Security Enhancement on Cloud Using Advanced Identity Based Encryption (Aibe)

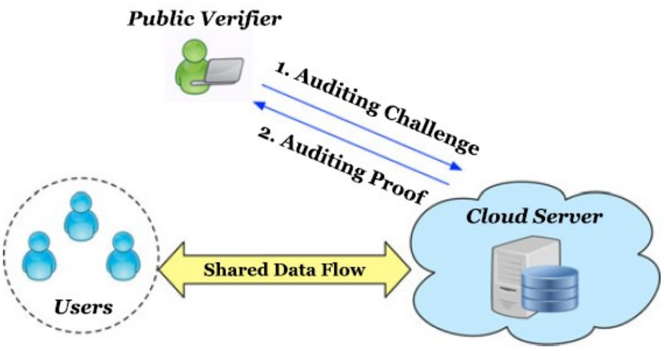
B.Swathi[1] , A.Madan Gopal[2], P.Durga Vinod[3]
[1]Assistant Professor, DEPT OF CSE, Dhanekula Institute of Engineering and Technology, A.P., India.
[2]B.Tech (CSE), Dhanekula Institute of Engineering and Technology, A.P., India.
[3]B.Tech (CSE), Dhanekula Institute of Engineering and Technology, A.P., India.

Abstract — *Cloud computing would be one of technologies which is going to play a vital role in the next generation of computer engineering field. The increased scalability and flexibility provided by the cloud computing has reduced the costs to a greater extent and therefore the technology has gained wide acceptance. The facility of Data outsourcing in the clouds enables the owner of the data to upload the data and other users can access the same. But, the data stored should be secure in the cloud servers. The data owner has lot of concern about security aspects present with the cloud computing. The data owners hesitate to adopt cloud computing services because of privacy protection issues of data and security of data. The proposed research work aims to undertake the critical issue of identity revocation wherein outsourcing computation into IBE has been introduced for the first time and a revocable IBE scheme in the server-aided setting has been proposed. This scheme offloads most of the key generation related operations to a Key Update Cloud Service Provider for key-issuing and key-update processes. Only a constant number of simple operations for PKG and users are left to perform locally. Data security is provided by using encryption, user authentication; re-encryption in the proposed data storage security model. The proposed system has also introduced outsourcing computation into IBE revocation, formalizes the security definition of outsourced revocable IBE for the first time to the best of our knowledge. Finally, experimental results have demonstrated the efficiency of the proposed construction.*

Keywords — ***Attribute Set-based Encryption, Cloud Computing.***

INTRODUCTION

Cloud computing is a model which enables the users for storing the data and programs and accessing them easily through an internet instead of using some hardware and software components in the computer. Encryption is a promising way to maintain the confidentiality of outsourced sensitive data, but it makes effective data utilization to be a very challenging task. In this paper, we focus on the problem of private matching over outsourced encrypted datasets in identity-based cryptosystem that can simplify the certificate management. To solve this problem, we propose an Identity-Based Private Matching scheme (IBPM), which realizes fine-grained authorization that enables the privileged cloud server to perform private matching operations without leaking any private data. We present the rigorous security proof under the Decisional Linear Assumption and Decisional Bilinear Diffie-Hellman Assumption. Furthermore, through the analysis of the asymptotic complexity and the experimental evaluation, we verify that the cost of our IBPM scheme is linear to the size of the dataset and it is more efficient than the existing work of Zheng. Finally, we apply our IBPM scheme to build two efficient schemes, including identity-based fuzzy private matching as well as identity-based multi-keyword fuzzy search.



The survey of major cloud service providers to investigate the security mechanisms to overcome the security issues discussed in this paper. We consider ten major cloud service providers. These providers provide their services in all major areas of cloud computing, including SaaS, PaaS and IaaS. List shows the list of service providers that we studied in this survey. In order to analyse the complete state of art of security in cloud computing, the survey needs to be more exhaustive. However, due to the fact that the scope of our work is not just to explore the state of art but to look at the major factors that affect security in cloud computing. Therefore we have intentionally not considered other cloud service providers in this survey. In list 2, we present the results of the survey that depicts the current state of security mechanisms. Information given in table 2 is based on the information available online at the official websites of these providers.

1. IaaS Service Provides is an Amazon EC2 Amazon S3 Go Grid

2. PaaS Service Provides Google Application Engine Microsoft Azure Services, Elastic Map Reduce

3. SaaS service provides Sales force Google Docs Security Issues on Cloud Computing Password Recovery 90% is using standard methods like other common services while 10% are using sophisticated techniques. Encryption 40% are using standard SSL encryption while 20% are using encryption mechanism but at an extra cost 40% are using advance methods like HTTPS access Data Location 70% have their data centers located in more than one country while 10% are located at a single location 20% are not open about this issue. Cloud computing is a model for information and services using exiting methods,

it uses the internet infrastructure to allow communication between client side and server side applications. Cloud clients service providers provides exist between that offers cloud platforms for their customers to use and create their own web services. When making decisions to adopt cloud services privacy or security has always been a major deal with these issues the cloud provider must build up sufficient controls to provide such level of security than the organization would have if the cloud were not used. The major security challenge is that the owner of the data has no control on their data processing. Due to involvement of many technologies including networks, databases, operating systems, resource scheduling, transaction management, concurrency control and memory management,various security issues arises in cloud computing. Top seven security threats to cloud computing discovered by "Cloud Security Alliance" (CSA) are : • Abuse and Nefarious Use of Cloud Computing • Insecure Application Programming Interfaces • Malicious Insiders. • Shared Technology Vulnerabilities • Data Loss/Leakage • Account, Service & Traffic Hijacking. • Unknown Risk Profile

