International Journal of Computer Applications Technology and Research
Volume 3– Issue 5, 309 - 311, 2014, ISSN: 2319–8656

Encrypted Query Processing Based Log Management in the Cloud for Improved Potential for Confidentiality

Nimmy Prabha
PPG Institute of Technology
Coimbatore, Tamil Nadu
India

C.Timotta
PPG Institute of Technology
Coimbatore, Tamil Nadu
India

Tina Rajan
PPG Institute of Technology
Coimbatore, Tamil Nadu
India

Abdul Jaleef P.K
PPG Institute of Technology
Coimbatore, Tamil Nadu
India

Abstract: To address privacy concerns current implementation allows access to log records that are indirectly identified by upload-tag values. We plan to propose a practical homomorphic encryption schemes that will allow encryption of log records in such a way that the logging cloud can execute some queries on the encrypted logs without breaching confidentiality or privacy. Anonymous network implement the anonymity of users and provide privacy. In this paper implement the anonymous of user by implementing anonymous tag generation. CryptDB is a system that provides practical and provable confidentiality in the face of these attacks for applications backed by databases. It works by executing queries over encrypted data using a collection of efficient aware encryption schemes.. It greatly reduces the communication overhead between a log monitor and the logging cloud needed to answer queries on logs.

Keywords: Cloud computing, Homomorphic encryption, CryptDB, logging, privacy, k-anonymity.

1. INTRODUCTION

Logs are composed of log entries each contain information related to a specific event that has occurred within the system. Logs which contain records related to computer security. Log management is essential to ensuring that computer security records are stored in sufficient detail for an appropriate period of time. Routing log analysis is beneficial for identifying security inciden[1]t, policy violation fraudulent activity and operational problem.

Organization also need to protect the availability of their log. Many log have maximum size ,since as storing 10,000 most recent events or keeping 100 mega bytes of log data when the size limit is reached the log might over write the older data with new data or stop logging together both of which would causes of loss of log data availability. Over writing will cause the loss of old data or log, if log is important it will cause problems. Logs serve many functions with most organization such as optimizing system and network performance, recording the action of users and providing data useful for investigate malicious activity.

Log generation and storage can be complicated by several factors including a high number of log sources: inconsistent log content format and time stamp among source and increasingly large volume of log data. To keep the large volume of log data, cloud is used, because of its flexibility property[17] the size of storage area can be increased whenever needed, no over writing process occur. Clouds are large pool of easily usable and accessible virtualized resources. Cloud computing allows consumes and business to use application without institution and access their personal files at any computer with internet access. Cloud providers have a strong incentive to maintain trust and as such empty a higher level of security[8]. The log records stored in the cloud will be more secure.

2. RELATED WORK

For network wide logging protocol Syslog[2] is standard one. UDP is used for transfer of log file. The main disadvantage for the syslog is, at the time of transfer of log record, the log file is not protected. Many approaches are developed to protect the log files Based on some cryptographic protocol. The approaches are syslog are syslog pseudo, syslog ng, reliable syslog[3] and forward integrity[5]. Syslog ng [6]is the next approach after syslog. The protection of log record during the transfer can be achieved in syslog ng.

The encryption of log files by SSL. The advantages of syslog ng are not protecting the data modification at the end point. If the authentication process is implemented this issue can be overcome. In syslog sign[7] implement authentication of user. Authentication at origin and the detection of missing messages is implemented in the syslog sign. The reliability of log record can be achieved by detection of missing messages by adding two certificate block i.e. certificate block and signature block. For pseudonymising log file[9] the next approach is proposed i.e. syslog. The disadvantage of this

approach is confidentiality and integrity of log file cannot be achieved. Reliable syslog[4] provide the device authentication and protect the integrity of log message. key generation technique in the cryptographic protocol is introduced in the forward integrity protocol. Different keys are generated foe every log file.

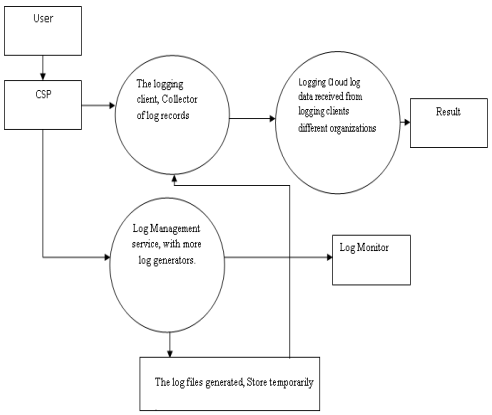
3. SYSTEM ARCHITECTURE

Cloud server: The same cloud server will store the log data from different users. The cloud service provider maintain the cloud server.

