AUSTRALIAN JOURNAL OF BASIC AND APPLIED SCIENCES

ISSN:1991-8178 EISSN: 2309-8414
Journal home page: www.ajbasweb.com

Fully Homomorphic Encryption (Fhe) Scheme For Secure Data Sharing In Cloud Storage

[1]Abinaya. B, [2]R.G. Suresh Kumar, [3]T. Nalini, [4]Suganthi. J, [5]Saranya. V

[1]*M.Tech(CSE) RGCET Puducherry*
[2]*Research Scholar Vels University Chennai*
[3]*Assistant professor Bharath UniversityChennai*
[4]*M.Tech(CSE) RGCET Puducherry*
[5]*M.Tech(CSE) RGCET Puducherry*

Address For Correspondence:
Abinaya. B, M.Tech(CSE) RGCET Puducherry
E-mail: abinayabskr25@gmail.com

ARTICLE INFO

Article history:
Received 26 April 2016
Accepted 21 July 2016
Published 30 July 2016

Keywords:
Security Mediator, Public Auditing, Key Auditing, Bilinear aggregate signature, Extensive Security, FHE Scheme.

ABSTRACT

Cloud computing technology is widely used so that the data can be outsourced on cloud can accessed easily. Different members can share that data through different virtual machines but present on single physical machine. But the thing is user don't have physical control over the outsourced data.To securely, efficiently, and flexibly share data with others in cloud storage, the new public-key based homomorphic authenticator is proposed. By utilizing public key based homomorphic authenticator with random masking privacy preserving public auditing can be achieved. The technique of bilinear aggregate signature and FHE Scheme is used to achieve key auditing. Key auditing reduces the computation overhead. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient.

INTRODUCTION

Cloud computing is an internet based computing model which provides on-demand service, local independence, scalability, elasticity, ubiquitous network access, resource pooling and pay-as-you-go policies. Cloud storage is nowadays very popular storage system. Cloud storage is storing of data off-site to the physical storage which is maintained by third party. Cloud storage is saving of digital data in logical pool and physical storage spans multiple servers which are manage by third party. Third party is responsible for keeping data available and accessible and physical environment should be protected and running at all time. Instead of storing data to the hard drive or any other local storage, we save data to remote storage which is accessible from anywhere and anytime. It reduces efforts of carrying physical storage to everywhere. By using cloud storage we can access information from any computer through internet which omitted limitation of accessing information from same computer where it is stored.

While considering data privacy, we cannot rely on traditional technique of authentication, because unexpected privilege escalation will expose all data. Solution is to encrypt data before uploading to the server with user's own key. Data sharing is again important functionality of cloud storage, because user can share data from anywhere and anytime to anyone. For example, organization may grant permission to access part of sensitive data to their employees. But challenging task is that how to share encrypted data. Traditional way is user can download the encrypted data from storage, decrypt that data and send it to share with others, but it loses the importance of cloud storage.

To Cite This Article: Abinaya. B, R.G. Suresh Kumar, T. Nalini, Suganthi. J, Saranya. V., Fully Homomorphic Encryption (Fhe) Scheme For Secure Data Sharing In Cloud Storage. ***Aust. J. Basic & Appl. Sci.,*** *10(12): 220-223, 2016*

Types of Cloud Computing:

Public Cloud:

Public clouds are made available to the general public by a service provider who hosts the cloud infrastructure. Generally, public cloud providers like Amazon AWS, Microsoft and Google own and operate the infrastructure and offer access over the Internet. With this model, customers have no visibility or control over where the infrastructure is located. It is important to note that all customers on public clouds share the same infrastructure pool with limited configuration, security protections and availability variances.

Private Cloud:

Private cloud is cloud infrastructure dedicated to a particular organization. Private clouds allow businesses to host applications in the cloud, while addressing concerns regarding data security and control, which is often lacking in a public cloud environment. It is not shared with other organizations, whether managed internally or by a third-party, and it can be hosted internally or externally.

Hybrid Cloud:

Hybrid Clouds are a composition of two or more clouds (private, community or public) that remain unique entities but are bound together offering the advantages of multiple deployment models. In a hybrid cloud, you can leverage third party cloud providers in either a full or partial manner; increasing the flexibility of computing. Augmenting a traditional private cloud with the resources of a public cloud can be used to manage any unexpected surges in workload.

Community Cloud:

A community cloud is a is a multi-tenant cloud service model that is shared among several or organizations and that is governed, managed and secured commonly by all the participating organizations or a third party managed service provider.Community clouds are a hybrid form of private clouds built and operated specifically for a targeted group. These communities have similar cloud requirements and their ultimate goal is to work together to achieve their business objectives.

