Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 2, February 2014, pg.361 – 365

RESEARCH ARTICLE

Secure Token Based Storage System to Preserve the Sensitive Data Using Proxy Re-Encryption Technique

A.Jeeva[1], Dr.C.Selvan[2], A.Anitha[3]

[1]M.E Student, Department of CSE & Anna University,
Sri Eshwar College of Engineering, India
[2]Associate Professor, Department of CSE & Anna University,
Sri Eshwar College of Engineering, India
[3]M.E Student, Department of CSE & Anna University,
Sri Eshwar College of Engineering, India
[1] jeevamecse@gmail.com; [2] selvan.coimbatore@gmail.com; [3] aspireanitha@gmail.com

Abstract— In the cloud computing environment, storing sensitive data is more difficult task. The privacy preserve cost is high when we encrypt entire sensitive data. Also encrypt data are not performing well in cloud application. This is becomes the challenging to preserve the sensitive data in cloud. So we analyse the data which is need to be encrypted and other is not. And also split the data in different parts and stored it in different cloud environment. Each part of data sets are contains the tokens. The storage server identifies the data using token keys. The proxy encryption technique is used to encrypt the proxy. When the client encrypts the data before outsourcing to the cloud server, the link between the client server and cloud server proxy is encrypted using proxy encryption technique. This enables the privacy to preserve the data attacks from the attackers.

Keywords— Cloud Computing, Sensitive Data, Privacy Preserving, Proxy Encryption, Token based system.

I. INTRODUCTION

The internet is involved in many new technologies. One of the most popular technology is cloud computing. Cloud computing environment provides the massive storages facility to the client. There are various types of data are stored in cloud computing environment. Some data are sensitive and some other data are not sensitive. Storing sensitive data in cloud storage system in more difficult problem. Client is encrypting the data before outsourcing it. [1] Encrypting entire data is consuming more cost and time. To recover this problem we analyses the entire data which is need to be encrypted and other in not. Because the sensitive data like medical records and other records are more sensitive one. Example we take the medical records. The medical records contains name, age, gender, disease type, hospital address and medical data are needed. In this data we need to analyse the data and encrypted the attributes like name and address. Because the name of the patient and address of the hospital

is sensitive data. This paper focuses on design a token based storage system for preserving the privacy of the data. In the cloud environment the large level of cloud distributed system are available. It is very effective because the message can recover from the cloud storage system. Storing sensitive data in third party cloud storage is making a serious sensitive issue to preserve the data. Usually, the volume of intermediate datasets is huge .Hence, we argue that encrypting all intermediate datasets will lead to high overhead and low efficiency when they are frequently accessed or processed.

The customer manages the underlying operating system, developed application, storage and some selected network component, but they don't control the cloud infrastructure. Cloud providers bill the IaaS customers based on number of resources allocated and consumed by them. Security consideration for IaaS includes the management of virtual resource allocation and addressing the virtualization vulnerabilities and risks that affect the IaaS delivery model. In the private cloud system model, the cloud infrastructure operated for the specific company needs. Client can have a high value of control of the physical and logical security issues of the private cloud infrastructure both the hypervisor and the hosted virtualized operating systems. We use a new threshold proxy re-encryption scheme and integrate it with a secure decentralized code to form a secure distributed storage system.

II. RELATED WORK

We analyse the privacy preserve and consider the cost issues of privacy preserving to pay-as-you-go scheme in cloud environment. We identify the data need to be encrypted. The token key and shared token will all client of the service. This problem in consider as unauthorised access to the encryption key. The centralized architecture for secure storage system provides good efficiency. Encryption involves well for data privacy in this technique.

The privacy data is necessary to encrypt and decrypt sensitive data in many cloud applications. Encryption is usually combined with other application to reduce the cost problems. A storage server's failure in modelled as ensured mistakes of stored tokens in the system. A proxy server can transmit the client data to cloud provider. [2] The entire proxy is encrypted in the system. The stored token is combines the blocks with the access in each storage system that solves in the storage server system. The client may share different type of data in the cloud server system. To retrieve the data from the service provider the data is decrypted in the cloud system. The token code in random process to generates the matrix code.

