I J C T A, 9(13) 2016, pp. 6329-6334

Key-Summative Searchable Encryption (KSSE) for Faction Information Distribution via Cloud Storage

Varsha Gupta[*] and M. Murali[*]

ABSTRACT

Cloud computing is an IT outsourcing or another way to describe revolution in information technology. It is a network based computing which provides storage, software, platform and infrastructure as a service. It provides cloud user to centralize storage for data and information in large number of remote storage server which are connected through network. It also provides internet access to computer services and resource. In cloud computing security, authentication, privacy, and access control of sensitive data and personal information of cloud users are big challenging issue when cloud provider's servers are not trusted domain of data owner. Data sharing is an important functionality in cloud storage. Sharing of data with large number of participants arise several issues, including privacy of data owner, authentication, data integrity and efficiency. One of promising way to construct an anonymous and authentic data sharing system is Ring signature. There is bottleneck for this solution to be scalable when the costly certificate verification in the traditional Public Key Infrastructure (PKI). Instead we can use Identity based (ID based) ring signature, which eliminates the process of certificate verification. In this paper "Key Summative Searchable Encryption (KSSE) for faction information distribution via cloud storage" we are going to discuss how to resolve above security issue in cloud data sharing.

Keywords: Cloud security; Data sharing; Authentication; Access control; Encryption; Decryption; Key.

I. INTRODUCTION

Cloud computing is a bunch of commodity computers networked together. These are operating together to serve a number of cloud customers with different need in same or different geographical location. With the help of virtualization cloud computing provides workload on demand basis. Cloud services are provided services to the cloud users using pay-as-you-use (pay per use) business model. These services are generally described as XaaS (X as a Service). Here X can be Software, Storage, Platform or Infrastructure etc. Cloud computing service provider provides these services to cloud user to build their applications in the internet in order to deliver them to end users. Because of this cloud users don't have to worry about software installing, maintaining hardware which is needed. These services are affordable as user pays for how much they use. Hence instead of establishing IT infrastructure they can use cloud services to reduce expenditure in IT. National Institute of Standard and Technology (NIST) defined five characteristics which are essential for cloud computing these are on-demand self-service, broad network access, rapid elasticity, resource polling, and measured service. There are mainly four types of cloud computing deploy model private cloud, public cloud, community cloud, hybrid cloud. There are so many advantages of cloud computing, some important advantages are cost efficient, almost unlimited storage, backup and recovery, easy access of information, automatic software integration, quick deployment. Although there are so many advantages of cloud computing, there are some disadvantages of cloud computing like technical issues, security in the cloud, prone to attack, privacy of data owner, authentication, data integrity and efficiency. So we will

[*] Department of Computer Science and Engineering, SRM University, Chennai-603203, Tamilnadu, India, *E-mail: vgupta926@gmail.com; murali.m@ktr.srmuniv.ac.in*

discuss how to resolve the security issue in data sharing with in cloud by Key Summative Searchable Encryption (KSSE) method which is proposed in this paper.

II. DESIGN OBJECTIVE OF SECURE DATA SHARING IN CLOUD

(A) Authentication

While accessing any information authentication is an important aspect to consider. The identity of the user and his access rights can be proved with login id and password for authentication. But the authentication of this type can be easily hacked. Some of the common existing authentication approaches like SMS based authentication, Password and PIN based authentication, Symmetric-key authentication, Public-key authentication, Biometric authentication.

(B) Integrity

It means only the authorized user can access and modify the information. In other words it is nothing but protecting the data from the unauthorized user.

(C) Confidentiality

It means limiting the access or putting restrictions on certain type of information.

(D) Access control

It means if the control is given to any person from the authorized user, then that person can have access over that information.

(E) Scalability

It means widespread of the information. Scalability is the capability of a system, network. The process of handling a growing amount of work or we can say that potential for accommodate that enlarged growth.

(F) Storage Efficiency

The ability to manage and store large amount of data that consumes the least amount of space is called storage efficiency when little or no impact on performance. Total operational cost is lower when storage is efficient.

(G) High Reliability

It means succeeded in avoiding an environment where normal accident can be expected due to complexity and risk factor. Data fault tolerant is used by the cloud user to ensure the high reliability of the service.

