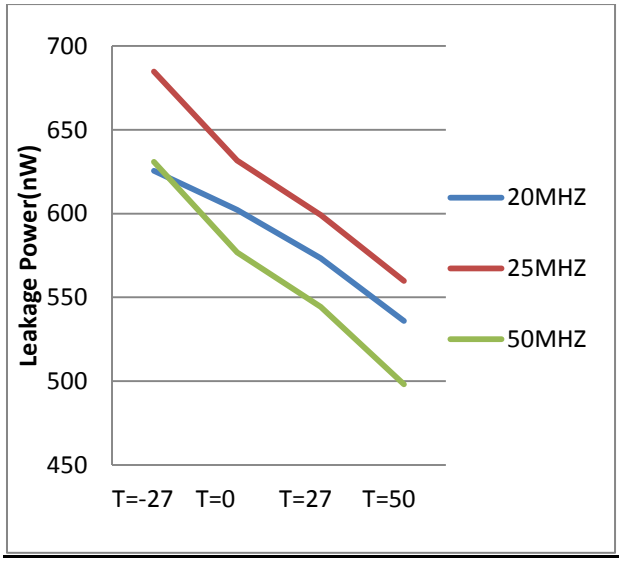


Figure10: Leakage power versus temperature for Dual Sleep Power Gating Technique

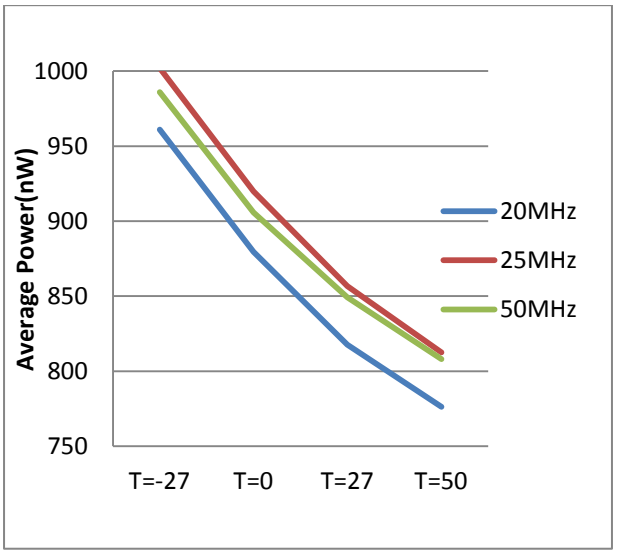


Figure8: Average power versus temperature for Stack Power Gating Technique

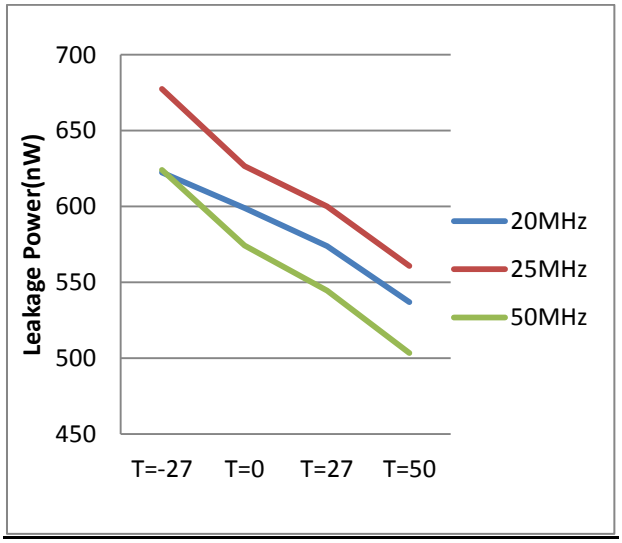


Figure11: Leakage power versus temperature for Sleep Power Gating Technique

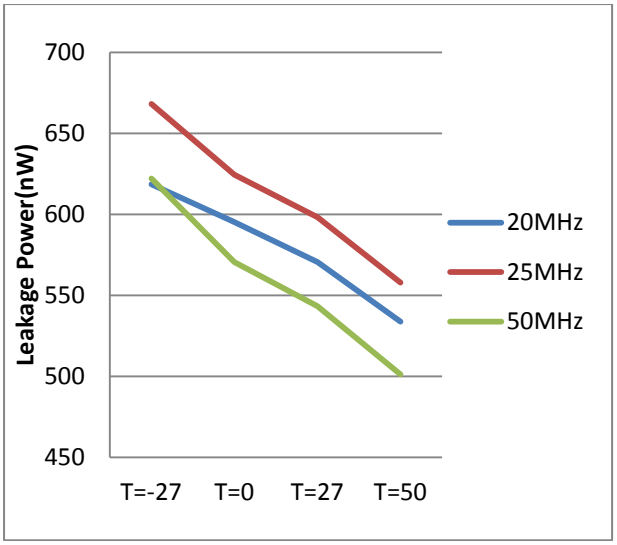


Figure12: Leakage power versus temperature for Stack Power Gating Technique

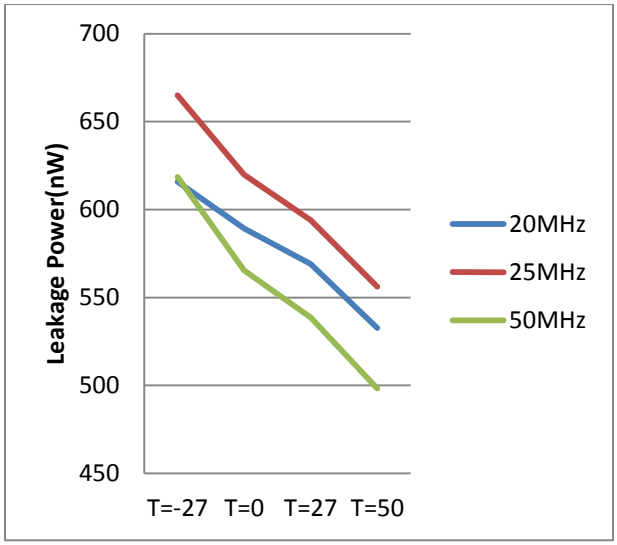


Figure13: Leakage power versus temperature for Sleepy Stack Power Gating Technique

6. RESULTS

In this paper an integration of BSCG and PG is achieved in sequential circuits. First BSCG technique is evaluated it selects the flip-flops for gated and the clock enable signal generated from BSCG used as sleep signal in PG. A synchronous circuit is implemented by using both BSCG and PG and there average power and leakage power are evaluated by power gating techniques at different global clock frequencies and at different temperatures. As Temperature increases both average and leakage powers are reduced and the best method is sleepy stack.

7. REFERENCES

[1] Jagrit Kathuria, M. Ayoubkhan and Arit Noor, "A review of clock gating techniques," in MIT IJ of ECE, vol.1 no. 2. Aug 2011 pp 106-114.

[2] P. Babighian, L. Benini and E. Macii, "A scalable algorithm for RTL insertion of gated clocks based on ODCs computation," IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 24, no. 1, pp. 29-42 Jan 2005.

[3] D. Garrett, M. Stan, and A. Dean, "Challenges in clock gating for a low power ASIC methodology," IEEE International Symposium on Low-Power Electronics and design, pp. 176-181, Aug. 1999.

[4] L. Benini, G. De Micheli, E. Macii, M. Poncino and R. Scarsi, "Symbolic synthesis of clock gating logic for low power optimization of synchronous controllers," ACM Trans. Des.Autom. Electron, Oct. 1999.

[5] Vishwanadh Tirumalashetty and Hamid Mahmoodi, "Clock gating and negative edge triggering for energy recovery clock," ISCAS 2007, New Orleans, LA pp. 1141-1144, 2007.