Log user: The log user receive the log record from the cloud server. The log data is transferred from the generator to the user in batches. The log user incorporate security protection on batches of accumulated log data and pushes each batch to the logging cloud.

Log generator: The temporary storage of log file in generator. The log files are divide into log batches and the encryption of log batches and key generation are take place in log generator.

Log Monitor: Log monitor generates queries to retrieve log data from cloud server. Based on the log data retrieve the log monitor performs analysis as needed. For monitor and review the log data, the function of log monitor.



The log monitor first accepts this tag and the log monitor generate another half tag then send to the cloud server. First tag generate then user upload log file to the cloud server with the help of this tag generation. The user want to retrieve the log data from cloud serve, the user should send the tag for retrieve this data.

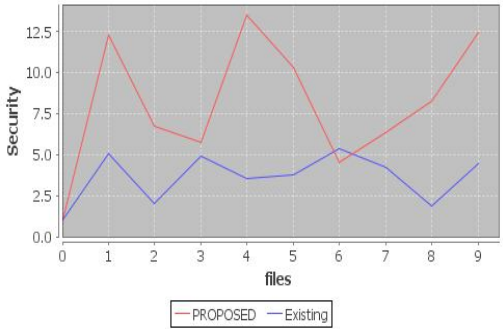
With the help of this tag cloud server or the log monitor check the user is authenticated or not. K-time Authentication protocol[21] is used here for authentication process .The cloud server contain the encrypted log data with the upload tag. The encryption of log record using different techniques.Proactive secret sharing[20] is used. During encryption public[16] and private key are the main content in the encryption.The upload tag is generated by using two half tag. One with the log monitor and user and another one with the log monitor and cloud server. So because of this the attacker attack the cloud server, they did not get details about the log data.

In a network privacy is the main concern, the solution for the privacy can be provided by anonymous communication[14][15]. he privacy in the network mean to protect from unknown spectators which causes threat to the organization. The main aim of anonymous communication in network is without releaving the organization identity, the organization can communicate with cloud for their use.

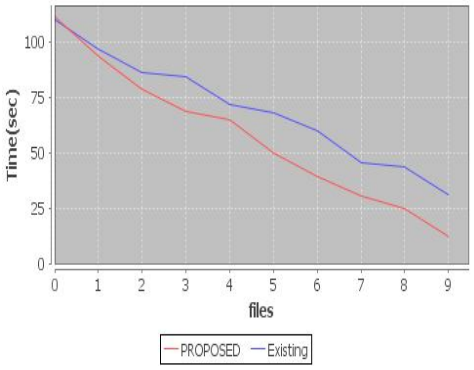
Cloud provide service to many organization or same cloud server store log data from different users. So privacy issues will occur in the cloud. By providing the anonymity[10] these can be controlled. The cloud server accepts log data only from authorized user. The user became authorized by generating an upload tag and send to the cloud server through log monitor.

4. ANALYSIS

The level of security is shown in graph. The graph shows security level of proposed system and existing system. The graph shows the security issues when adversary party get the sensitive information. The security of log files on the basis of encryption techniques[19] used in the existing system and the proposed system. In the proposed system the encryption of log file by homomorphic encryption. After evaluation of both existing and proposed system, homomorphic encryption is efficient one.



The computation time of both proposed system and existing time is show in the below graph. The protocol at the log client side starts by generating an initial set of keys[13] that are distributed to the remote shares repositories (implemented on the same machines as the log generators) to satisfy the Shamir secret sharing[17] scheme. The batch is uploaded to the cloud with appropriate upload and deletes tags included in the packet object.



5. HOMOMORPHIC ENCYPTION

The main idea in encryption technique is to conversion of plain text to cipher text. The encrypted data undergone some complex mathematical operation without compromising the encryption. Homomorphic encryption allows some mathematical operation at the time of encryption and decryption. The encryption of data occur on datas which divided into batches. While batches formed and rejoined the relationship among these batches is preserving.

In cloud computing homomorphic techniques played an important role in encryption . Selected mathematical operation is supported in partial homomorphic encryption techniques[18].This technique is independent to the number of cipher text generated. Main issue in partial homomorphic technique is: only selected mathematical operations supported. To overcome this issue fully homomorphic technique can use. In fully homomorphic techniques almost all type of mathematical operation can supported..

