RESEARCH ARTICLE OPEN ACCESS

Attribute-Based Data Sharing

Ms. Rahila Fatima Mir Asif Ali
Student, CSE Department, at Dr. Seema Quadri Institute of Tech, Aurangabad, Maharashtra, India

Messages addressed to specific users can be decrypted by Key Generation Centre (KGC) by generating their private keys. Data owner wants the data to be delivered only to specified user and not to unauthorized person that is the data owner makes their private data accessible only to authorized person. We propose attribute based encryption and escrow problem which means written agreement delivered to a third party to overcome this problem. Attribute based Encryption (ABE) is a type of public-key encryption in which the private key of a user and the cipher text are dependent upon attributes. It is a promising cryptographic approach.

I. Introduction

If we take today's scenario, the use of technology and internet made us relax in portability of data. We can nowadays share almost everything others like pictures, movies, thoughts, etc. If we need an emergency help from a doctor or hospital for chronic diseases like cardio, hepatic, neuro related previous data, we are now able to produce with the help of internet or cloud technology. Due to large number of internet users, it is also required to protect our data from being misused. An unauthorized person should not be made access to the private data of an individual. For this reason we are required to take care of data by implementing data protection techniques like cryptography. Our work in this area is based on Attribute based Encryption.

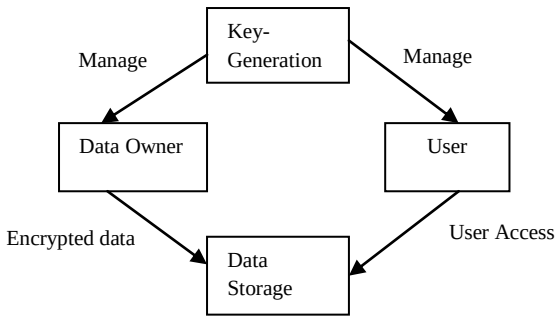

Fig 1. Architecture of a data

We are using the cipher text policy attribute based encryption that provides us to define set of attributes required by the decryptor for the cipher text. Everyone using the technique based on policy decrypts the required data. By this method, we didn't need data server to prevent data from unauthorized user access. There are many challenges, in using the attribute based encryption system in data sharing environment. The key generation process gives an approach for reduction of processing and authorization certification. We in this paper are proposing a model to work on attribute based encryption technique for the shared data. Proposed model works as shown in the fig. 1. Here the data storage contains the shared data which can be accessed by data owner and user. The data is managed by the key generation module which generates a key for encryption. The key generation module manages the data owner and user domains. The policy is defined in the key generation module which is implemented to manage the two modules viz data owner and user.

II. Literature Survey

In literature we studied found that many researchers working on attribute based encryption uses almost similar techniques. Changsha et al [1] in their study propose a novel two-dimensional-scalable access control by generating access keys. Their analysis showed the scheme is able to provide collusion resistance, as well as forward and backward secrecy. Ming et al [2] enabled dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. Huang Qinlong et al [3] presented a multiparty access control model, enabled the disseminator to update the access policy of ciphertext if their attributes satisfy the access policy.

Zhu et al [4], Linke et al [5] [7] [9] experimentally proved that fuzzy authorization can achieve fuzziness of authorization among heterogeneous clouds with security and efficiency. Correa et al [6] and Jadliwala et al [15] proposed WhACKY! to harness the multi-source information from tweets to link Twitter profiles across other external services. WhACKY! guarantees that the mapped profiles are 100% true-positive and helps quantify the unintended leakage of Personally Identifiable Information (PII) attributes. During the process, WhACKY! is able to detect duplicate Twitter profiles connected to multiple external

services. Yanchao et al [8] presented two novel schemes for users to detect fake top-k query results as an effort to foster the practical deployment and use of the proposed system. Yan Zhu et al [10] proposed a novel cryptographic comparison method based on forward and backward deviation functions. The method supported dual range comparisons and tree-oriented keyword search, as well as almost constant complexity for large size of integer range. They also provided several authentication mechanisms for preventing unpermitted access and verifying validity of protocol output.

Varalakshmi et al [11] proposed SMOADS - Secured Multi Owner Attribute-based Data Sharing - along with dynamic manager to ensure secured data sharing on cloud and also reduce the hacking probability. They proposed work, dynamism introduced at various levels which reduces the scope of hacking. The multi-level dynamism is characterized by multi owner and dynamic manager - defined by Certificate Authority (CA) and these are made effective through the proven CP-ABE Shuaishuai et al [13], Xin et al [16] for efficient decryption and revocation. Liu et al [12], Tenglong et al [14] proposed a shared authority based privacy-preserving authentication protocol (SAPA) to address above privacy issue for cloud storage. In the SAPA, shared access authority is achieved by anonymous access request matching mechanism with security and privacy considerations, attribute based access control is adopted to realize that the user can only access its own data fields and proxy re-encryption is applied by the cloud server to provide data sharing among the multiple users. Meanwhile, universal composability (UC) model is established to prove that the SAPA theoretically has the design correctness. It indicates that the proposed protocol realizing privacy-preserving data access authority sharing, is attractive for multi-user collaborative cloud applications. Ling-Hua et al [17] developed two tools previously called ISG and DWL and ISG is for generating information systems and DWL is for generating web systems using building files of ISG to build the file system of a web-based system and each attribute of an object to be specified for translating these settings to Java. Dutta et al [18] proposed a technique of using a well-known threshold-based visual secret sharing scheme to address the issue of privacy and trust in cloud databases and database-as-a-service offerings. They considered data records with at least one prime attribute and proposed an indexing technique for the secret shares of records in a large database based on some properties of the secret sharing technique. Their technique was aimed at minimizing storage overhead of secret shares as well as high speed upload and retrieval of data. Their implementation using Hadoop Distributed File System (HDFS) with Matlab showed that technique minimizes storage overhead due to secret shares and ensures high speed data upload and retrieval.

