International Journal of Computer Applications Technology and Research
Volume 7–Issue 04, 158-162, 2018, ISSN:-2319–8656

Addressing Security Issues and Challenges in Mobile Cloud Computing

Nirmal Kumar Gupta
Jaypee University Anoopshahr
Anoopshahr, India

Gaurav Raj
Jaypee University Anoopshahr
Anoopshahr, India

Abstract: The emergence of cloud computing has brought tremendous impact on software organizations and software architecture design. With the development of cloud computing and mobile internet, mobile cloud computing is becoming a new mode of application. With the widespread development of mobile applications and advances in mobile cloud computing, some other forms of requirements and security issues have been emerged. Mobile cloud computing provides resources residing over cloud and services provided for mobile devices. These resources and services from cloud are available for mobile user over their mobile devices. It also provides benefits for developing specialized mobile applications for them. However, increased security and privacy risks exists due to data outsourcing and synchronization over the Internet. This research paper provides the review on mobile cloud computing, its security issues, challenges and suggests some solutions.

Keywords: mobile cloud computing, cloud security, privacy, data security, challenges

1. INTRODUCTION

In today's world of computing, cloud computing has provided a new kind of computing environment different from traditional computing, in which hardware, software and other services are provided on-demand in a virtualized manner. Cloud computing provides a service model which uses the network to access shared resources to access remotely hosted computing resources to the clients for their business needs.

The basic service model of cloud computing utilizes Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Services (IaaS) for providing various services [1]. Mobile Cloud Computing (MCC) is a computing idea which connects mobile computing with cloud computing. MCC combines the benefits of mobile computing and Internet used on mobile devices with cloud computing [2]. That is the reason for MCC to be called as cloud computing services using the mobile Internet. MCC has enabled the data storage and its processing possible outside the mobile device. Instead of storing the software and data over the Internet rather than on a single device, cloud computing seems to provide on-demand access to resources and services. Using MCC the earlier intensive computations performed on mobile devices, storage of data and other control information has been transferred to the cloud and therefore the computing power and resources available with mobile devices are left to be used for some other useful work. It also has facilitated for mobile cloud applications and data storage to be shifted from mobile phones to the cloud, thus enabling the applications and mobile computing to reach a broader range of mobile users, not just smartphone users.

2. MOBILE CLOUD COMPUTING ARCHITECTURE

In MCC, the mobile network and cloud computing are combined to provide the best service to the mobile users. Since data and software is stored over the Internet instead of on a single device, cloud computing is able to provide on-demand access. The application runs on the remote server and sends the results to the user. The overview of mobile cloud computing architecture is shown in Fig. 1. In this architecture, the individual mobile device is connected to the base station of the mobile radio network. There exist Base Transceiver Stations (BTS) which facilitates mobile devices to communicate with the network. Their purpose is to provide an interface to establish a network connection between mobile devices and the network. The requests generated from the users are communicated over the wireless network to the cloud through the mechanism called Authentication, Authorization and Accounting (AAA). Once the requests generated from the users is reached to the cloud, these requests are processed through the cloud controller and corresponding cloud service accesses these requests.

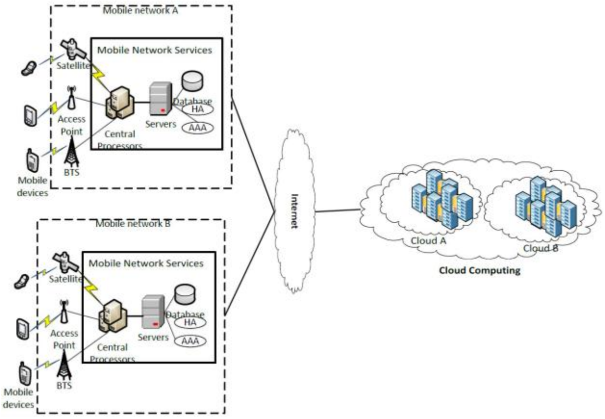

Fig. 1. Mobile Cloud Computing Architecture [3]

3. CHARACTERISTICS OF MOBILE CLOUD COMPUTING

Mobile Cloud Computing has some major characteristics which includes Security, Reliability, Scalability, less maintenance, less cost and platform independence etc. [4]

3.1 Computing as a Service

A very fundamental principle of cloud computing is that it is considered "as a service" where specific services are provided through cloud to its users by the cloud service provider. The services provided in this way are generally categorized based upon the applications used through it [5]. Here are some examples of areas of application offering services: like financial, managerial or analytical. For using the services through the cloud there must be some agreed terms of use between user and service provider. Such an agreement describes the actions which can be taken in case of failure from either side. This failure can result in denial of service to the customer from the service provider or may result in a legal liability for service provider. Besides the actions which could be taken from either side, such agreement also includes a privacy policy which describes the way in which a user's data will be stored and managed for its privacy.

