ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Secured Encryption System for Multiple Cloud Users

Somnath Hande[1], Sampat Medhane[2]

M Tech [IT] Student, Dept. of IT, BVDUCOE, Pune, India[1]

Assistant Professor, Dept. of IT, BVDUCOE, Pune, India[2]

ABSTRACT: As emergence of digitization vast amount of data generated from various aspects like industries, academics, entertainment etc. this data is available in different formats like text to image and audio-video. Therefore, to manage such amount of data is a challenge for researchers and until now cloud infrastructure a great proven option for such data storage. Cloud is a large pool of resources and these resources dynamically match load. Due to dynamic expansion used a cloud, it's difficult to identify of what kind of resources are utilize and in which place (i.e. continent/country). These characteristics make it crucial and somewhere not attainable in any cost to deal with appropriate security, privacy and trust mechanisms in the cloud. We propose a new architecture that incorporate cloud storage service with data confidentiality and possess a feature of executing simultaneous operations on encrypted data and along with the geographically distributed clients are to connect directly to these cloud database which is encrypted and they also provided to execute their operations over the cloud database. This system intended for hospital system to maintain security of user's data. These papers give details about this project work with following sections.

KEYWORDS: Encryption, Access control policies, Query translation, Data isolation, Database.

I. INTRODUCTION

Cloud computing is now a popular because of its extensive abilities and having best computing for use, where cloud users can store and process their information into the cloud from anywhere. Cloud users take advantage from on asks for a high-grade efficient services and applications from a stack of ongoing available resources of computing [1]. Key features publicized are multi-tenancy, pay-per-use, elasticity and maximal resource utilization.

These extensive features add meaning to standing big environment such as information centers by the job management/virtualization and service management.

In addition, these available resources not placed in one country or not on same continent. Due to dynamic spreading of a cloud, it is not easy to locate which resources used in which country. Therefore, it results in problem of data handling and security. To manage such remote resources is not possible in internet-connected world because there is possibility of attacks on travelling data-to-data centers. A main problem in data communication the saving and utilization of data is that contents of the data may be sensitive, like credit card numbers, business plans, or other personal information. Saving and utilization of sensitive data on cloud infrastructure provided by a third party raises issues of data leakage. Therefore, this is unauthorized disclosure of information. There is one option to this issue, encrypt data over the user system before uploading data to the server then evaluate queries by again evaluating encrypted information server to the client, decrypt information, and evaluate the query on users system. These issues are the addressed regarding information storage by using cryptographic solutions when does not need to perform computations over encrypted information. Our goal is to give data isolation, data confidentiality for cloud databases that represent open database. Behind these two problems, there are three issues: operation of SQL operators over encrypted information; a selective encryption strategy enforces access control mechanisms; available methods do not prescribe the scalability and performance for typical cloud services [2].

So here in this project work, we propose architecture to encrypt database which is been accessed by number of users (MuteDB) that assures data privacy by evaluating operations over encrypted data and by applying access control policies by encryption. By grouping these two mechanisms, MuteDB assures privacy of data saved on cloud even in most vulnerable situations.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Reminder of this paper articulates how we can achieve this goal. Section II gives details of previous research regarding encryption for data in context of cloud infrastructure. Section III shows design of proposed architecture. Section IV shows overview of results. Section V concludes our discussion with summarization of future enhancements.

II. RELATED WORK

A security issue about cloud database stack is clearly is crucial issue that research trying to solve. In cloud data is been saved on third party. A sensitive data is been tackled by cloud service vendor. Recently Cloud Security Alliance reported problems of data leakage as security issue in the cloud infrastructure. Security breakage of data can disturb you personal life also. So data placed on cloud should protect for assurance of its owner's privacy. To address such issues researches has been going on in 2002 [3] proxy server less architecture with distributed metadata had been proposed. This architecture don not have any median proxy so single point failure problem get solved [3]. Metadata is been circulated in clients due to that client have state link to database. in this method clients have own encryption mechanism to encrypt data and can manage metadata locally. This architecture is not same as PSB because it provides proxy for each client. This architecture is not able to solve consistency problem still because number of clients are in access.

In 2005, concept of DBMS engines encryption of information has been proposed [4]. This scheme is been based on idea of transparent encryption of available information. This scheme has ability to build a faithful DBMS on unfaithful cloud data storage. However, this DBMS engine is not trusted because cloud providers control it so TDE technique is not appropriate for the cloud infrastructure. This approach gives data confidentiality for frameworks where storage system being compromised. However, it requires a modified DBMS engine that is not suitable with open source and business specific DBMS software acquired by cloud vendors. The author contribution in [4] using encryption for managing access to encrypted information saved in a cloud. These results are not suitable to usage contexts where scenario of the database updated, and not supports concurrent accesses from number of clients mostly spread on a geographical distance.