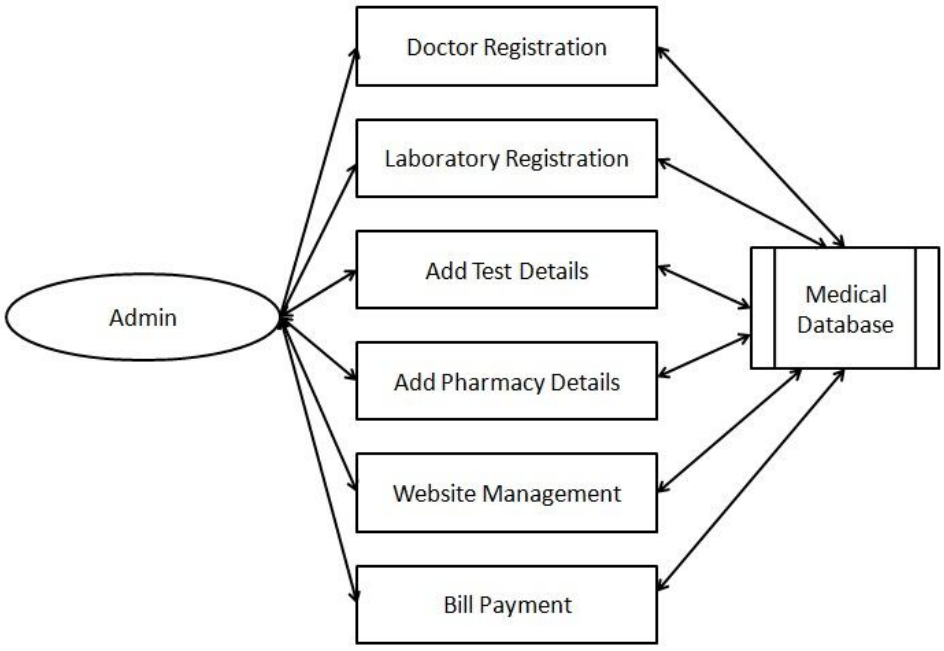

Fig 1.Admin Control flow

A decryption is successful if and only if the token in having the same code. Our goal is to automatically retrieve the token key from the cloud service provider in the cloud computing environment. This is increases the token management process. [1]The attacker in the cloud that ensures a token can only give the access to the correct user in system. The data privacy is caused by retrieve the sensitive data to store longer in the storage server. Storage and computation services in cloud are equivalent from all cost related issues in the cloud computing environment.

In the fig 1,the data owner can encrypted the sensitive data before it outsourced.The encrypted data stored in the cloud storage. The authorized used only can access the data in the cloud storage. The requested access of the data can retrived from the cloud server.The reponse of the request has transmits from the required flied in the cloud. The secure access channel must transmit the data signals in the environment.Authorized user can get the right to access the sensitive data in cloud.The data is also encrypted in the user side

