Survey on cloud database security using onion encryption techniques

Meera Gor [1], Prof.Gayatri Jain [2]

[1]CE, LJIET, GTU
Ahmadabad, Guajarat , India
Meegor29@gmail.com

[2]CE, LJIET, GTU
Ahmadabad, Guajarat, India
Gayatree.jain@gmail.com

Abstract
Cloud provides facilities to their client database storage to keep data on demand. Data stored on third party sever so security of data is main concern. There is data can be store in encrypted form but it is not convent to every time download encrypted data, decrypt and modify them and again encrypt data and upload on cloud storage. Their solution is layer of encryption on data which secure the data in layer on encryption algorithm and query which execute on data is also encrypted on encrypted data and get data. Onion encryption technique is one of them. This paper gives the survey of this technique and other aspects.

Keywords: *database security, onion Encryption, layer structure*

1. Introduction

Database service model provide users power to create, store, modify and retrieve data from anywhere in the world as long as they have access to the internet. It introduces several challenges, an important issue being data privacy [8]. Where critical information is placed in infrastructures of entrusted third parties, ensuring data confidentiality is of paramount importance [2].Data outsourcing has become a widely used data service. A growing number of data owners tend to upload their local database to the cloud server and rely on its fast and robust services for query processing and storage management, such as file backup, file synchronization, or file sharing[4].Database Security key Issue: Data Confidentiality, Data Access Controllability, and Data Integrity

2. Reviewed Paper

In this section first described a paper which focuses on onion encryption technique to securely store data on third party server. There is paper which also shows the possible attack on this.

Technique and also addresses the benefits of the technique.

In This Paper[1], author Luca Ferretti, Fabio Pierazzi, Michele Colajanni, and Mirco Marchetti are proposed model and a methodology that allow a renter to estimate the costs of plain and encrypted cloud database services even in the case of workload and cloud price variations in a mid-term . By instantiating the model with actual cloud provider prices, they can settle on the encryption and adaptive encryption cost of data confidentiality. Proposed architecture where each client executes an encryption engine that manages encryption operations. This software module is accessed by external user applications through the encrypted database interface.

In this paper[2] Author Luca Ferretti, Michele Colajanni, and Mirco Marchetti they propose a architecture that integrates cloud database services with data confidentiality and the possibility of executing concurrent operations on encrypted data. This is the first solution supporting geographically distributed clients to connect directly to an encrypted cloud database, and to execute concurrent and independent operations including those modifying the database structure. The proposed architecture has the further advantage of eliminating intermediate proxies that limit the elasticity, availability, and scalability properties that are basic in cloud-based solutions. The efficacy of the proposed architecture is evaluated through theoretical analyses and extensive experimental results based on a prototype implementation subject to the TPC-C standard benchmark for different numbers of clients and network latencies. Standard benchmark shows that the performance impact of data encryption on response time becomes negligible because it is masked by network latencies that are typical of cloud scenarios.

In this paper[3] Ihsan H. Akın, Berk Sunar they proposed practical and secure middleware to protect database deployed on semi-honest cloud servers. They target web applications that run CryptDB in the multiuser setting. Therefore all queries and data are relayed through a trusted proxy server which also maintains the master key. As it turns out that online attacker or malicious database administrator by tampering with the integrity of the CryptDB protected database entries, which are communicated between the database server and the proxy server, can recover sensitive information of other users through any user account on the web application. Even worse, the administrator can easily escalate the privilege level of his web application account to that of an administrator. What is unusual is that these attacks are possible without attacking the proxy and the web application server in any way. they show that even when the integrity of the database is protected, by manipulating the queries with the aid if a simple user account on the web application with no additional privileges, the online attackers or DBA can scan the CryptDB protected database for sensitive information on specific victims by tampering with the queries. Finally, they demonstrated with a simple example, that frequency analysis attacks cannot be taken lightly and deserve more serious attention.

In this paper[4] Shurong Ping, Haiqin Wu, Liangmin Wang they define a new cipher text retrieval method. In this method, the database is divided into several block encryptions, and each block encryption is assigned to an index file correspondingly. The index files are encrypted with onion encryption, which allows the server to execute the queries while protecting data Confidentiality. The experiment indicates that this encryption scheme can improve the efficiency of encrypted database retrieve. And encrypt the database with AES algorithm in ECB. The proxy uploads encrypted block and index files to the cloud server. The proxy intercepts all the SQL queries and gives the keys to cloud server in order to perform onion decryption using the UDFs. Finally, the cloud returns the encrypted data block as a result. The experimental results indicate that the encryption scheme in this paper has higher query efficiency than others.

In this paper[7] Author Carlo Curino,Evan P. C. Jones,Raluca Ada Popa,Nirmesh Malviya,Eugene Wu,Sam Madden,Hari Balakrishnan,Nickolai Zeldovich in this paper Relational Cloud overcomes three significant challenges: efficient multi-tenancy, elastic scalability, and database privacy. For privacy, they developed the notion of adjustable privacy and showed how using different levels of encryption layered as an “onion” can enable SQL queries to be processed over encrypted data. The key insight here is for the client to provide only the minimum decryption capabilities required by any given query.