[6] K. Roy, S. Mukhopadkyay and H. Mahmoodi-meimand, "Leakage current mechanisms and leakage reduction techniques in deep sub micrometer CMOS circuits," Proc. IEEE, vol. 91, no. 2, pp. 305-327, Feb 2003.

[7] V. De and S. Borkar, "Technology and design challenges for low power and high performance," in Proc. Int. Symp. Low Power Electronics and Design, 1999, pp. 163-168.

[8] C. Mead, "Scaling of MOS technology to sub micrometer feature sizes," Analog Integrated Circuits Signal Process, vol. 6, pp. 9-25,1994.

[9] A. Keshavarzi, K. Roy and C. F. Hawkins, "Intrinsic leakage in low power deep sub-micron CMOS ICs," in Proc. Int. Test Conf, 1997, pp. 146-155.

[10] K. Usami and N. Ohkubo, "A design approach for fine-grained run time power gating using locally extracted sleep signals," in Proc. Int. Conf. Comput. Design, 2006, pp. 151-161.

[11] Z. Hu, A. Buyuktosunoglu, V. Srinivasan, V.Zyuban, H. Jacobson and P.Bose, "Micro-architectural techniques for power gating of execution units," Proc. ISLPED'04, pp. 32-37, 2004.

[12] J. Tschanz, S. Narendra, Y.Ye, B. Bloechel, S. Borkar and V. De, "Dynamic sleep transistor and body bias for active leakage power control of microprocessors," IEEE J. Solid state circuits, vol. 38, no. 11, pp. 1838-1845, Nov. 2003.

[13] L. Bolzani, A.Calimera, A. Macii, E.Macii and M. Poncino, "Enabling concurrent clock and power gating in an industrial design flow," in Proc. Des. Auto. Test Eur. Conf. 2009, pp. 334-339.

[14] L. Benini and G. De Micheli, "Transformation and synthesis of FSMs for low power gated clock implementation," IEEE Trans. On CAD, vol. 15, no. 6, pp. 630-643, 1996.

[15] L. Bolzani, A.Calimera, A. Macii, E.Macii and M. Poncino, "Integrating clock gating and power gating for combined dynamic and leakage power optimization in digital CMOS circuits," DSD08: IEEE 11th Euro micro Conference on Digital System Design, September 2008, pp. 298-303.

[16] Li Li, Ken Choi and Haiqing Nan, "Activity-driven fine-grained clock gating and run time power gating integration," IEEE transactions on VLSI systems, vol. 21, no.8, Aug 2013.

International Journal of Computer Applications Technology and Research
Volume 3– Issue 11, 751 - 755, 2014

An Enhanced Model for Adoption of Local Software: A Case of Kenya

Maurine Awuor Onyango
JKUAT
Nairobi, Kenya

Michael Kimwele
JKUAT
Nairobi, Kenya

Wilson Cheruiyot
JKUAT
Nairobi, Kenya

Abstract: The share of developing countries in the global software market has risen and now accounts for around 5 percent of sales. A small number of developing countries have successfully developed their own software industries and have continued to strengthen the sector even after 2000. However, many customers in Kenya frequently opt for better packaged and marketed software from India, United State or Unite Kingdom, even when these have to be overhauled to suit the Kenyan market. In doing so, the customers deny the local products the much needed breathe of life that is required to enable them to survive in the competitive software marketplace. Relatively little research has examined a model for the adoption of local software, either as a unique task or in the context of local software development in Kenya. This study attempted to explain how adoption of local software development is affected by the individual, technological, environmental and organizational determinants in Kenya. In this framework, explanatory research design was used. The population for this study was the 347 Information Technology and Information Communication Technology companies which provide software services in Kenya and their customers/users. The list was obtained from members of Kenya Information Communication Technology Providers Association. A sample of 35 managers from firms was taken and also 70 users. Purposive sampling was applied to select the product managers while random sampling was used to select the 70 customers. In this study, primary data was collected using a structured questionnaire. The researcher used Statistical Package for Social Sciences Version 20 (SPSS) to generate the descriptive statistics and inferential results. Confirmatory Factor Analysis was used to analyze the data and Structural Equation Modeling using Analysis of Moment Structures was used to validate the research model. Post study interview was carried out to test the applicability of the model. Data collected from interview was analyzed and presented using content analysis. The expected results include a model that can used to enhance adoption of local software. The study findings indicated that there was low level of local software adoption. Results further indicated that individual factors, technological factors, organizational factors and environmental factors were negatively correlated with adoption of local software adoption.

