Advances in Computer Science and Information Technology (ACSIT)
p-ISSN: 2393-9907; e-ISSN: 2393-9915; Volume 4, Issue 1; January-March, 2017, pp. 47-49
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/Publication.html

Performance Evaluation on Data Management Approach for Single Cloud using MES (Modern Encryption Standard)

V. Vijeya Kaveri[1], Pavithra Elango[2] and Maria Navis Godslin[3]

[1,2,3]Dept of Information Technology, Sathyabama University, Chennai
E-mail: [1]vijerama.kaveri@gmail.com, [2]pavichitra95@gmail.com, [3]mariaagods@gmail.com

Abstract—*In this paper, a Modern Encryption standard is introduced to evaluate the performance of data management in single cloud server. Availability of cloud users increased in computerised world due to its advantages and services. Because of variation in cost public cloud server become more popular towards consumers. Due to the rapid increase of cloud consumers faces lots of issues in privacy factor. It leads to lack of confidentiality on personalised data. To overcome the privacy issues encryption technique is introduced. We proposed multiple encryptions with single cloud server. The sharing of data is allowed only for verified user in the cloud server. The user can access the data by using the cryptography key received from the cloud server. For each and every access of application in cloud, user gets different encryption keys from the server. Once the secret key is used for one application, the user cannot be use the same key to access the other application.*

Keywords*: Modern encryption standard (MES), cloud server, cryptography key, cloud consumers, data management*

1. INTRODUCTION

Cloud computing plays major role today’s IT world. Cloud computing provides lots of benefits including fast data access, cost, flexible data management and so on. Data owners shared their sensible personal information on cloud like their personal email, Health details, accessing details, personalized licence number. Due to lack of privacy there is the chance of loss of confidentiality over vast data owner. To secure those data various encryptions are introduced. Here the encryption keys act as the firewall for user’s sensible records. To protect their privacy, the encrypt key is used to encrypt their own data with efficient secret cryptography keys. Single cloud server has multiple numbers of encrypted applications with multiple users. The consumer uses their own data after the decryption. Due to the rapid expansion of data, the data owners tend to store their data into the cloud to release the burden of data storage and maintenance [1]. However, as the cloud customers and the cloud server are not in the same trusted domain, our outsourced data may be under the exposure to the risk. Thus, before sent to the cloud, the sensitive data needs to be encrypted to protect for data privacy and combat unsolicited accesses. Unfortunately, the traditional plaintext search methods cannot be directly applied to the encrypted cloud data any more. The traditional information retrieval (IR) has already provided multi-keyword ranked search for the data user. In the same way, the cloud server needs provide the data user with the similar function, while protecting data and search privacy. It is meaningful storing it into the cloud server only when data can be easily searched and utilized.

Due to the usage of sensitive data in the cloud network increase the more number of owners. In order to secure the data, keyword based data privacy to enable the data protection. Personal and sensible data's are mostly encrypted in cloud server before sending. While searching the secured data with search technologies makes the search unusable. To meet the efficient privacy requirements lots of encryption techniques. Some may have data which is very sensitive that should not be accessible by any person other than the owner thereby, comes the most commonly used term by people called security. Modern organizations are moving towards the methodology and privacy is improved by the way of using multiple secret key services. Data is defined as collection of information. Here, information can be considered as structured information or unstructured information. Sensitive information can be present both in structured as well as in unstructured data. Security is a major concern in enterprise applications. Information stored in retail and finance domains are very sensitive[]. Protecting the private data, filtering attacks from unknown sources thereby ensuring security is the hot research area. There are services known as DP (Data Providing) services. These services are used to access the enterprise or any organization' data quickly through web services []. To get response for complex queries, composition of services is a must.

2. RELATED STUDY

In paper[1],the author has described the fact that backward secrecy is not needed for this scheme makes the Add algorithm more effcient, since it does not require the owner to send a message to the server. Our multi-user construction is very effcient on the server side during a query: when given a trapdoor, the server only needs to evaluate a pseudo-random permutation in order to determine if the user is revoked.A more expensive authentication protocol would be required for each search query in order to establish the identity of the querier.

