Enhancement of database security in cloud using onion layer encryption technique

M e e r a G o r [1] , P r o f . G a y a t r i s . j a i n (p a n d i) [2]

[1]CE, PG-Department, LJIET
Ahmadabad,Gujarat, India
Meegor29@gmail.com

[2]CE, PG-Department, LJIET
Ahmdabad,Gujarat, India
Gayatree.jain@gmail.com

Abstract

Cloud provides various services to make task easy and done remotely. One of the services cloud provides is database storage or database as service. Transmitting data from client machine to cloud database is not safe in terms of confidentiality, integrity and privacy of data. Cryptography for security is general way to secure or encrypt the data. Here we proposed a model for encrypting database in not one layer but more than two layer of encryption using onion layer of encryption technique which provide database security in layer of encryption so data are more secure and confidential while transmitting to the cloud database and result of the model is increased the confidentiality and integrity of database.

Keyword: *cloud, database as service, onion encryption, confidentiality, integrity.*

1. Introduction

Database service model provide users power to create, store, modify and retrieve data from wherever in the world as long as they have access to the internet. It introduces a number of challenges, an important concern being data privacy [8]. Where important information is located in infrastructures of entrusted third parties, ensuring data confidentiality is of paramount importance [2]. Data outsourcing has become a usually 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 strong 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.

Data as a service (DaaS) and Database as a service (DBaaS) are the different conditions used for data management in the Cloud. They differ on the basis of how data is stored and managed. Cloud storage is virtual storage that enables users to store documents and stuff. Drop box, Cloud. Are popular cloud storage services. DaaS allows user to store data at a remote disk available through Internet. Cloud storage cannot work without basic data management services. So, these two terms are used interchangeably. DBaaS is one step ahead. It offers complete database functionality and allows users to access and store their database at remote disks anytime from any place through Internet. Amazon's SimpleDB, Amazon RDS, Google's Big Table, Yahoo's Sherpa and Microsoft's SQL Azure Database are the commonly used databases in the Cloud.

2. Related work

Where critical information is located in infrastructures of entrusted third parties, ensuring data confidentiality is of paramount importance. 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 space management, such as file backup, file synchronization, or file sharing. Motivated by drastic savings in hardware, software, and IT costs cloud computing gained mainstream popularity. However, due to the unprecedented level of data sharing cloud computing also gave rise to new security concerns. For instance, despite intense efforts by the research community, secure cloud based data storage has remained elusive. While standard encryption techniques provide a baseline solution, they are too rigid, i.e. further useful operations on encrypted data such as text search, or standard aggregation operations on encrypted databases are difficult to maintain in a practical approach. Especially given the range of queries supported by databases such as point, range, and collection queries the task at hand becomes even more complex.

Onion layer structure is mainly having two methods for the encryption of the cloud database. They both use the same schema to secure the database difference is that SQL-aware method predefine the layer of the encryption on database but in adjustable query-based encryption method is dynamically select the layer of encryption.

1. SQL-aware method
2. Adaptive method

Onions of encryption is an encryption scheme which was first planned in database software called CryptDB raised by Computer Science and Artificial Intelligence Laboratory (CSAIL) of Massachusetts Institute of Technology (MIT). CryptDB is a DBMS that can protect confidentiality of data though executing the encrypted query. Main characteristic of CryptDB is onions of encryption. This encryption scheme encrypts data into multiple encryption layers, and each layer simply supports a specific query operation. A key part of CryptDB is adjustable query-based encryption, which can dynamically adjust onions to the most appropriate encrypted layer that enables executing the most requested queries.

3. Literature survey

Onion encryption technique to securely store data on third party server. There is paper which also shows the potential attack on this. Technique and also addresses the benefits of the technique.

In Paper[1], author Luca Ferretti, Fabio Pierazzi, Michele Colajanni, and Mirco Marchetti are proposed model and a methodology architecture where each client executes an encryption engine that manages encryption operations. This software component is accessed by external user applications throughout the encrypted database interface.