In 2007, Vipul Goyal et al. developed a new system for fine-grained transaction of encrypted data based on cryptography. This system serve as Attribute Based key policy Encryption scheme [5] that is KPABE. In this system, cipher texts tagged by private keys and attributes set to control which cipher texts decrypted by user. Research works describes the need of this mechanism to distinguish audit-log information and transmit encryption. This method explains mandate of private keys that classify Encryption hierarchically on identity that is HIBE.

Furthermore, [6] Siani Pearson and Azzedine Benameur presented paper on clod security, Author described how issues related to privacy and security comes regarding cloud computing and discussed options, that help to address these issues. Author here mainly mentioned that instead of combination of known techniques, there is need of unique mechanisms to address privacy and security solutions. Author contributed deep knowledge regarding privacy issues in context of cloud, traditional security models, Trust issues, legal aspects.

Similar to this concept Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou presented research work [7] for fine-grained data access control. This approach focus on issue to keep important user data confidential from insiders, unfaithful servers, available techniques commonly provide cryptographic techniques through publishing keys for decryption only to authenticated users. Paper also addresses the problem of continuously gaining scalability, access control confidentiality and fine-grains. Author completed this goal by stringently grouping techniques of encryption scheme based on attributes that is ABE, proxy re-encryption. As a result, this proposed scheme secured under standard cryptographic models. Then in next research [8], authors solved the problem of ranked search for multi keyword on encrypted data for cloud, and established different privacy requirements. In a group of various multi-keyword semantics, author selected the effective similarity measures of matching coordinates, i.e. for any possible matching, to efficiently obtain nearer outsourced text to the keywords of query, and use similarity of inner products to quantitatively execute such measure for similarity. To fulfill the issue of providing multiple keywords semantic without privacy disturbing, author proposed MRSE based on authenticated inner product execution. It results in two mainly extended MRSE schemes that achieves different privacy needs in two different threat models. Here thorough survey privacy and efficacy assurance of proposed schemes is been explained and crosschecked through real time dataset. This shows proposed mechanism gives low performance overhead for counting and communication. In future, this method can adopt more ranking scheme for multiple keywords.

Furthermore in 2013, research focused on to process Analytical Queries over Encrypted Data [9]. Here author focused on MONOMI [9], a system for efficiently executing logical queries on private data using an unfaithful server.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

By executing most query executions on encrypted data, MONOMI protects data confidentiality. This technique based on client-server query execution to perform queries that could not effectively operate alone on encrypted data. This method applies space proficient encryption, combined homomorphic summing and per-row pre calculation refining to increase performance of queries for encrypted information. This technique enhances performance on greedy algorithms through effective query execution plans.

At the end of 2014 Michael Beiter a et al. focused on encryption techniques based on point to point policy for multiple users data management. In this paper, a unique user-centric data control technique has been proposed and described. This mechanism involves policies specific to machine which shows permitted access that are connected to information or link to information and passes with it as it travel in between different users.

Author describes various different mechanisms that can support multiple control and verification. Author considered how key management could simplify by means of applying secret sharing instead of a public key infrastructure as the cryptographic spunk of the scheme. In contrast to PKIs, secret sharing techniques are a defined multi-party cryptographic tool that shows the original issue more efficiently more ever with an inherently significantly higher level of security.

Therefore, by using reference of some previous work we are going to design our system, which will clear in next section.

III. PROPOSED WORK

We proposed the first architecture, called Multi-User relational Encrypted Data Base (MuteDB) that guarantees data confidentiality by evaluating operations on encrypted data and by applying access control policies through selective encryption methods. MuteDB is combination of these two methods the only solution ensuring confidentiality of data stored in the cloud. Our system is limited to hospitals now where data of patient and doctor's is been maintained in cloud infrastructure. In addition, our intended work focus on setting access privileges to users (doctors/ patience) and data will display in encrypted form. Our solution works even in dynamic scenarios, in which users and access control policies change over time, without the need to renew and redistribute user credentials. The proposed architecture has specifically designed for cloud database scenarios where multiple users can access the cloud database through the Internet possibly from different geographical areas. Below is the flow of system that depicts how design will go on.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