In this paper[5] Prakruti Chandrashekar, Sashank Dara they propose storage efficient SQL-aware encrypted databases that preserve the format of the fields. The fundamental architecture of our modified version is same as CryptDB .In our modified FP-CryptDB they preserve the formats and lengths of the input strings. They choose Flexible Naor and Reingold (FNR), which is a length preserving block cipher for inputs 32 to 128 bits . it preserve the lengths and formats while encrypting IPv4 , Time Stamps thay also give experimental results of storage improvements in CryptDB using FNR encryption scheme. And also explore the feasibility of adopting Format Preserving Encryption for SQL-aware encrypted databases. Experimental results show approximately 50% storage efficiency in FP-CryptDB. The performance degrades in the case of FP-CryptDB as compared to CryptDB. It could be noticed that the performance degrades y _ 7x times.

In this paper[8] Author Ziynet Nesibe Dayıo glu, Mehmet Sabir Kiraz, Fatih Birinci, and ˙Ihsan Haluk Akın ,In paper they define CryptDB as given. CryptDB is a new database management system for protecting data confidentiality while preserving confidentiality and performing a standard set of SQL queries in an efficient way. CryptDB seems to be practical compared to other attempts at solving the problem of computing with encrypted data and the database can be fully moved to the Cloud with no security concern because all the data are already encrypted and never revealed to the database administrator. CryptDB is the first practical Database Management System for running most standard queries on encrypted data. It does not make any changes to the DBMS. That the current search algorithm is not enough to meet all the search queries. They give a detailed analysis about the efficiency and security aspects. With some modification to the current form, the system Can be more secure and can provide all necessary functionality in order to execute all possible queries.

In the paper[9] author Faisal Shahzad, Waheed Iqbal, Fawaz S. Bokhari they use cryptDB for securing E-health data in cloud. Various laws require the privacy of this data to be ensured and usually this is achieved using strict access control methods. they identify that CryptDB successfully provides the data confidentiality on the database server when deployed on the cloud. they also find that for a mix workload, the average performance of the OpenEMR with CryptDB in the cloud remains under two seconds which makes CryptDB a viable option for providing security to EHR systems deployed in the cloud. This is the first study to integrate CryptDB with OpenEMR and to profile performance overhead to ensure. We evaluated CryptDB under light, medium and heavy user load and observed that CryptDB when deployed on the cloud successfully provides the data confidentiality on the database server. they observed a better performance of CryptDB in terms of less average response time when deployed on cloud testbed as opposed to results generated in local testbed. For a mix of workloads, the average performance of the OpenEMR with CryptDB in cloud testbed remained under two seconds. This study suggests that CryptDB is a viable option for providing security to EMR systems deployed in the cloud. the data confidentiality under different deployment and varying workload scenarios in the cloud.

3. Research Gape

Confidentiality and unauthorized access in data security is main concern. Still there is authentication and privacy of data is not achieved. Data security in third party server is still and essential for the public cloud and there also loophole in provided systems.

4. Conclusion

After survey of this paper we can conclude that the onion layer encryption is secure and provide better data security in third party server but it does not provide the authenticity of the use and there is some attack is possible on it and also get the idea to prevent from attack.

Acknowledgement

I would like to thanks my faculty member who guided me when I needed help, also like to thank every person who help me and guide me in this work by their experience and knowledge.

Reference

[1]L. Ferretti, F. Pierazzi, M. Colajanni and M. Marchetti, "Performance and Cost Evaluation of an Adaptive Encryption Architecture for Cloud Databases", IEEE Transactions on Cloud Computing, vol. 2, no. 2, pp. 143-155, 2014.

[2]L. Ferretti, M. Colajanni and M. Marchetti, "Distributed, Concurrent, and Independent Access to Encrypted Cloud Databases", IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 2, pp. 437-446, 2014.

[3]I. Akin and B. Sunar, "On the Difficulty of Securing Web Applications Using CryptDB", 2014 IEEE Fourth International Conference on Big Data and Cloud Computing, 2014.

[4]S. Ping, H. Wu and L. Wang, "Block-Based Method and Its System for Outsourcing Data by Using Onions of Encryption", 2015 Third International Conference on Advanced Cloud and Big Data, 2015.

[5]C. Örencik and E. Savaş, "An efficient privacy-preserving multi-keyword search over encrypted cloud data with ranking", Distributed and Parallel Databases, vol. 32, no. 1, pp. 119-160, 2013.

[6]P. Chandrashekar, S. Dara and V. Muralidhara, "Efficient Format Preserving encrypted databases", 2015 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), 2015.

[7] Curino, Carlo et al. "Relational Cloud: A Database-as-a-Service for the Cloud." 5th Biennial Conference on Innovative Data Systems Research, CIDR 2011, January 9-12, 2011 Asilomar, California.

[8] Z. N. Dayıo ˘ glu, M. S. Kiraz, F. Birinci, and ˙I. H. Akın, “Secure Database in Cloud Computing:CryptDBRevisited,”INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE, vol. 3, no. 1, 2014.

[9] F. Shahzad, W. Iqbal, and F. S. Bokhari, “On the use of CryptDB for securing Electronic Health data in the cloud: A performance study,” 2015 17th International Conference on E-health Networking, Application & Services (HealthCom), 2015.

First Author: Meera K. Gor Pursuing master degree in computer engineering from, LJIET(GTU) and meegor29@gmail.com
Second Author: Prof.Gayatri S. Pandi(Jain).Presently, She is Head of the Department in PG Department of LJIET, Ahmdabad and gayatree.jain@gmail.com