The problems occurs in symmetric searchable encryption can be achieved any type of query but Strong privacy guarantee, however, comes at the cost of a logarithmic number of rounds of interaction for each read and write.Using techniques for memory checking one can make those solutions robust against malicious servers at the price of additional overhead.Less efficient compared to private-key solutions.The data in PIR(private information retrieval) is always unencrypted, any scheme that tries to hide the access pattern must touch all data items. Otherwise, the server learns information.

In paper[2],the author says that any user in the group can store and share data files with others by the cloud. The encryption complexity and size of cipher texts are independent with the number of revoked users in the system. User revocation can be achieved without updating the private keys of the remaining users.

In less Confidential, any member should be able to download the data without key.Identity privacy is one of the most significant obstacles for the wide deployment of cloud computing.Without the guarantee of identity privacy, users may be unwilling to join in cloud computing systems because their real identities could be easily disclosed to cloud providers and attackers.

In paper[3],the author says that,The techniques defines in this provide provable secrecy for encryption, in the sense that the untrusted server cannot learn anything about the plaintext given only the cipher text.It also supports hidden queries.Better space efficiency is available with a block-oriented scheme.

The problems occurs in Padding scheme would introduce space inefficiency. Also, for security reasons we cannot decrease the word length below a certain limit.

In paper[4],More efficient in terms of computation for the Search algorithm.The client to invoke the Metadata Storage with a minimum bandwidth and high efficiency.Both search and update are performed with high effciency at a minimum cost.

The problem is that,Information leakage occurs in stored documents.Possibility for revealing little information to the server.

In paper[5],the author states the data encryption scheme that does not require a trusted data server. In the scheme the server can perform encrypted searches and updates on encrypted data without knowing the plaintext or the decryption keys.

The defect with this is,changing keys may result in decrypting all the data with the old key and re-encrypting it using the new keys. For large data sets, this is not practical.Fully collusion-resistant proxy encryption schemes is still an open problem.PIR schemes are computationally ex- pensive

In paper[***6],*** *The author described that,*the computational cost of such verification is a large number of bilinear pairings and exponentiations, which grows linearly with the number of attributes in the predicate. As a result, the computation overhead at signer side will not be reduced at all even after outsourcing.

Dishonest behaves could be prevented to a great extent if S-CSP will be punished if detected.Eliminating the most computational overhead at signer

3. EXISTING SYSTEM

Analysis begins when a user or manager begins a study of the program using existing system.

During analysis, data collected on the various files, decision points and transactions handled by the present system. The commonly used tools in the system are Data Flow Diagram, interviews, etc. training, experience and common sense are required for collection of relevant information needed to develop the system. The success of the system depends largely on how clearly the problem is defined, thoroughly investigated and properly carried out through the choice of solution. A good analysis model should provide not only the mechanisms of problem understanding but also the framework of the solution. Then the proposed system should be analyzed thoroughly in accordance with the needs.The drawback of the existing system is that it is very difficult to retrieve data from case files. It is difficult to handle the whole system manually and it is less accurate and to keep the data in case files for future reference because it may get destroyed. Moreover it is very difficult to retrieve data. Redundancy of data may occur and this may lead to the inconsistency. The manual system is so time-consuming.

4. IV.PROPOSED SYSTEM

Sharing the secret key approaches the data management for single clouds to maintain the confidentiality. We are using multiple encryptions with single cloud service. The data are shared with selected user after the encryption.

The success of the system depends largely on how clearly the problem is defined, thoroughly investigated and properly carried out through the choice of solution. A good analysis model should provide not only the mechanisms of problem understanding but also the framework of the solution. These literacy skills are traditional literacy, information literacy, media literacy, health literacy, scientific literacy and computer literacy. Among these, media and computer literacy’s are peculiar to the Internet context. From Norman and Skinner

(2011), illustrates the relationship between these literacy skills in a lily model.