Methods Used:

Jahid *et al*. (2011) described the EASiER, an architecture that supports fine-grained access control policies and dynamic group membership by using attribute-based encryption and it is possible to remove access from a user without issuing new keys to other users or re-encrypting existing cipher texts. Chase *et al* (2007) proposed a model named as Multi authority Attribute based encryption. This scheme allows any polynomial number of independent authorities to monitor attributes and distribute secret keys. In a multi-authority ABE scheme, multiple attribute-authorities monitor different sets of attributes and issue corresponding decryption keys to users, and encryptors can require that a user obtain keys for appropriate attributes from each authority before decrypting a message. Chase gave a multi-authority ABE scheme using the concepts of a trusted Central Authority (CA) and Global IDentifiers (GID). Ruj *et al*., (2011) proposeda new model for data storage and access in clouds named as Distributed access control. This scheme avoids storing multiple encrypted copies of same data. In the framework for secure data storage, cloud stores encrypted data (without being able to decrypt them). Shuchenget.al builds a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi-trusted servers. To achieve fine-grained and scalable data access control for PHRs, Attribute Based Encryption (ABE) techniques to encrypt each patient's PHR file. Different from previous works in secure data outsourcing focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users (Chase, M. *et al*., 2009).

Wang.*et al* (2013) described the security Mediator a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi-trusted servers. To achieve fine-grained and scalable data access control for PHRs, we leverage Attribute Based Encryption (ABE) techniques to encrypt each patient's PHR file. Different from previous works in secure data outsourcing focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users (LI Shuchengyu M. *et al*., 2013). The SEM computes a blind signature with its private key, and returns this blind signature back to the data owner. Zhang *et al*., (2004) described algorithm to construct a logical key graph based on the unified relations of membership groups and resource groups. The algorithm encrypts all data streams in a resource group with a single data encryption key, called resource-group key, which results in fewer data encryption keys than the MG key management scheme.

Besides, in order to improve feasibility and save on the expense in the security paradigm, it is preferred to get the information retrieval result with the most relevant keys that match users interest instead of all the keys, which indicates that the keys should be ranked in the order of relevance by users interest and only the keys with the highest relevance are selected by the users. A series of searchable symmetric encryption schemes have been

proposed to enable search on cipher text. Traditional schemes enable users to securely retrieve the cipher text, but these schemes support only Boolean keyword search, i.e., whether a key exists in a system or not, without considering the difference of relevance with the queried keys of these encrypted data in the result. Preventing the security from involving in ranking and entrusting all the work to the user is a natural way to avoid information leakage. However, the limited computational power on the user side and the high computational overhead against information security. Here are the drawbacks spotted in the existing system.

- To improve security without sacrificing efficiency, schemes presented in show that they support top-k single key retrieval under various scenarios.
- Authors made attempts to solve the problem of top-k multi-keys over encrypted data.These schemes, however, suffer from two problems – Boolean representation and how to strike a balance between security and efficiency.
- In the former, data are ranked only by the number of retrieved keys, which impairs search accuracy. In the latter, security is implicitly compromised to tradeoff forefficiency, which is particularly undesirable in security-oriented applications.

Results:

By utilizing public key based homomorphic authenticator with random masking privacy preserving public auditing can be achieved. The technique of bilinear aggregate signature is used to achieve key auditing. Key auditing reduces the computation overhead. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient. Achieves Key auditing where multiple delegated auditing asks for different keys from different users can be performed simultaneously by the user and also supports dynamic operations on data blocks i.e. data update, append and delete. So the concepts of similarity relevance and scheme robustness to formulate the privacy issues in encryption schemes, and then solve the insecurity problem by proposing a random key encryption scheme is introduced.

Novel technologies in the cryptography community and information retrieval community are employed, including homomorphic encryption and vector space model. In the proposed scheme, the majority of computing work is done on the encrypted data while the user takes part in ranking, which guarantees top k multi-keys provides efficient retrieval of data over encrypted data with high security and practical efficiency.

Discussion (Fully Homomorphic Encryption):

A cryptosystem that supports arbitrary computation on ciphertexts is known as Fully Homomorphic Encryption (FHE) and is far more powerful. Such a scheme enables the construction of programs for any desirable functionality, which can be run on encrypted inputs to produce an encryption of the result. Since such a program need never decrypt its inputs, it can be run by an untrusted party without revealing its inputs and internal state. The existence of an efficient and fully homomorphic cryptosystem would have great practical implications in the outsourcing of private computations, for instance, in the context of cloud computing.The utility of fully homomorphic encryption has been long recognized. The problem of constructing such a scheme was first proposed within a year of the development of RSA.