(H) Encryption decryption

In the cryptography encryption is the process of changing messages into unreadable form or encoding messages in such a way that only authorized person can read it after decrypting the messages.

III. EXISTING SYSTEM

In existing system centralized approach describes the how to store and access the sensitive information in cloud. For distribution of secret keys and attributes to all users the single key distribution center (KDC) used. But unfortunately, a single key distribution center (KDC) is not only a one single point of failure but also difficult to maintain because in a cloud environment large number of users that are supported. The

scheme does not support authentication when uses a symmetric key approach. In Ciphertext-Policy Attribute-Based Encryption (CP-ABE) contain the secret key that can decrypt the file. So when the user tries to access a file, the system will match the user attributes that associated with user key. The system will decrypt the file, if those attributes satisfies the access policy associated with the file, otherwise it will not be decrypted.

(A) Disadvantages of Existing System

- The centralized approach keywords are sent to the cloud encrypted, and without knowing the actual keyword for the search the cloud returns the result. Data records should have keywords associated with them to enable the search, is main problem here.
- In existing system distributed key only possible. Data will be encrypted but key not secure.
- It also addresses the concern of data leaks in the cloud storage.
- The key distribution center (KDC) is a single key management uses a symmetric key approach and does not support authentication.
- The KDC is not only a single one point of failure but also difficult to maintain because in a cloud environment large number of users that are supported.
- The user can create and store a file and other users can only read the file. Other than the creator write access was not permitted to users.

IV. PROPOSED SYSTEM

In this concept of Key-Summative Searchable Encryption (KSSE), all the data is encrypted before it is uploaded in cloud storage so that later it can be retrieved by those who are having decryption keys. In the Proposed system introduce a new decentralized access control scheme used for secure data storage. By using this scheme, cloud server helps to identify the user as an authorized one, without knowing the user identity before storing the data. In key aggregation or summative method single key will be using for encryption and decryption. In which a data owner distribute a single key to another user for sharing a large number of documents, and for querying the shared documents single trapdoor only needs to submit by user to the cloud. In addition, the scheme has an added feature of access control which means authorized users can access the data.

We can use Identity based (ID based) ring signature, which eliminates the process of traditional costly certificate verification. In this KSSE there are three users: creator, reader & writer. Creator receives a token from a trustee i.e. organization after giving ID to the trustee. There is multiple key distribution centers (KDC) which can be scattered. A creator gives their token to one or more KDC's then creator receives keys for encryption & decryption and for signing from KDC's. The message is encrypted under access policy which means it decides who can access or which participant can access the data stored in the cloud. The proposed system flexibly shares large number of data within cloud storage and appears securely, efficiently.

(A) Advantages of Proposed System

- The decentralized access control scheme used for secure data storage. Using this scheme an authorized user is identified by the help of cloud server, without knowing the user identity before storing the data.
- The multiple key distribution centers (KDC) used for distributing secret keys and attributes to users.
- It is provide the high security by using encryption and decryption keys for sensitive information.
- Based on the attributes the cipher text is sent to the cloud and then cloud verifies the attribute key signature and stores the cipher text.

- The cloud sends cipher text when user wants data. If the user has matching attributes key with access policy, it can get back original message by decryption process.