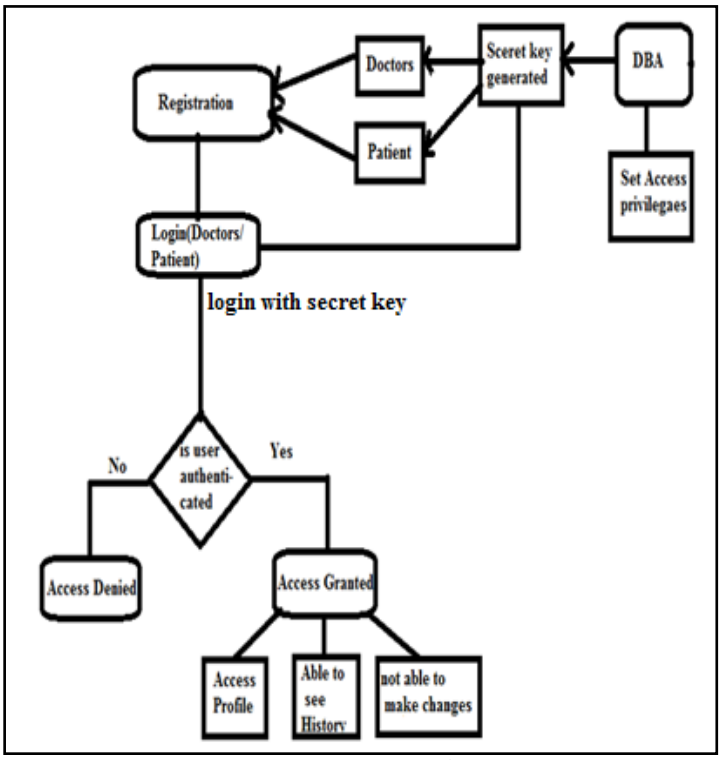

Fig 1: System Workflow

Next section shows results analysis regarding this flow.

IV. RESULT ANALYSIS

In this section, we are going to articulate result analysis of this project work. Our aim is here to encrypt user data to maintain its confidentiality. Therefore, to achieve the goal we designed a system for hospital where doctors and patients data is been placed on cloud, and to maintain security of this data we are providing encryption mechanism. Here user (doctor/patient) needs to register first. Database administrator set all access privileges to them according to that after registration one secret key generated for respective user. User can log in to system by using that secret key only, once user log in he can see his data but not able to change in it. User able to see only those data, which granted by DBA if user want to see more, he can request to admin. User can see his data in encrypted form. Only specific user can see his data no else cannot interfere in due to that privacy maintained. Below figures are showing actual view of a system.