In this paper[2] Author Luca Ferretti, Michele Colajanni, and Mirco Marchetti they proposed architecture has the further improvement of eliminating intermediate proxies that limit the flexibility, availability, and scalability properties that are basic in cloud-based solutions

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 in the same way. The index files are encrypted with onion encryption, which allows the server to execute the queries while defensive data Confidentiality. The experiment indicates that this encryption scheme can improve the efficiency of encrypted database take back

In the paper[9] author Faisal Shahzad, Waheed Iqbal, Fawaz S. Bokhari they 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 effectively provides the data confidentiality on the database server when deployed on the cloud.

4. Proposed method

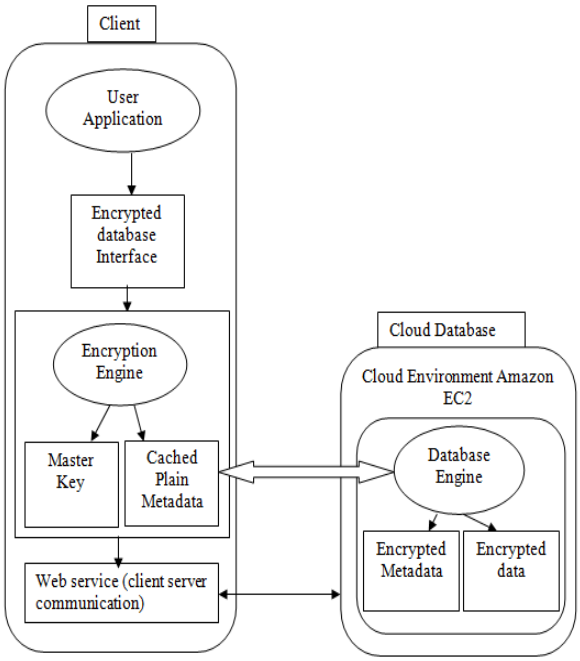
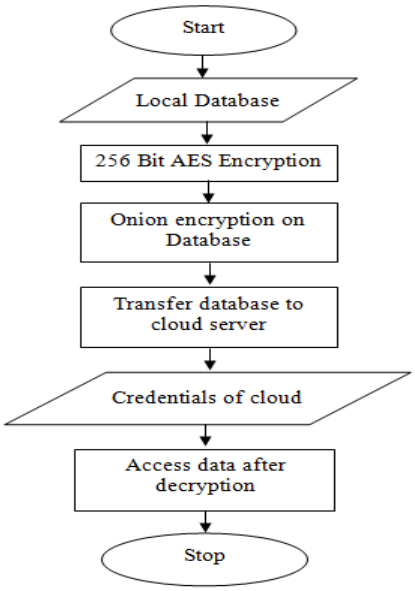


Fig.1.Proposed model

The proposed system support adaptive encryption method for database security in public cloud. Proposed system provides data confidentiality and integrity using onion encryption technique using AES 256 bit algorithm.

Encrypted data is stored in the cloud database; Plain metadata represent the further information that is required to execute SQL operations on encrypted data; Encrypted metadata is the encrypted version of the metadata that are stored in the cloud database; Master key is the encryption key of the encrypted metadata that is distributed to legitimate clients. Web service (client server communication) communicates between client and the server Database is at Amazon EC2 Cloud environment. Proposed model ensure its effectiveness and efficiently eliminate the limitation of computations on values encrypted for different principle. In proposed model data encrypted in column level, row level, table level, and entire database .we can see database format is not changed when data is encrypted. And decryption of database can be done by the authorized person only.AES 256 bit encryption is most secure algorithm in cryptography encryption.

Fig.2: Flow diagram of proposed model



5. Experiment and Result

Implementation of this proposed work required minimum configuration of hardware and software is Amazon ec2 instance with Intel Xeon processor and 4 GB RAM, 100 GB HDD having Microsoft server 2012 (64 bit) Operating system and Java 8, My SQL software must be installed to implement the above proposed work.