3.2 Service Model

The services provided by cloud computing are generally classified using SPI (SaaS, PaaS, IaaS) model which represents the various levels of services provided by the service provider to the user through the cloud services. Using SPI model the various services such as the software to be used for development of some application, the platform required or other needed infrastructure can be provided in a seamless manner [6]. SPI service model is summarized in Fig. 2.

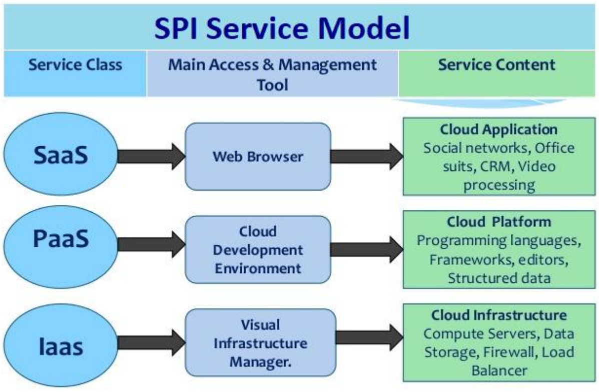
SPI Service Model
Service Class
Main Access & Management Tool
Service Content
SaaS
Web Browser
Cloud Application
Social networks, Office suits, CRM, Video processing
PaaS
Cloud Development Environment
Cloud Platform
Programming languages, Frameworks, editors, Structured data
Iaas
Visual Infrastructure Manager.
Cloud Infrastructure
Compute Servers, Data Storage, Firewall, Load Balancer

Fig. 2. Summary of the SPI Service Model

3.2.1 Software as a Service

The highest layer of SPI model is "Software as a Service" (SaaS). The applications needed by the users are hosted through SaaS layer of SPI model which provides protocols and other services through the network, defined by the service provider. With the development of support technologies for a better web services the use of SaaS is becoming more popular. Once the service provider is chosen carefully security of data can be assured.

3.2.2 Platform as a Service

The PaaS provides the next layer of SPI model which is mostly used as a software development platform by the software developers. This layer provides the services which are used by the developers to write code and manage it through the use of the cloud. In this regard cloud is used to provide development tools and data management and other services required for security.

3.2.3 Infrastructure as a Service

The last and lowest level of SPI model is known as Infrastructure as a Service (IaaS). IaaS is a single-tenant cloud layer where the provider of cloud services provides dedicated resources, which are shared among different customers. Therefore, the requirement of for a large starting investment of various hardware resources including networking devices, servers, switches etc. are minimized. Such provisions provide a greater degree of flexibility in terms of achieved functionality and economically. Such kind of flexibility are generally not available in centralized data and hardware centers. Whenever needed more resources can be added in less time over cloud which can be utilized by the users.

4. SECURITY IN THE MOBILE CLOUD COMPUTING

One of the major issues about MCC is that most cloud providers are concerned about is ensuring the privacy of the user and the integrity of data or applications. Security issues in MCC must be handled in an effective manner because it considered is a combination of mobile networks and cloud computing. We can divide security issues mainly in two categories:

1. Security issues associated with the cloud
2. Mobile network user's security

4.1 Security issues associated with the cloud

The various technologies like virtualization, operating systems, scheduling of resources, database management, concurrency control, load balancing and memory management etc. are included in cloud technologies. This introduces various security related risks in cloud whose intensity and nature may be different than the risks associated with traditional software and services [7]. Figure 3 shows data protection risks to regulated data [8] Network connection dependency and data sharing. Integrating applications and security are some of the major challenges in MCC environment.