From the related works our proposed system overcomes lots of drawbacks. Then the proposed system should be analyzed thoroughly in accordance with the needs.

Data Storage: Considering the security issue of the data storage, such as the storage format and privacy information data protection. A proper database with higher security level should be choosing.

Data Presentation: In order to provide a concise and beautiful view of the data. The data presentation can combine with different presentation formats such as histogram and table, etc according the medical data requirement.

Planned approach towards working: - The working in the organization will be well planned and organized. The data will be stored properly in data stores, which will help in retrieval of information as well as its storage.

5. SYSTEM ARCHITECHURE

Secret sharing data management approaches for multiple clouds to maintain confidentiality that involves a secret sharing scheme. Data sharing with a large number of participants must take into account several issues, including efficiency, data integrity and privacy of data owner. We are using encryption with cloud service. Data owner only needs to distribute a key to a user for sharing a number of documents. Share data for selected user only, Auditor verified the user after sharing data. User download data and received the cryptography key for mail. If the user has cryptography matching with access policy, it can decrypt and get original message. It is provide the high security by using encryption and decryption keys for sensitive information.

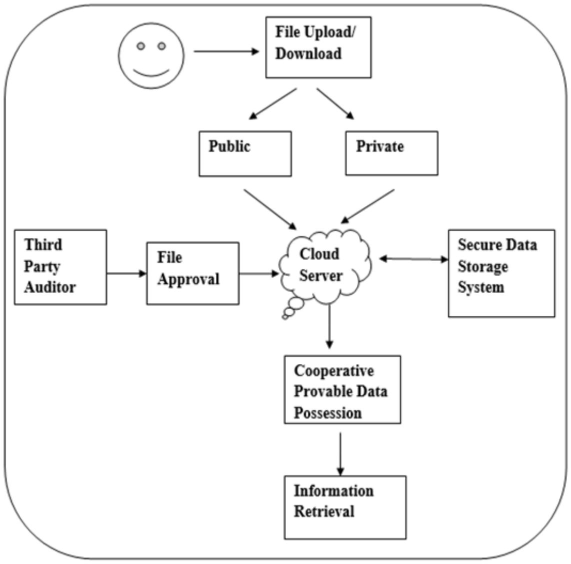

Fig. 1.1: System architecture

6. ALGORITHM

MES ENCRYPTION ALGORITHM

This function takes the input as the plain text from the server and coverts into chipper text by adding secret key.

Step1 : start Main

Step2: Input file (plain text)

Step3: read the file

Step 4: generate cipher key

Step 5: cipher text= length of file (key +plain text)

Step6: read the encrypted file

Step7: open encrypted file

Step 8: end

7. CONCLUSION

The MES encryption is used to encrypt and decrypt the data stored in the single cloud server. The method is used to test the any type of confidential file. The result shows free from common attacks.

REFERENCES

[1] XidianXiaofeng Chen,Secure Outsourced Attribute-Based Signatures. State KeyLaboratory of Integrated Service Networks, University, Xi’an, China,Jan 2014

[2] Zhongma Zhu,Mona:Secure Multi-Owner Data Sharing for dynamic Groups in cloud,Sch. of Inf. Sci. & Eng., Southeast Univ., Nanjing, ChinaDec 2014

[3] TranThaoPhuong,Shared and Searchable Encrypted Data For Untrusted Servers,Japan Advanced Institute of Science and Technology, 1-1 Asahidai, Nomi, Ishikawa, Japan,Mar 2013

[4] Cong Wang, Searchable Symmetric encryption:Improved Definitions and efficient Construction,Dept. of ECE, Illinois Inst. of Technol., Chicago, IL, USA,Aug 2010

[5] Saeed Sedghi Adaptively Secure Computationally Eccient seachable symmetric encryption, University of Twente 2 Eindhoven University of Technology, 2010.

[6] DawnXiaodingSongPractical Techniques for searches on Encrypted Data,California Univ., Berkeley, CA, USA,Aug 2002.