V. SYSTEM ARCHITECTURE

(A) Block Diagram of KSSE System

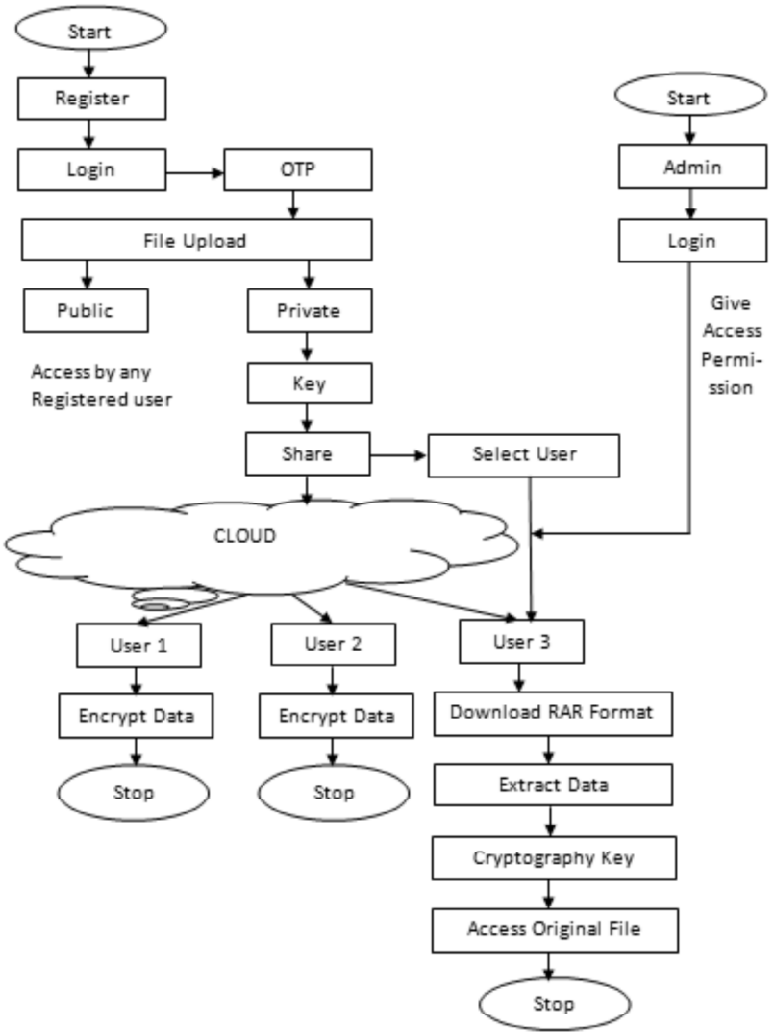

Figure 1: Block Diagram of KSSE System

(B) Block Diagram Description

In this process (Fig. 1. Block Diagram of KSSE System) cloud user, register them by giving general information like name, age, date of birth, gender, email id, phone number. After registration process admin sends the login id and password to user via email. User can login by provided user id and password. After that for authentication verification, otp (one time password) will be generated which user can receive via email. Once the correct otp is generated, user can upload document file by two options that is public and sharing (private). Files which are uploaded publicly are accessed by other users in group. If user wants to upload data as sharing (private) for only number of another user then it requires a key which is used to encrypt the data. After that user has to share the key with an authorized another user. Then after verified by admin another user can access data and download data but is in encrypted format (.rar format). When data is extracted by authorized user the cryptography key is received via email. By entering correct cryptography

key decryption is done and the authorized user can access the original file. If any unauthorized user downloads the shared file which is encrypted, they are not able to access the original file because user does not have the cryptography key.

(C) Modules Description

Architecture design is divided into five modules. These modules will describe each individual phase in more descriptive manner to understand the mechanism of proposed system.

1. *Secure stroage:* The user authentication process is done by the admin. Every user's give their personal details for registration process. For accessing the cloud space every user will get an ID after registration process. The user can edit the information if they want then submit all the details to the admin and later admin will edit and update the information. This process is controlled by the Admin. Every user share their data and information in their own cloud space provided by the admin. Only the registered user can store data in cloud for providing security because information may be sensitive or important.
2. *Key re-authentication:* The information and data shared by the user in the cloud is encrypted by using MD5 algorithm. All the information shared by every user is encrypted based on the data sensitivity and stored in the cloud. Client side configuration performs two main actions. The two actions are access control and permission control. Access control – this process is based on the server control features by Admin. Permission control – this process is based on the client control features.
3. *Integrity checking:* Integrity checking is the process of comparing the encrypted information with altered cipher text. If there is any change in detection a message will send to the user that the encryption process is not done properly. If there is no change in detection means then it will allow doing the next process. Integrity checking is mainly used for anti-malware controls. The encrypted data is decrypted only by the public key of data owner by another user. Converting cipher text into plain text is called decryption. AES (Advance encryption standard) algorithm is used for encryption and decryption the information. The user can see data and also can download data with high security.
4. *Data sharing:* By using that user's public key the encrypted data or information forwarded to another user account which is stored in the cloud. If any user wants to share their information with their friends or someone they can directly forward the encrypted data to them. Without downloading the data the user can forward the information to another user. Secure Data Forwarding is implemented by detecting flag generation where for sharing flags will be 0-1 and where for forwarding flags 1-1 is detected. If flag 1-1 is detected then data are filtered out by applying Filtering technique.
5. *Filtering security:* In filtering security fine-tuning is done to match application's distinct characteristics to avoid advance attacks in web apps. Content filtering usually works by specifying character strings, if matched, then screened out undesirable content that is to be indicated. Typically screened content for pornographic and sometimes also for hate oriented or violence content.