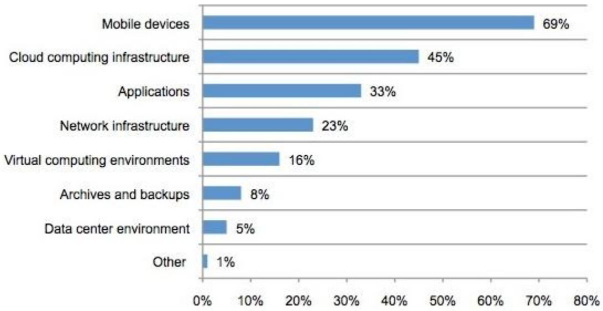

Fig. 3. Data Protection risks in MCC

In MCC, sharing of infrastructure between multiple clients may cause the risk of data visibility by other users. In addition, cloud users want to ensure that critical data is not accessible and utilized illegally, even by cloud providers. Since the web-based interface is used for on-demand services to be provided to clients which causes the probability of unauthorized access to the interface which might be higher than the traditional systems. According to Gartner [9], before making a choice of cloud vendors, users should ask the vendors for seven specific safety issues: Privileged user access, regulatory compliance, data location, data segregation, recovery, investigative support and long-term viability. According to [10], there can be two types of communication, namely, external "customer-to-cloud" communication and internal "cloud-to-cloud" communication. In the first case the cloud services are accessible via the internet using standard internet mechanisms and protocols to transmit data or applications between clients and the cloud. This type of communication is similar to any other communication on the Internet. Indeed, data in transit can be the target of several malicious attacks [9] [10]. These attacks include denial of service (DoS), eavesdropping, identity theft, altered environment etc. The second type is related to the communication between the VMs. This communication is targeted for malicious attacks because of the various factors which includes the shared communication infrastructure, the virtual network, and the bad security configuration. Cloud security has close relationship with the corporate security policies. They must go beyond the difficult requirement of passwords and login privileges. It is necessary to move to the next level and think about security in terms of usage and types of data. The more sensitive they are, the higher the security must be and the more the choice of the type of Cloud is critical and crucial.

The level of security of the public cloud is not optimized for professional use, but its flexibility and value can make it attractive to many small organizations. The Private Cloud is based on the same principle as the public cloud, but it is of course owned by a company and intended for a smaller number of users, customers or partners of the company owner. Finally, the hybrid cloud is a mix of private and public clouds. It is made up of several internal and external partners. Its interest lies in its ability to navigate data between the public and private according to their sensitivity to optimize costs. Regardless of its type, cloud solution providers rely on a mix of proprietary and open source code to ensure the security and integrity of the data they host and protect. According to [11], whatever the form of the Cloud Computing contract is, this contract must absolutely include these five key points, namely, data localization, law and Jurisdiction, service levels provided by the MCC provider, reversibility and access to data and data security. In addition, the order of importance of these five key points will vary according to the service used (IaaS, PaaS, SaaS) and its purpose (storage space, development environment, billing tool).

According to [12], cloud security challenges are the dispersion of international data and privacy laws, the need to be addressed for various issues like local management, multi-tenancy, logging challenges, data ownership issues, and Guaranteed quality of service, dependence of secure H-viewers, interest for hackers, security of virtual OS in the Cloud, possibility of massive interruptions of service, encryption needs for security in the Cloud, public cloud security versus private cloud security etc. According to [13], there are nine main risks, namely Data Breaches, Data Loss, Account Hijacking, Insecure APIs, Denial of Service, Malicious Insiders, Abuse of Cloud Services, Insufficient Due Diligence and Shared Technology Issues. Regarding the legal responsibilities for data security and privacy in the cloud, according to [13], they find that the customer is legally responsible for its data and usage, including anything concerning their compliance with legal obligations, while, the provider is subject to technical and organizational obligations. It is committed to preserving data integrity and confidentiality, protecting and recovering data, encrypting data etc.

4.2 Mobile network user’s security

Some of the security concerns in mobile network user are discussed below:

Loss of control over data: The paradigm of MCC is changing the way information is managed, especially with respect to the processing of personal data. Storing personal data on a server somewhere in cyberspace could pose a great threat to privacy. Because tenants and users lose physical control over their data and applications, this raises a number of issues.

Data security and privacy: With public or community clouds, the data may not remain in the same system, which poses multiple legal problems. The biggest concern that everyone seems to agree with the cloud is security. Data security and privacy are at the forefront of almost all the concerns. The main challenge for MCC is how it addresses the security and privacy concerns of the companies that are considering adopting it [14]. The fact that the company's valuable data resides outside the company's firewall raises serious concerns. Piracy and various attacks on the cloud infrastructure would affect multiple clients, even if only one site is attacked. These risks can be mitigated through the use of security applications, encrypted file systems, data loss software and purchase of security hardware to track unusual server behavior.

Data control: Data can reach the provider in several ways with some data belonging to others. A host administrator has a limited scope of control and accountability within a public infrastructure implementation as a service (IaaS), not to mention a platform as a service (PaaS). Hosts must have confidence that their provider will provide adequate control, while recognizing the need to tailor their expectations to the amount of reasonable control in these models.