Keywords: *Adoption, Local Software, Model, individual factors, technological factors, environmental factors, organisational factors.*

1. BACKGROUND AND RESEARCH PROBLEM

Software is critical in today's markets. The importance of information and communication technologies, and thus the software that makes them function, is growing rapidly in both industrial and consumer markets. E-commerce, the Internet, enterprise-integration systems, and wireless networking are just some of the high-profile systems and applications dependent on effective software development. For software development, modern agile software development models address certain parts of this problem space (Boehm and Turner 2004). They are thus gaining more and more attention in many industrial product development organizations.

Local software production and development can spur economic growth in Africa and other developing economies, says report by UN Conference on Trade and Development 2013. Information Economy Report 2012 shows that ICT software and services are dominated by developed world. African countries, Kenya included must look onto ways of increasing the adoption and diffusion of innovation and to solve the problems they are experiencing.

Adoption rate of local software development in Kenya is very low. The biggest challenges facing software innovators in Kenya are the skill to package the software products, and the capital for marketing. Many Kenyans build softwares that never grow beyond a few customers. Many customers frequently opt for better packaged and marketed software from India, US or UK, even when these have to be overhauled to suit the Kenyan market. In doing so, the customers deny the local products the much needed breathe of life required to enable them survive in the competitive software marketplace (Kabugi, 2013).

The majority of studies relating to technology diffusion and adoption have been conducted in developed countries. Most of the studies focus on individual adoption behaviors and decisions. They do not necessarily lend themselves to studying organizational adoption of technology (King and Gribbins, 2002). Therefore, there is need for a research to come up with adoption model that suits the developing countries like Kenya and also a model that looks at the individual level of adoption and also the organization level.

In addressing the factors influencing software adoption in organizations there is the need for a model that specifically highlights these issues. Relatively little research has examined a model for the adoption of local software, either as a unique task or in the context of local software development in Kenya. This study attempts to explain how adoption of local software development is affected by the individual behaviours, technological, environmental and organizational determinants in Kenya.

2. RESEARCH OBJECTIVES

i. To establish the effect of individual, technological, organizational and environmental factors on the adoption of local software development.
ii. To formulate and evaluate the model for adoption of local software development.

3. METHODOLOGY

This research intended to empirically validate the proposed theoretical model (and hypotheses) of local software development in Kenya. Data from software developers includes those have not adopted local development at all, those that adopted and succeeded and those that attempted but failed were obtained touching on their perceptions, plans, success/fail factors, challenges, extents of adoption, actual gains etc. In this framework, explanatory research design was used. Studies that establish causal relationships between variables are termed as explanatory studies. The emphasis here is on studying a situation or a problem in order to explain the relationship between variables (Saunders, Lewis and Thorn, 2003). The target population for this study was the 347 IT and ICT companies which provide software services in Kenya and are listed as members of Kenya ICT Providers Association and also their users/customers. A sample of 10% which is 35 firms was taken. Two customers from each of the 35 firms were selected purposively. However, simple random sampling was used to select the 35 firms. In total the research had a sample of 105 (users and developers) to give the questionnaires. According to Gay, (2001) and Mugenda and Mugenda, (2003) a sample of 10-30% is deemed adequate for this study.