VI. CONCLUSION

The proposed method mainly describes about the modules which are present in the Key Summative Searchable Encryption (KSSE) for faction information distribution via cloud storage. In key aggregation or summative method single key will be using for encryption and decryption. In which a data owner distribute a single key to another user for sharing a large number of documents, and for querying the shared documents single trapdoor only needs to submit by user to the cloud. In addition, the scheme has an added feature of access control which means authorized users can access the data. Hence the efficiency improved in terms

of security, authentication, access control, confidentiality, integrity and scalability. In the proposed system only privilege is given read option for document to authorized user but for future work privilege can be provided to the authorized user to write (edit) the data and secure sharing in cloud environment. In this proposed scheme the security analysis and performance evaluation both confirm provably secure and practically efficient for confidential data sharing in cloud.

ACKNOWLEDGMENT

This work was supported by SRM University, Chennai, Tamilnadu, India.

REFERENCES

[1] B. Wang, B. Li, and H. Li, "Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud", Proc. 10th Int'l Conf. Applied Cryptography and Network Security, pp. 507-525, 2012.

[2] C. Chu, S. Chow,W. Tzeng, et al. "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage", IEEE Transactions on Parallel and Distributed Systems, 2014, 25(2): 468-477.

[3] S. Kamara, C. Papamanthou, T. Roeder. "Dynamic searchable symmetric encryption", Proceedings of the 2012 ACM conference on Computer and communications security (CCS), ACM, pp. 965-976, 2012.

[4] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine Grained Data Access Control in Cloud Computing", Proc. IEEE INFOCOM, pp. 534-542, 2010.

[5] X.F. Chen, J. Li, X.Y. Huang, J.W. Li, Y. Xiang. "Secure Outsourced Attribute-based Signatures", IEEE Trans. on Parallel and Distributed Systems, DOI.ieeecomputersociety.org/10.1109/TPDS.2013.180, 2013.

[6] X. Liu, Y. Zhang, B. Wang, and J. Yan. "Mona: secure multiowner data sharing for dynamic groups in the cloud", IEEE Transactions on Parallel and Distributed Systems, 2013, 24(6): 1182-1191.

[7] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance:The Essential of Bread and Butter of Data Forensics in Cloud Computing", Proc. ACM Symp. Information, Computer and Comm.Security, pp. 282-292, 2010.

[8] R. Curtmola, J. Garay, S. Kamara, R. Ostrovsky. "Searchable symmetric encryption: improved definitions and efficient constructions", In: Proceedings of the 13th ACM conference on Computer and Communications Security, ACM Press, pp. 79-88, 2006.

[9] D. Boneh, C. G, R. Ostrovsky, G. Persiano. "Public Key Encryption with Keyword Search", EUROCRYPT 2004, pp. 506C522, 2004.

[10] Y. Hwang, P. Lee. "Public Key Encryption with Conjunctive Keyword Search and Its Extension to a Multi-user System", In: Pairing-Based Cryptography C Pairing 2007, LNCS, pp. 2-22, 2007.

[11] F. Zhao, T. Nishide, K. Sakurai. Multi-User Keyword Search Scheme for Secure Data Sharing with Fine-Grained Access Control. Information Security and Cryptology, LNCS, pp. 406-418, 2012.

[12] J. W. Li, J. Li, X. F. Chen, *et al.* "Efficient Keyword Search over Encrypted Data with Fine-Grained Access Control in Hybrid Cloud", In:Network and System Security 2012, LNCS, pp. 490-502, 20120.