Quality of service: quality of service is one of the most important factors that companies consider a reason not to move their commercial applications to the cloud. They consider that SLAs (Service Level Agreements) provided by cloud providers are not currently sufficient to guarantee the requirements to run cloud-based development applications, particularly in terms of availability, performance, reliability and scalability. In most cases, companies are reimbursed for the duration of the non-availability of the service, thus most current SLAs reduce commercial losses [15]. Without a guarantee of service quality, companies will not host their critical infrastructure in the cloud.

Transparency: When a cloud provider does not expose the details of its own internal policy or technology, hosts or users must rely on vendor security claims. Hosts and users may still require some transparency from providers as to how they handle security, privacy, and security incidents in the cloud.

Legal and Regulatory Compliance: It may be difficult or unrealistic to use public clouds if your data is subject to legal restrictions or regulatory compliance. You can expect vendors to create and certify cloud infrastructures to meet the needs of regulated markets. Achieving certification can be a challenge because of the many non-technical factors, including the current state of general knowledge of the cloud. As best practices for MCC encompass a broader scope, this concern should disappear.

Incompatibility Issue: The storage services provided by a cloud service provider may be incompatible with the services of another provider in case some user decides to switch from one to the other. Providers are known for creating what the world of hosting calls "persistent services," services that an end user may have difficulty moving from one cloud provider to another.

Performance and cost of bandwidth: Companies can save money on hardware, but they have to spend more on bandwidth. This can be a low cost for a smaller application, but it can be high for an application that requires a large amount of data. Providing intensive and complex data through the network requires sufficient bandwidth. For this reason, many companies expect a reduced cost before moving to the cloud.

Low Performance of the network: the provision of complex services through the network is clearly impossible if the bandwidth of the network is not enough. Many companies expect improved bandwidth and lower costs before considering switching to the cloud. Many applications in the cloud still consume too much bandwidth.

Integration: Many applications have complex integration needs to connect to other applications in the cloud, as well as other local applications. This includes the integration of existing cloud applications with enterprise applications and existing data structures. It is necessary to connect the application in the cloud to the rest of the company in a simple, fast and profitable way.

5. SOME SOLUTIONS TO SECURITY PROBLEMS IN MCC

The correct implementation of security measures is mandatory in MCC to provide a secure infrastructure that can only ensure and increase confidence that the stored data is safe with the service provider. This can be achieved by the following means:

Data encryption: In the public cloud, resources are shared by multiple users in the cloud and, as a result, the responsibility of their providers is to entrust the separation of data to their customers. Data encryption is a common approach that providers follow to protect their customers' data, but the question is whether the data is stored in encrypted format or not. Many providers follow private/public key encryption to ensure data security. To store critical data, organizations can think of a private or hybrid cloud where the data will be in a secure corporate firewall. An important way to increase data protection, privacy and integrity is to ensure that data is protected in transit and when stored in the cloud by using file-level encryption. As CSA (Cloud Security Alliance) [16] Guidance notes, “Encryption offers the benefits of minimal use of the cloud service provider and dependence on operational failure detection.” Encrypted data-centric protection means that data cannot be used by anyone without the key to decrypt it. It does not matter if the data transmits or is stored, it remains protected. The owner of the decryption keys maintains the security of this data and can decide whom to allow access to what data. Encryption procedures can be integrated into the existing workflow for cloud services. For example, an administrator could encrypt all data in the backup before sending them to the storage cloud. One of the best security solutions for cloud and virtualized environments is portable encryption at the file level, focused on data on all computer platforms and operating systems, and operates in a private, community, public or hybrid cloud.

Refactoring Data: Simply applying the encryption method does not guarantee the security of the data transfer. In the case of data transmission, the greatest risk is related to the encryption technology in use. Instead of using encryption and decryption, the data can be divided into smaller packets that can then be transmitted to the receiver through different routes. Such an approach will reduce the chances of capturing information by unauthorized persons. The data does not make sense unless all the data is received.

Restricted access: Restricted user access can range from simple username/password protection to some challenge-response test in login forms. When an employee no longer needs to access the data center, their access privileges to the data center must be immediately revoked. Cloud providers can also consider password authentication at a time when customers will get a temporary password from the SSN/mobile device, which contributes to data security even if the password is compromised.