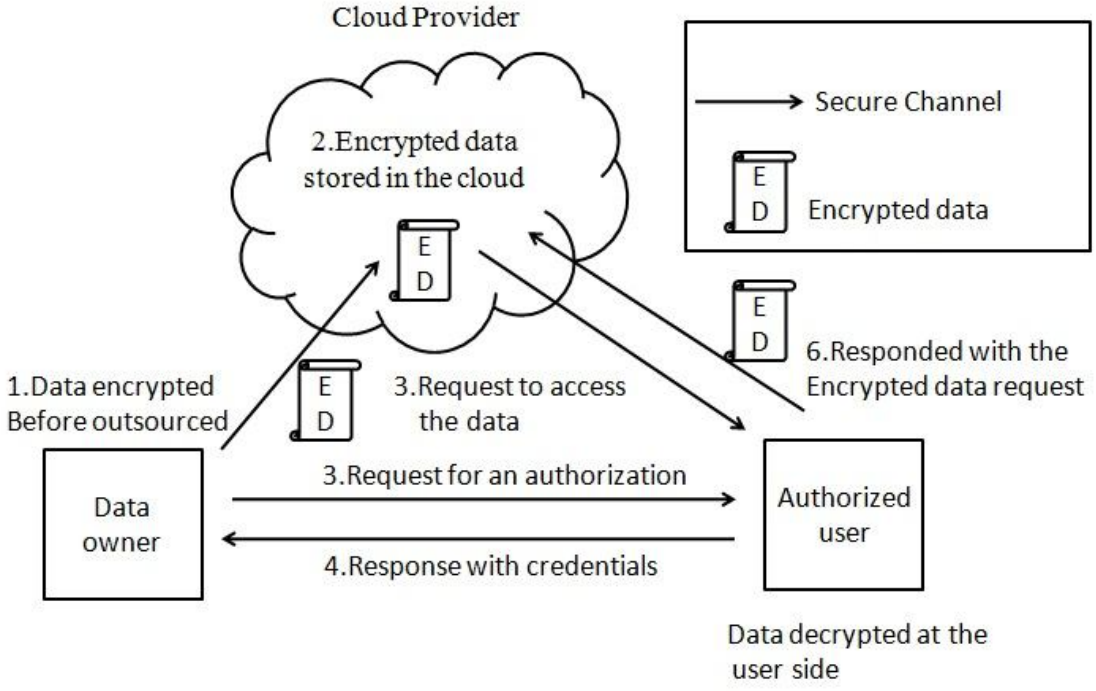

Fig 2. Privacy preserving in cloud

III. PROBLEM ANALYSIS

A. SECURE DATA MANAGEMENT

Cloud system is managed sensitive data in the cloud computing environment. The privacy sensitive data in the cloud storage model in the secure system in enabled an authorized user or server cannot get the data of the storage. The privacy preserving issues and made in the efficient way to configure the cloud system in the cloud environment. [3][4]The data spited in the several part and analyse the part of the messages need to be encrypted. First consider the system to configure the privacy scheme in the cloud environment. This method is used to evaluate the technical aspects of the proposed system. This can be demonstrated if reliable hardware and software capable of meeting the needs of proposed system. It can be acquired or developed in the required time.

B. COST MINIMIZATION PROBLEM

This is the willingness and ability of the management, employees, end-user to operate and support for a proposed system. This method is used for finding how much effort goes for education and training the staff for the system, which is to be developed. Sensitive data cost of intermediate data that involved in encryption and decryption operation in the cloud environment. Cloud providers have configure the different cost models of storing data in the cloud computing. So the client is enabling to provide the correct cloud server to provide the relevant operation on the cloud provider.