The data used for the purpose of the study was primary data collected by the researcher, through questionnaires and interviews. A questionnaire technique since it is suited for exploratory research. The researcher used frequencies, averages and percentages in this study. The researcher used Statistical Package for Social Sciences Version 20 (SPSS) to generate the descriptive statistics and also to generate inferential results. The individual hypotheses were tested using correlation analysis. Regression analysis was used to demonstrate the relationship between adoption of local software development and the determining factors. According to Mugenda and Mugenda (2003), the regression technique used to analyze the degree of relationship between two variables.

The multiple linear regression models adopted for the study was as follows:

$Y=\alpha + \beta_1X_1+ \beta_2X_2+ \beta_3X_3+ \beta_4X_{4+}\varepsilon$

Where: Y = Adoption of local software development

X_1 = Individual related constructs

X_2 = Technology related constructs

X_3 = Organizational related constructs

X_4 =Environmental related constructs

In the model α was the constant term while the coefficients β_1 to β_4 was used to measure the sensitivity of the dependent variable (Y) to unit change in the explanatory variables (X_1, X_2, $X_3$and X_4). ε is the error term which captures the unexplained variations in the model.

The first stage was testing /analysis of the model which was by running regression and correlations among the various variables. This was done after formulating the model, coming up with the correct questionnaire and then data collection.

The second stage was to identify which hypothesis was rejected and which ones were accepted.

According to Lule et al, (2012), to modify the model, ie to see which variables are the best at explaining the variance in adoption, factors analysis and structural equation modeling will be is used. Specifically, SPSS 20and AMOS module was used to perform Structural Equation Modeling (SEM). This is Structural Equation Modeling (SEM) software that uses Confirmatory Factor Analysis (CFA) to align the tested measures to the specific constructs and constraining the variances of each measure to the latent construct it should represent. In addition to assessing the degree to which each measure contributes to its latent construct, CFA also tests the separation between constructs by evaluating the fit in the overall model. There are four groups of fit measures and among the many measures of fit, four popular measures were use in this study. $\chi 2$ /df, GFI, TLI and RMSEA.

4. RESULTS AND FINDINGS

In order to establish the statistical significance of the independent variables on the dependent variable (adoption of local software) regression analysis was employed. Table 1 shows that the coefficient of determination also called the R square are 77%. This means that the combined effect of the predictor variables (individual factors, technological factors, organizational factors and environmental factors) explains 77% of the variations in adoption of local software. The correlation coefficient or R of 87.7% indicates that the combined effect of the predictor variables has a strong and positive correlation with adoption of local software. This also meant that a change in the drivers of adoption of local software has a strong and a positive effect on adoption of local software.

Table 1: Regression Model Fitness

Indicator	Coefficient
R	0.877
R Square	0.77
Std. Error of the Estimate	0.27412

Table 2 displays the regression coefficients of the independent variables. The results reveal that individual factors, environmental factors, technological factors and organizational factors are statistically significant in explaining adoption of local software. The findings imply that there is a significant relationship between environmental factors, organizational factors, technological factors, individual factors and adoption of local software.

Table 2: Regression Coefficients

Variable	Beta	Std. Error	t	Sig.
Constant	4.272	0.325	13.157	0.000
Individual Factors	0.471	0.122	3.865	0.001
Technological Factors	-0.059	0.008	-7.375	0.000
Organizational Factors	-0.062	0.011	-5.634	0.000
Environmental Factors	-1.038	0.216	-4.805	0.000

4.1 Combined Model Validation

A combination of constructs for both users and developers was used to generate the final model named TOIE model. The final result values from the developers and the users were added and then divided by two so as to come up with the values of the final model using SPSS software. In the case of the organizational factors the values for the factors were used as they were because it was only in the questionnaire of the developers.