Backup and recovery: In MCC, the data is stored in a distributed location. Cloud clients will never be able to determine the exact storage location of their records and the importance of data backup and recovery appears. The backup software must include cloud-based APIs, which allows simple backup and recovery in the main cloud storage providers. The backup and restoration services guarantee that one can always recover the data. A questionable question is whether to back up all the data or make a backup of critical and vital data. If the provider agrees to save crucial data, the question is how to determine the priority of the data. The simplest and least complicated way is to protect the entire workstation or server. It is essential that the backup application encrypts confidential data before sending it to the cloud off-site, protecting data in transit through a WAN to a storage location in the cloud and data storage on the site as cloud storage.

Access control: Access control and management of user profiles become more complex with cloud services because information sources can be hosted somewhere other than the cloud service that needs them. Clients must identify reliable sources for this information and ensure mechanisms to transmit information from the reliable source to the cloud service. It is also important to periodically reconcile the information between the cloud service and the source. Customers must confirm that cloud providers support their access control requirements appropriately for cloud resources.

6. CONCLUSION

Mobile Cloud Computing (MCC) is an emerging and futuristic technology due to the variety of benefits and applications offered to mobile subscribers. The main reason for the possible success of MCC and the great interest of organizations around the world are due to broad category of services provided with the cloud, but the current technology does not provide all the requirements that MCC needs. Researchers face many challenges to make MCC work in reality. Besides the various benefits provided through MCC some security issues need to be addressed to ensure that it is a safe and reliable services could be provided. This paper has discussed some security issues and possible solutions concerning MCC. Securing MCC user’s privacy and integrity of data or applications is one of the major issues most cloud service providers have given attention.

7. REFERENCES

1. Luo, J.Z., Jin, J.H., Song, A.B. and Dong, F., 2011. Cloud computing: architecture and key technologies. Journal of China Institute of Communications, 32(7), pp.3-21.

2. Dinh, H.T., Lee, C., Niyato, D. and Wang, P., 2013. A survey of mobile cloud computing: architecture, applications, and approaches. Wireless communications and mobile computing, 13(18), pp.1587-1611.

3. Prasad, M.R., Gyani, J. and Murti, P.R.K., 2012. Mobile cloud computing: Implications and challenges. Journal of Information Engineering and Applications, 2(7), pp.7-15.

4. Padma, M. and Neelima, M.L., 2014. Mobile Cloud Computing: Issues from a Security Perspective. International Journal of Computer Science and Mobile Computing, 3(5), pp.972-977.

5. Krutz, R.L. and Vines, R.D., 2010. Cloud security: A comprehensive guide to secure cloud computing. Wiley Publishing.

6. Mell, P. and Grance, T., 2009. Effectively and securely using the cloud computing paradigm. NIST, Information Technology Laboratory, 2(8), pp.304-311.

7. Ali, M., Khan, S.U. and Vasilakos, A.V., 2015. Security in cloud computing: Opportunities and challenges. Information Sciences, 305, pp.357-383.

8. Donald, A.C., Oli, S.A. and Arockiam, L., 2013. Mobile cloud security issues and challenges: A perspective. International Journal of Electronics and Information Technology (IJEIT), ISSN, pp.2277-3754.

9. Gartner: Seven cloud-computing security risks. InfoWorld. 2008-07-02.

http://www.infoworld.com/d/security-central/gartner-seven-cloudcomputing-security-risks-853.

10. Chen, S., Nepal, S. and Liu, R., 2011, September. Secure connectivity for intra-cloud and inter-cloud communication. In Parallel Processing Workshops (ICPPW), 2011 40th International Conference on (pp. 154-159). IEEE.

11. Rohrmann, C.A., Cunha, S.R. and Falci, J., 2015. Some legal aspects of cloud computing contracts. J. Int't Com. L. & Tech., 10, p.37.

12. Kshetri, N., 2013. Privacy and security issues in cloud computing: The role of institutions and institutional evolution. Telecommunications Policy, 37(4), pp.372-386.

13. Los, R., Shackleford, D. and Sullivan, B., 2013. The notorious nine cloud computing top threats in 2013. Cloud Security Alliance.

14. Bhadauria, R. and Sanyal, S., 2012. Survey on security issues in cloud computing and associated mitigation techniques. arXiv preprint arXiv:1204.0764.

15. Das, S., Kagan, M. and Crupnicoff, D., 2010. Faster and efficient VM migrations for improving SLA and ROI in cloud infrastructures. DC CAVES.

16. Everett, C., 2009. Cloud computing–A question of trust. Computer Fraud & Security, 2009(6), pp.5-7.