A solution proved more elusive; for more than 30 years, it was unclear whether fully homomorphic encryption was even possible. During that period, partial results included the Boneh–Goh–Nissim cryptosystem that supports evaluation of an unlimited number of addition operations but at most one multiplication, and the Ishai-Paskin cryptosystem that supports evaluation of (polynomial-size) Branching program. Homomorphic encryptions allow complex mathematical operations to be performed on encrypted data without compromising the encryption. In mathematics, homomorphic describes the transformation of one data set into another while preserving relationships between elements in both sets Homomorphic encryption is expected to play an important part in cloud computing, allowing companies to store encrypted data in a public cloud and take advantage of the cloud provider’s analytic services.

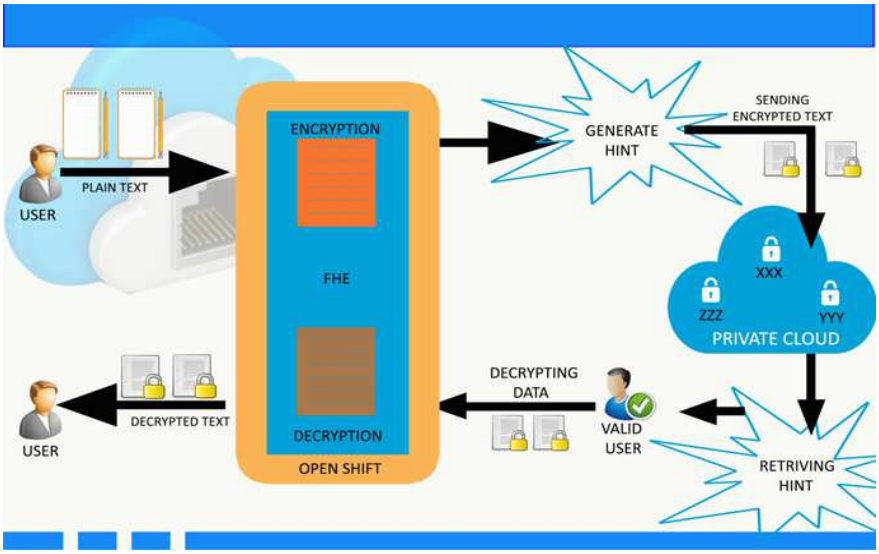

Fig. 1: FHE Architecture

Advantages:

- To achieve better robustness and improve efficiency.
- This scheme fulfills the secure multi-keyword top-k retrieval over encrypted data. Specifically, for the first time we employ relevance score to support multi-keyword top-k retrieval.

Conclusion:

To share data flexibly is vital thing in cloud computing. Users prefer to upload there data on cloud and among different users. Outsourcing of data to server may lead to leak the private data of user to everyone. Encryption is a one solution which provides to share selected data with desired candidate. Sharing of decryption keys in secure way plays important role. Public-key cryptosystems provides delegation of secret keys for different cipher text classes in cloud storage. The delegate gets securely an aggregate key of constant size. It is required to keep enough numberof cipher texts classes as they increase fast and the cipher text classes are bounded that is the limitation.

REFERENCES

Atallah, M.J. *et al*, 2009. Dynamic and Efficient Key Management for Access Hierarchies :Proceedings on ACM Transaction on Information and System Security (TISSEC), pp: 1-18.

Chase, M. *et al*., 2009. Improving privacy and security in multi-authority attribute-based encryption: Proceedings of the 16th ACM conference on Computer and communications security, pp: 121-130.

Goyal, V. *et al*, 2006. Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data: Proceedings on 13th ACM Conference on Computer and Communication Security (CCS), pp: 89-98.

Jahid *et al*., 2011. easier: encryption-based access control in social networks with efficient revocation: proceeding of the 6th ACM Symposium on Information, Computer and communications Security, pp: 411-415.

LI Shuchengyu M. *et al*., 2013. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption: Proceedings on IEEE Transactions on parallel and distributed system, pp: 131-143.

Melissa Chase, 2007. ,Multi-authority Attribute Based Encryption, Theory of Cryptography, 4392: 515-534.

Ruj *et al*., 2011. Distributed Access Control in clouds: Proceeding of IEEE 10th International Conferenceon Trust, security and privacy in computing and communications, pp: 91-98.

Wang, B. *et al*, 2013. Storing Shared Data on the Cloud via Security-Mediator: Proceedings on IEEE 33rd Int'l Conf .Distributed Computing Systems (ICDCS), pp: 124-133.

Wang, C. *et al*., 2013. Privacy-Preserving Public Auditing for Secure Cloud Storage:Proceedings on IEEE transaction on computer, pp: 362-375.

Zhang, Q. *et al*, 2004. A centralized key management scheme for hierarchical access control: Proceedings on global telecommunications conference, pp: 2067-2071.