The validation of the model was done by use of Analysis of Moment Structures (AMOS) module. AMOS is add-on module for SPSS. It is a program to assist with structural

equation modeling (SEM).AMOS is always used to help in modification and validation of model.
The Model Test shows that 42% of the variation in adoption is accounted for by the four factors (individual factors, technological factors, environmental factors and organizational factors). This percentage is very low. This requires that some modification should be done to get a percentage more than 50%. The above model shows poor fit as shown by the chi square of 32.274 and a p value of 0.000,degrees of freedom = 6. If the chi-square is significant, the model is regarded, at least sometimes, as unacceptable. The p value should not be significant. It should be more than 0.05 according to Hu and Bentler, 1995
According to James Bowers, Jr., MABen Jarrett in their study and which was adopted by researchers like Arbuckle (2007), Blunch (2008), if a model has a poor fit it can be modified by adding or removing connections, adding variable or dropping variables. To get a model with a good fit I therefore decided to modify the model by adding connections and have correlation between the independent variables.

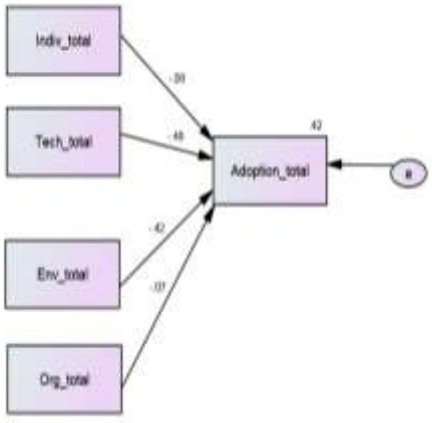


Figure 1: Result of the Model Test

4.2 Validated and Final Model (TOIE Model)

The squared multiple correlations are the proportion of variance that is accounted for by its predictors. The final model in figure 2 shows that 90% of the variation in adoption is accounted for by the four factors (individual factors, technological factors, environmental factors and organizational factors).
Table 2 shows that the model fitness is good. A good fit indicates that the model is fit. This is indicated by a CMIN Value of 14.260 and a p value of 0.65.

Table 2: CMIN

Model	NPAR	CMIN	DF	P	CMIN/DF
Default model	20	14.260	5	0.65	2.852
Saturated model	20	.000	0		
Independence model	5	90.269	15	.000	6.018

The research by Lule et al. (2012) had the standards to be used to show a good fit. The standard values for $\chi 2$ /df, GFI, TLI and RMSEA. The table below shows the standard values used and which were compared with the values which the validated model of TOIE produced.

It was important to look at the regression of the final validated model so as to get the significance values of the validated model and to check if the independent variables were affecting the dependent variable negatively or positively. Table 3 shows the significance and the beta values for both unstandardized and standardized model.

Table 3: Validated model Regression Coefficients

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.
	B	Std. Error	Beta		
(Constant)	1.727	.300		5.759	.000
Individual factors	-.094	.043	-.110	-2.178	.034
Technological factors	-.178	.049	-.272	-3.638	.001
Environmental factors	-.127	.030	-.206	-4.222	.000
Organization factors	.755	.092	.644	8.177	.000

a. Dependent Variable: adoption of local software

The above table shows the regression coefficients of the combined and final model. All the independent variables were significant in predicting adoption of local software. Individual factors, technological factors, Environmental factors and organization factors had p-values of 0.034, 0.001, 0.000 and 0.000 respectively.
Increase in individual factor by one unit decreases adoption of local software by 0.110 while increase in the Technological factors by one unit will decreases adoption of local software by 0.272. On the other hand increase environmental factors by one unit decreases adoption of local software by 0.206. Finally increase in organization factor by one unit increases adoption by 0.644.
Order of importance among the four factors is as follows: Organization factors affect the adoption of local software the most. This is because when the organization develops a good culture towards local software development then they will develop good software with high quality and also when the organization is big and have enough resources they will be able to invest more in the process of software development. Quality things are always expensive. It is then followed by Technological factors; this is because when the software is compatible and is secure more people will use it. Environmental factors are the third factor to affect adoption of local software. Individual factors affect the adoption of local software development but at a low rate. This is because the PEOU and PU can easily change. If a user is told by someone that Oracle is the best software then they can easily believe them and stick to using that Oracle software.