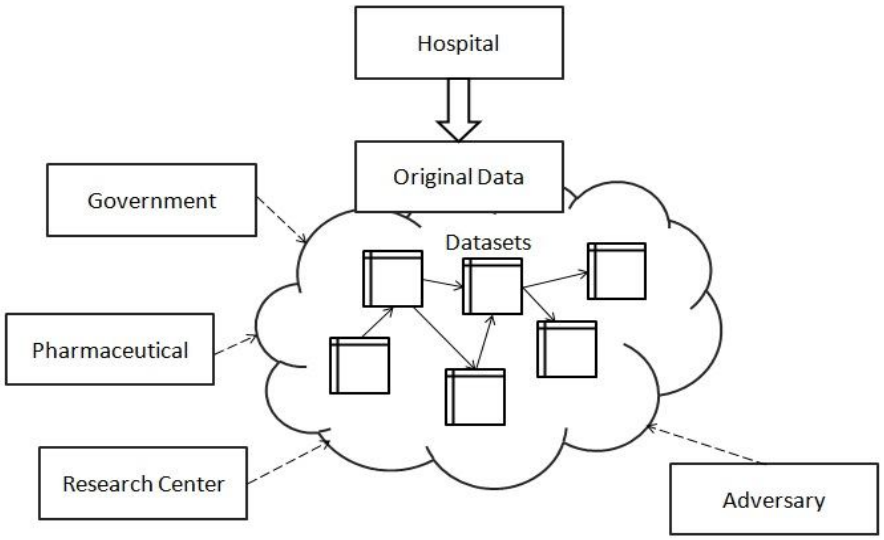

Fig 2. Privacy threads due to intermediate datasets

IV. CONSTRUCTION OF SECURE CLOUD SYSTEMS

The proxy re-encryption technique is used in different way to encrypt and decrypt the messages.Converstion of a proxy encryption technique is shared the secret token in the each server. The server is shared the token key in the system that enables the proxy encryption scheme in the environment. [5] We the data is retrieve from the cloud computing environment the tokens and matched with the token that client have. If the tokens are same means the cloud server retransmit the data to the client. Tho the stored data with the secure activity that ensure the data is retransmitted to the cloud client side. [6][7] This will happens in the cloud server environment. To retrieve the messages in the cloud server environment the messages and user will ensure the data in the cloud computing environment. The correct retrieval of the data and tokens that compare the secret tokens in the system. The storage cost also reduced in the technique. Because the high sensitive data will stored in the high reliable cloud environment and low sensitive data will stored in the low reliable cloud environment. The different between the cloud system and token management system will ensures data secure system in the cloud computing.

V. CONCLUSION

The cloud servers and the tokens are stored in the cloud storage system. The data is analysed before outsourcing to cloud providers. Analysed which data is need no encrypt and which is not encrypt. The proxy encryption technique is support the encoding and decoding of the sensitive data. The cloud system is completely decentralized with storage servers in the cloud computing environment. The real world sensitive data is stored in the various cloud server environment that need to reduce the cost problem for the cloud storage. The various types if data and sensitive information will provides the secrete key and signature of the entire system. The system will optimize the level of configuration in the cloud server environment.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica and M. Zaharia, "A View of Cloud Computing," Commun. ACM, vol. 53, no. 4, pp. 50-58, 2010.

[2] R.Buyya, C.S.Yeo, S.Venugopal, J.Broberg and I.Brandic, "Cloud Computing and Emerging It Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility," Fut. Gener. Comput. Syst., vol. 25, no. 6, pp. 599-616, 2009.

[3] L.Wang, J. Zhan, W. Shi and Y. Liang, "In Cloud, Can Scientific Communities Benefit from the Economies of Scale?," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 2, pp. 296-303, 2012.

[4] H. Takabi, J.B.D. Joshi and G. Ahn, "Security and Privacy Callenges in Cloud Computing Environments," IEEE Security & Privacy, vol. 8, no. 6, pp. 24-31, 2010.

[5] D. Zissis and D. Lekkas, "Addressing Cloud Computing Security Issues," Fut. Gener. Comput. Syst., vol. 28, no. 3, pp. 583-592, 2011.

[6] D. Yuan, Y. Yang, X. Liu and J. Chen, "On-Demand Minimum Cost Benchmarking for Intermediate Dataset Storage in Scientific Cloud Workflow Systems," J. Parallel Distrib. Comput., vol. 71, no. 2, pp. 316-332, 2011.

[7] S.Y. Ko, I. Hoque, B. Cho and I. Gupta, "Making Cloud Intermediate Data Fault-Tolerant," Proc. 1st ACM Symp. Cloud Computing (SoCC'10), pp. 181-192, 2010.

BIOGRAPHY

A.Jeeva born in Sivaganga, Tamilnadu, India in 1990. He received B.Tech degree in Computer science and Engineering, Kalasalingam University, Tamilnadu, India. He is currently pursuing M.E Degree in Computer science and Engineering in Anna University, Chennai, Tamilnadu, India. His research interests in Cloud Computing. He is a active member of an IEEE Association.

Dr.C.Selvan has been working as an Associate Professor in the department of CSE, in Sri Eshwar college of Engineering, Coimbatore since 2012. He is an IEEE member. He had been doing research in Government College of Technology, Coimbatore, Tamilnadu, India. He has published 5 papers in International Journals. His area of interest is Mobile Computing, Mobile communication and Data Mining.

A.Anitha born in Coimbatore,Tamilnadu,India in 1991. She received B. Tech degree in Sasurie College of Engineering from Anna University, Coimbatore. She is an IEEE member, she currently pursuing M.E in Sri Eshwar College. Her area of interest is Mobile Communication and Cloud computing