PROPOSED SYSTEM

Existing System:-

Cloud computing, a new technology for a long dreamed vision of computing as a utility, has been gaining a great deal of momentum in the IT industry. Many organizations, enterprises and even individuals outsource their data into the cloud so as to enjoy the on-demand high quality data storage services and computing resources. Despite such benefits, data outsourcing deprives the data owners of direct control over their own outsourced data, which could reveal some private sensitive information, such as Personal Health Records (PHRs), facebook photos, financial trans-actions or business documents. To maintain the privacy of owners' sensitive data against untrusted cloud servers, data encryption before outsourcing is a promising solution. In our previous work, we adopted different encryption skills to solve some data privacy problems in PHRs systems and mobile social networks as well as much other work .However, data encryption may severely hinder several functionalities of data, for instance, private matching over outsourced encrypted datasets.

Proposed System:-

The main contributions of this paper are summarized as follows:

1) We propose a novel cryptographic primitive: identity-based private matching over outsourced encrypted datasets (IBPM),and formally define the framework and the security for IBPM. Then we present a concrete construction of the IBPM under the DLN and DBDH assumptions. Our

IBPM scheme has three distinctive features as follows:

- Our solution is in identity-based setting so that it can simplify the certificate management;
- The cloud users delegate the costly private matching operations without giving the cloud any capability in breaching the secrecy of the datasets;
- Our scheme realizes fine-grained authorization for private matching over outsourced encrypted datasets. In othew ords, only the cloud server who has the authorization token can perform private matching between two users encrypted datasets. What's more, with our scheme, the users can delegate the cloud server to check whether they have outsourced the same data to cloud before uploading the encrypted data.

LITERATURE SURVEY

J.Wei et al. [1] proposed a notation called Revocable Storage Identity-Based Encryption (RS-IBE) this provides a forward/backward security of the cipher text content by introducing the functionalities of user revocation and simultaneously the updation of the cipher text will be done. The performance of the proposed system is more advantageous in terms of efficiency and functionality and it is feasible for cost-effective and data-sharing system.

J.Y.Huang et al. [2] they have concentrated on the identity based key management system for the configurable hierarchical cloud computing environment. This proposed system consists of computation on the encryption, authentication and also provides the efficient key reconstruction in case of PKG failures. Due to this facility it reduces the key construction cost on cloud computing data centres.

S.Qui et al. [3] they have studied the problem about the private matching over the outsourced encrypted datasets in the identity based cryptosystem and this can be simplified by the certificate management. So they have proposed an Identity Based Private Matching Scheme (IBMP) which enables the cloud server to perform the private matching operations without any leakage of the private data content. They analysed the data through the asymptotic complexities and with the experimental results they found that the cost of the IBPM was linear to the size of dataset and it is also more efficient then the existing system which was proposed by Zheng [30]. So in this system they try to include two things for better matching they are the identity-based fuzzy private matching and the identity based multi-keyword fuzzy search.

CONCLUSION

In this paper, Encryption scheme describes the amount of time and computational resource required for the evaluation. Analysis shows the attribute set-based encrypted data stores on cloud and protects from the unauthorization users mainly usefully for banking services. To prevent server from learning the file content of each segment searched by monitoring the users search patterns. Future direction of our analysis is to avoid the intrusion objects without user presence.

REFERENCES

[1] Good Teachers are worth more than thousand books, we have them in Our Department.

[2] [1] Agalya, R. V., and K. Karthika Lekshmi. "A Verifiable Cloud Storage using Attribute Based Encryption and Outsourced Decryption with Recoverability."

[3] [2] Wei, Jianghong, Wenfen Liu, and Xuexian Hu. "Secure Data Sharing in Cloud Computing Using Revocable-Storage IdentityBased Encryption."

[4] [3] Huang, Jyun-Yao, I-En Liao, and Chen-Kang Chiang. "Efficient identity-based key management for configurable hierarchical cloud computing environment."Parallel and Distributed Systems (ICPADS), 2011 IEEE 17th International Conference on. IEEE, 2011.

[5] [4] Qiu, Shuo, et al. "Identity-Based Private Matching over Outsourced Encrypted Datasets."

[6] [5] Tseng, Yuh-Min, et al. "Identity-Based Encryption with Cloud Revocation Authority and Its Applications."

[7] [6] Wang, Cong, et al. "Secure ranked keyword search over encrypted cloud data." Distributed Computing Systems (ICDCS), 2010 IEEE 30th International Conference on. IEEE, 2010.

[8] [7] Wang, Cong, et al. "Privacy-assured outsourcing of image reconstruction service in cloud." Emerging Topics in Computing, IEEE Transactions on 1.1 (2013): 166-177.

[9] [8] Li, Jingwei, et al. "Outsourcing encryption of attribute-based encryption with mapreduce." Information and Communications Security. Springer Berlin Heidelberg, 2012. 191-201.

[10] [9] Green, Matthew, Susan Hohenberger, and Brent Waters. "Outsourcing the Decryption of ABE Ciphertexts." USENIX Security Symposium. Vol. 2011. No. 3. 2011.

[11] [10] Agme, Varsha S., and Archana C. Lomte. "Security Enhancement of Outsourced Data on Cloud Using Identity Based Encryption." (2014).