4.3 Validated Model

The validated model in Figure 2 has 90 % coefficient of determination which is a very high percentage indicating that the model is very good. The model has a good Chi-square of 14.260 and p value of 0.65. The higher the probability level (p

value) associated with chi square, the better the fit. Amos reports the value of chi-squre as CMIN. Some of the construct exhibited stronger significance than others, this is through the –ve and +ve values on the figure. The –ve values will decrease the adoption of local software while the +ve values will increase the adoption of local software. The model is generic and can be used in any developing country. In the figure it is clear to view the correlation between the independent variables (covariance) and also the correlation between the independent and dependent variables (regression)

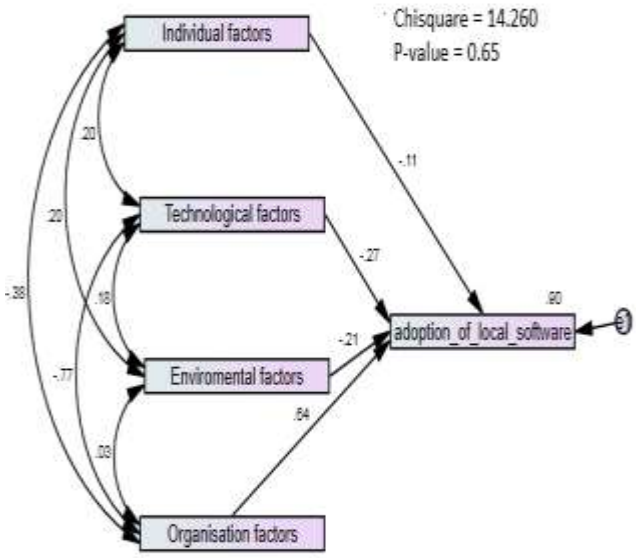


Figure 2: Validated Model

5. CONCLUSIONS AND RECOMMENDATIONS

Based on the objectives and the findings of the study from the users the following conclusion can be made: There was insignificant relationship between adoption of local software and perceived ease of use and regulatory environment. On the other hand there was significant relationship between adoption of local software and perceived usefulness, compatibility and security and privacy. The users need a software which is secure, compatible and useful to them. Developers should therefore consider these factors when developing softwares.

Based on the objectives and the findings of the study from the developers the following conclusion can be made: There was insignificant relationship between adoption of local software and perceived usefulness. There was a significant relationship between adoption of local software and developers` entrepreneurship capabilities, perceived ease of use, organization culture and organization size and resources, industry competition, regulatory environment. The developers of local software should consider these factors when developing.

It is therefore clear that even though some of the factors were not significant to the users, the same factors were important to the developers. This then required the combination of all the factors so as to come up with a final model. When the variables under the four main categories so as to come up with the main factors affecting adoption of local software development. It was therefore clear that perceived usefulness, developers` entrepreneurship capabilities, compatibility and security and privacy perceived ease of use, organization culture and organization size and resources, industry competition, regulatory environment affect the adoption of local software development. The above variables fall under Individual, Technological, organizational and environmental factors. The countries like India, USA, UK and other developing countries have put into consideration when developing and adopting their local softwares and this have made them have an edge over the developing countries.

There was correlation between the independent variables, this shows that they have a relationship to each other. Individual, Technological, organizational and environmental factors relate with each other and must be considered when developing the local software.

The final model is fit when the following four factors were combined, Individual, Technological, Organizational and Environmental factors. All the above factors were significant determinants of adoption of local software. Organization factors affect the adoption of local software the most. It is then followed by Technological factors. Environmental factors are the third factor to affect adoption of local software. Individual factors affect the adoption of local software development but at a low rate. All these factors must be considered when developing software.

The government should use these findings and be able to give tax incentives to the local software developers so that they can be able to invest more in the local software development. Also the government should be able to put strict laws concerning copyright and patents. This will enable the developers or the innovators of the technology to have the full rights on the innovation and be able to sell and meet the market demand.