Fig.3: Encrypted database

Fig.4: Encrypted database

In Fig.:3 shows source address of data and destination of the database where encrypted database is stored. Fig.:4 show the encrypted database where database, table attribute and row of table are in encrypted form.Fig.5 shows the encrypted database in Table form

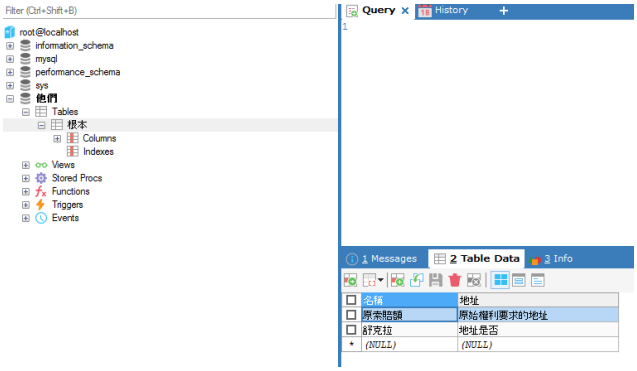


Fig.5: Encrypted database in table form

We can have almost 100% security because it is near impossible crack the 256 bit AES Encryption Algorithm. By providing security with the Integrity and Confidentiality makes the data more secure while data transfer. Thus, securing data remains an important priority of cloud managers to prevent global cloud security threats.

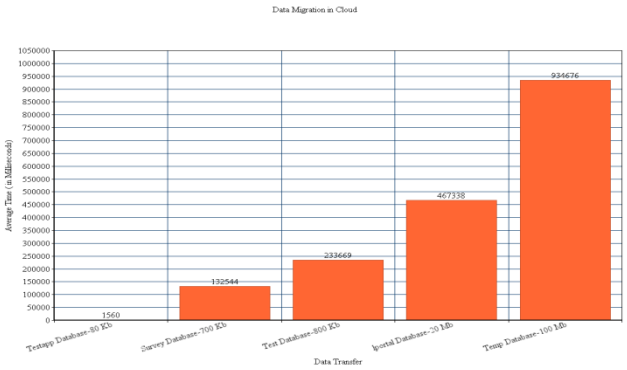


Fig.6: Graph data migration in cloud

Above graph shows data migration which is average time v/s data transfer in millisecond which indicates the transfer rate increases as data increases.

6. Conclusions

Nowadays cloud is getting more and more explored by researchers and organization because of their need and easy sharing functionality. Cloud database as service provide database storage for private and public data for personal or business oriented both. In both way database security is common issue in cloud. In this we proposed framework which provide data confidentiality and Integrity by onion layer structure using adaptive encryption method which encrypt the entire database in layer and the to retrieve data execute query is also in encrypted form the data can't be retrieve by the unauthorized person. Which make the database secure by confidentiality and integrity.

Acknowledgments

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.

References

[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, no.1,pp120-180,2014,.

[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,no. 3,pp. 90-120, 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),no. 1,pp. 104-140, 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]N. vurukonda and B. Rao, "A Study on Data Storage Security Issues in Cloud Computing", *Procedia Computer Science*, vol. 92, pp. 128-135, 2016.

[9]"Oracle Software Downloads | Oracle Technology Network | Oracle", *Oracle.com*, 2017. [Online]. Available http://www.oracle.com/technetwork/indexes/downloads/index.html#java. [Accessed: 15- Mar- 2017].

[10]"Cryptography & Network Security-Atul Kahate", *Scribd*, 2017. [Online]. Available: https://www.scribd.com/doc/159080504/Cryptography-Network-Security-Atul-Kahate. [Accessed: 15- Mar- 2017].

[11] "Survey on cloud database security using onion encryption techniques." Gor, Meera, and Gayatri Jain. *database* 1.6 (2016).

First Author: Miss. Meera gor, Masters of computer engineering student at LJIET, Ahmdabad.

Second Author: Prof. Gayatri s. Pandi(jain),Head of the department, LJIET , ahmdabad.