6. CONCLUSIONS

In proposed homomorphic encryption schemes to encrypt the log records. In that the logging cloud can execute some queries on the encrypted logs without breaching confidentiality or privacy[12]. A system that provides a practical and strong level of confidentiality in the face of two significant threats confronting database-backed applications: curious DBAs and arbitrary compromises of the application server and the DBMS. CryptDB meets its goals using three ideas: running queries efficiently over encrypted data using a novel encryption strategy, dynamically adjusting the encryption level using onions of encryption to minimize the information revealed to the untrusted DBMS server, and chaining encryption keys to user passwords in a way that allows only authorized users to gain access to encrypted data. The implementation of the logging client is loosely coupled with the operating system based logging.

7. REFERENCES

[1] K. Kent and M. Souppaya. (1992). *Guide to Computer Security Log Management, NIST Special Publication800-92*[Online].Available: http://csrc.nist-.gov/publications/nistpubs/80092/SP800-92.pdf

[2] Sarbanes-Oxley Act 2002. (2002, Sep.). *A Guide to the Sarbanes-Oxley Act* [Online]. Available: http://www.soxlaw.com.

[3] C. Lonvick, *The BSD Syslog Protocol*, Request for Comment RFC 3164, Internet Engineering Task Force, Network Working Group, Aug. 2001.

[4]D. New and M. Rose, *Reliable Delivery for Syslog*, Request for CommentRFC 3195, Internet Engineering Task Force, Network Working Group, Nov. 2001.

[5] M. Bellare and B. S. Yee, "Forward integrity for secure audit logs," Dept. Comput. Sci., Univ. California, San Diego, Tech. Rep., Nov. 1997.

[6] BalaBit IT Security (2011, Sep.). *Syslog-ng—Multiplatform Syslog Server and Logging Daemon* [Online].Available: http://www.balabit.com/network-security/syslog-ng

[7] J. Kelsey, J. Callas, and A. Clemm, *Signed Syslog Messages*, Request for Comment RFC 5848, Internet Engineering Task Force, Network Working Group, May 2010.

[8] D. Ma and G. Tsudik, "A new approach to secure logging," *ACM Trans. Storage*, vol. 5, no. 1, pp. 2:1–2:21, Mar. 2009.

[9] U. Flegel, "Pseudonymizing unix log file," in *Proc. Int. Conf. Infrastruture Security*, LNCS 2437. Oct. 2002, pp. 162–179.

[10] C. Eckert and A. Pircher, "Internet anonymity: Problems and solutions,"in *Proc. 16th IFIP TC-11 Int. Conf. Inform. Security*, 2001, pp. 35–50 .

[11] M. Rose, *The Blocks Extensible Exchange Protocol Core*, Request for Comment RFC 3080, Internet Engineering Task Force, Network Working Group, Mar. 2001.

[12] B. Schneier and J. Kelsey, "Security audit logs to support computer forensics," *ACM Trans. Inform. Syst. Security*, vol. 2, no. 2, pp. 159– 176, May 1999.

[13] J. E. Holt, "Logcrypt: Forward security and public verification for secure audit logs," in *Proc. 4th Australasian Inform. Security Workshop*, 2006, pp. 203–211.

[14] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second generation onion router," in *Proc. 12th Ann. USENIX Security Symp.*, Aug. 2004, pp. 21–21

[15] The Tor Project, Inc. (2011, Sep.) *Tor: Anonymity Online* [Online]. Available: http://www.torproject.org

[16] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Trans. Inform. Theory*, vol. 29, no. 2, pp. 198–208, Mar. 1983.

[17] Rajiv R Bhadari and Nithin Mishra"Encrypted IT Auditing and Log Management on Cloud Computing" IJCSI,Vol 8,Issue No:1,September 2011.

[18] G. R. Blakley, "Safeguarding crypRtographic keys," in *Proc. Nat. ComputConf.*, Jun. 1979, p. 313.

[19] Sashank Dara "Cryptographic Challenges for computational Privacy in public clouds",CISCO system India pvt Ltd, 2011.

[20] Simarajeet Kaur" Cryptography and Encryption in Cloud Computing"VSRD_IJCS, vol2(3)242-245.

[21] I. Teranishi, J. Furukawa, and K. Sako, "*k*-times anonymous authentication (extended abstract)," in*Proc 10th Int. Conf. Theor. Appl. Cryptology InforSecurity*, LNCS 3329. 2004, pp. 308–322.