The final model TOIE consists of the factors which are required in adoption of technology and softwares. It has the individual factors which is lacking in TOE and are very important and also have the Technological, environmental and organizational factors which is lacking in TAM model. It's therefore considered superior than the other earlier models

5.1 Recommendations

The developers must be able to have entrepreneurial knowledge and skills so as to be able to maintain the business and get advantage over the competitors. This is one of the reasons why India is one of the biggest producers of software.

There was a negative and significant relationship between adoption of local software and regulatory environment. It is therefore recommended to the government to give developers of local softwares incentives such as tax breaks and laws that place minimum requirements for development of local softwares and also the laws that will guard the copyright.

It is therefore recommended that when developing local software all the above factors must be considered. This will help to increase the adoption of our own softwares hence improve the economy.

The developers must be able to have entrepreneurial knowledge and skills so as to be able to maintain the business and get advantage over the competitors. This is one of the reasons why India is one of the biggest producers of software.

The model is generic and therefore can be implemented in other developing countries so as to boost the economy of the developing countries. Technology is the key to development.

7. REFERENCES

[1] Arbuckle, J.L (2003). Amos 5.0 Update to the AMOS User's Guide (S. 77-85). Chicago: Small Waters Corp.

[2] Arbuckle J. L.(2012) IBM, SPSS,Amos, 21User's Guide.

[3] Florence Tushabe, Venansius Baryamureeba,PaulBagyenda Cyprian gwang and Peter Jehopiousers (2010) . The Status of Software Usability in Uganda

[4] Gay, L.R. (1981). Educational Research: Competencies for Analysis and Application. Charles E Mairill Publishing Company, A Bell and Howell Company, Collumbus, Toronto; ,London: Cited in Mugenda OM, Mugenda AG (2003) Research Methods: Quantitative and Qualitative Approaches.Afr. Centre Technol. Studies (ACTS) Nairobi, Kenya.

[5] Global Information Technology Report (2006), World Economic Forum, Geneva.

[6] Grenning, J. (2001). Launching XP at a Process-Intensive Company.IEEE Software, Vol. 18, No. 6, pp. 3–9.

[7] Hall, B. H.& Khan, B. (2003). Adoption of New Technology, NBER Working Paper Series.

[8] Hart O. Awa, Ojiabo Ukoha (2012). Proceedings of Informing Science & IT Education Conference (InSITE) pg.582.

[9] Hausmann, R.& Rodrik, D. (2002). Economic development as self-discovery, Kennedy School of Government, Harvard University, Cambridge, Mass, mimeo.

[10] José Carlos Martins Rodrigues Pinho, Ana Maria Soares, (2011). Examining the technology acceptance model in the adoption of social networks, Journal of Research in Interactive Marketing, Vol. 5 Iss: 2/3, pp.116 – 129.

[11] Joseph Ssewanyana Michael Busler (2007). International Journal of Education and Development using Information and Communication Technology (IJEDICT), 2007, Vol. 3, Issue 3, pp. 49-59.

[12] Juhanilivari et al and MadgaHuisman(2007) . The relationship between organizational culture and deployment of systems development methodologies pg (35-58).

[13] Kabugi, N(2013). A New Window into Kenya Software Industry. Retrieved from http://www.standardmedia.co.ke/mobile/?articleID=2000097110

[14] Karlström, D. &Runeson, P. (2006). Integrating agile software development into stage-gate managed product development. Empirical Software Engineering, Vol. 11, No. 2, pp. 203–225.

[15] Lule, I; Omwansa, T. K and Prof. Waema, T. M (2012). Application of Technology Acceptance Model (TAM) in M- Banking Adoption in Kenya. International Journal of Computing and ICT Research, Vol. 6 Issue 1, pp 31-43.

[16] Mugenda, O. M. & Mugenda, A. G. (2003). Research Methods: Quantitative and Qualitative Approaches, Acts Press, Nairobi-Kenya