Fig. 2. Registration Window

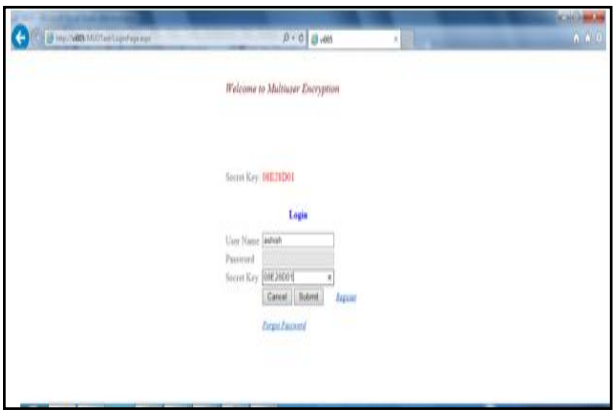

Fig. 3. Login With secret key

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Fig. 4. Records updating

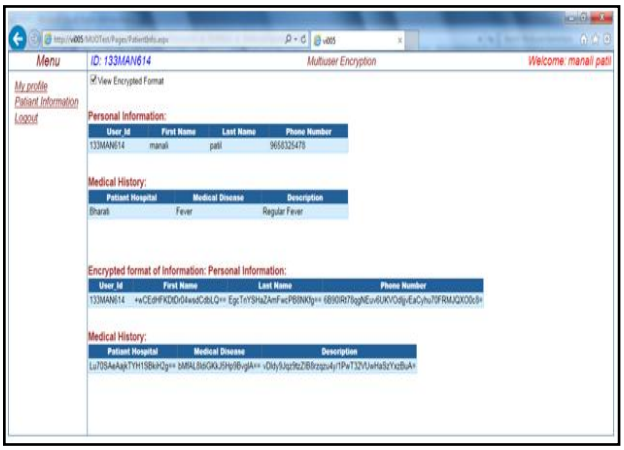

Fig. 5. Patient records

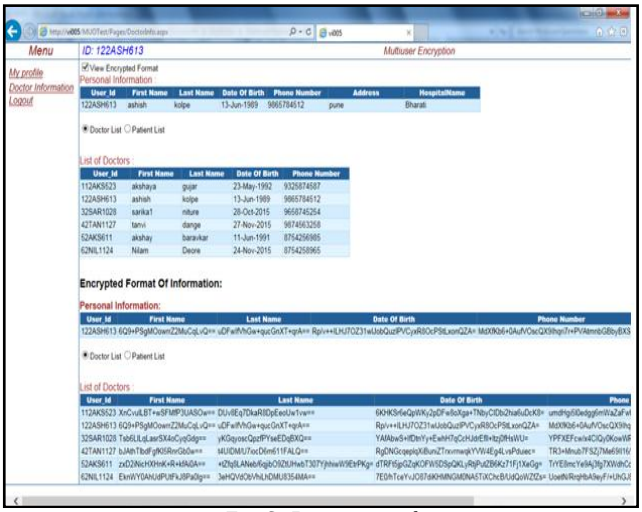

Fig. 6. Doctors record

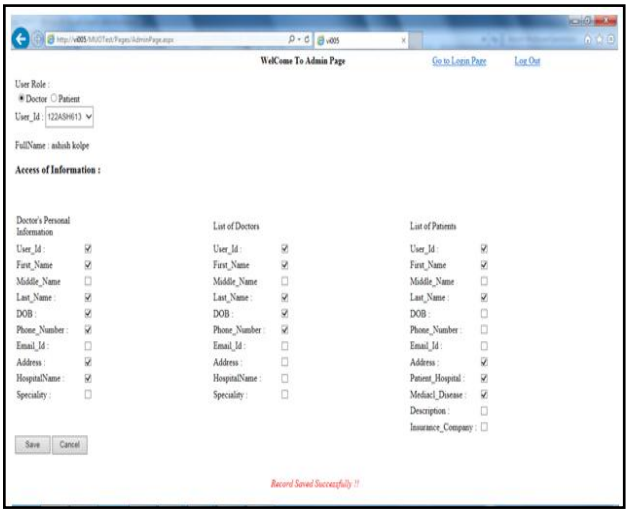

Fig. 7. Admin page

This page shows marked checkboxes are access to users.

V. CONCLUSION AND FUTURE WORK

In this project work, we introduce security issues in cloud regarding outsourcing. Reviewed some previous techniques which focus on maintain data confidentiality and tried to find solution by combination of previous techniques. This project work maintains user's data security effectively. We articulated our system with its flow and results. Currently system is been designed for secure database by using encryption mechanism for text database. This implementation now do not support any uploading and downloading also don not have any features of image, video and audio. In future, we can adopt these features in to system. In addition, this is platform dependent system so in future we can overcome this limitation.

REFERENCES

[1].N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data," Proc.IEEE INFOCOM, pp. 829-837, Apr, 2011.

[2] L. M. Vaquero, L. Rodero-Merino, and R. Buyya, "Dynamically scaling applications in the cloud," *ACM SIGCOMM Computer Communication Review*, vol. 41, no. 1, pp. 45–52, 2011.

[3].H. Hacigu¨mu¨ s¸, B. Iyer, C. Li, and S. Mehrotra, "Executing SQL over Encrypted Data in the Database-Service-Provider Model," Proc. ACM SIGMOD Int'l Conf. Management Data, June 2002.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

[4] Damiani, E., De Capitani di Vimercati, S., Foresti, S., Jajodia, S., Paraboschi, S., Samarati, P.: Metadata Management in Outsourced Encrypted Databases. In: Jonker, W., Petkovi´c, M. (eds.) SDM 2005. LNCS, vol. 3674, pp. 16–32. Springer, Heidelberg (2005)
[5] Vipul Goyal, Omkant Pandey, Amit Sahai, Brent Waters., "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data." This research was supported in part by NSF, the US army research office Grant No. W911NF-06-1-0316, 2007
[6] Siani Pearson and Azzedine Benameur, "Privacy, Security And Trust Issues Arising From Cloud Computing." IEEE, 2010, pp. 693-701.
[7] Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou, "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing." Was supported in by US national science foundation, 2010.
[8] Ning Cao, Cong Wang, Ming Li, Kui Ren, and Wenjing Lou., "Privacy-Preserving Multi-keyword Ranked Search over Encrypted Cloud Data." Was supported in by US national science foundation ,2011.
[9] Stephen Tu, M. Frans Kaashoek, Samuel Madden, Nickolai Zeldovich, "Processing Analytical Queries over Encrypted Data." VLDB Endowment, Vol 6, No. 5, 2013, pp. 1-11.
[10] Michael Beiter a, Marco Casassa Mont b, Liqun Chenb, Siani Pearson, "End-to-end policy based encryption techniques for multi-party data management." Computer standards and interfaces 36(2014) , pp. 689-703.