III. Proposed Model

Let there be a space of users. Let there be the identity of each user space with descriptive attributes in the system. Let there be a set of users that hold the attribute, which is referred to as an attribute group. This group will be used as a user access or revocation list Let there be the universe of such attribute groups. Let there be the attribute group key that is shared among the non revoked users.

The key generation centre and the data-storing center are involved in the user key issuing protocol. In the protocol, a user is required to contact the two parties before getting a set of keys. The key generation centre is responsible for authenticating a user and issuing attribute keys to him if the user is entitled to the attributes. The secret key is generated through the secure 2PC protocol between the key generation centre and the data-storing center. They engage in the arithmetic secure 2PC protocol with master secret keys of their own, and issue independent key components to a user. Then, the user is able to generate the whole secret keys with the key components separately received from the two authorities. The secure 2PC protocol deters them from knowing each other's master secrets so that none of them can generate the whole secret keys of a user alone.

The first step of the key issuing protocol is to generate the user secret keys using secure 2PC protocol between the key generation centre and the data-storing center. When the key generation centre authenticates a user who is entitled to a set S of attributes, the key generation centre starts to perform the secure 2PC protocol with the data-storing center. Then, the user receives two key components from the data-storing center and key generation centre, respectively, as a result of the protocol. We require that the user can derive the whole secret key set using the two key components.

Since the first CP-ABE scheme was proposed, dozens of the subsequent CP-ABE schemes have been suggested, which are mostly motivated by more rigorous security proof in the standard model. However, most of the schemes failed to achieve the expressiveness of the scheme, which described an efficient system that was expressive in that it allowed an encryptor to express an access predicate in terms of any monotonic formula over attributes. Therefore, in this section, we will be developing a variation of the CP-ABE algorithm partially constructed in order to enhance the expressiveness of the access control policy instead of building a new CP-ABE scheme from

scratch. Its key generation procedure is modified for our purpose of removing escrow. The proposed scheme is then built on this new CP-ABE variation by further integrating it into the proxy re-encryption protocol for the user revocation.

To handle the fine-grained user revocation, the data storing center must obtain the user access or revocation list for each attribute group, since otherwise revocation cannot take effect after all. This setting where the data-storing center knows the revocation list does not violate the security requirements, because it is only allowed to re-encrypt the cipher texts and can by no means obtain any information about the attribute keys of users.

The scheme of construction will contain the following steps.

1) System setup
2) Key Generation
3) Data Encryption
4) Data Re-encryption
5) Data Decryption
6) Key Update
7) Key Revocation
8) Efficiency

IV. Conclusion

To conclude, the implementation of access policies is important in the data sharing environment. In this study, we proposed an attribute based data sharing scheme which will be implemented on a fine-grained data access control. The proposed scheme issues a key that removes key escrow. The user keys are generated by computation such that any key generation center cannot derive the private key. Thus, the proposed scheme enhances data privacy and confidentiality in the data sharing system. Therefore, the proposed scheme achieves more secure and fine-grained data access control in the data sharing system. We would like to point that the proposed scheme is efficient and scalable to securely manage user data in the data sharing system.

References

[1]. Changsha Ma ; Chang Wen Chen "*Secure media sharing in the cloud: Two-dimensional-scalable access control and comprehensive key management*", Multimedia and Expo (ICME), 2014 IEEE International Conference, DOI: 10.1109 /ICME. 2014. 6890308 , Publication Year: 2014 , Page(s): 1 – 6

[2]. Ming Li ; Shucheng Yu ; Yao Zheng ; Kui Ren ; Wenjing Lou, "*Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption*", Parallel and Distributed Systems, IEEE Transactions, Volume: 24 , Issue: 1, DOI: 10.1109/TPDS.2012.97, Publication Year: 2013 , Page(s): 131 - 143

[3]. Huang Qinlong ; Ma Zhaofeng ; Yang Yixian ; Niu Xinxin ; Fu Jingyi, "*Improving security and efciency for encrypted data sharingin online social networks*", Communications, China, Volume: 11 , Issue: 3, DOI: 10.1109/CC.2014.6825263, Publication Year: 2014 , Page(s): 104 – 117

[4]. Zhu, S. ; Gong, G., "*Fuzzy Authorization for Cloud Storage*", Cloud Computing, IEEE Transactions Volume: PP , Issue: 99, DOI: 10.1109/TCC. 2014.2338324, Publication Year: 2014 , Page(s): 1

[5]. Linke Guo ; Chi Zhang ; Hao Yue ; Yuguang Fang, " *A privacy-preserving social-assisted mobile content dissemination scheme in DTNs*", INFOCOM, 2013 Proceedings IEEE, DOI: 10.1109/INFCOM.2013. 567034, Publication Year: 2013 , Page(s): 2301 – 2309

[6]. Correa, D. ; Sureka, A. ; Sethi, R., "*WhACKY! - What anyone could know about you from Twitter*", Privacy, Security and Trust (PST), 2012 Tenth Annual International Conference, DOI: 10.1109/ PST. 2012.6297918, Publication Year: 2012 , Page(s): 43 - 50

[7]. Linke Guo ; Chi Zhang ; Yuguang Fang, "*Privacy-preserving revocable content sharing in geosocial networks*", Communications and Network Security (CNS), 2013 IEEE Conference, DOI: 10.1109/CNS. 2013. 6682699 , Publication Year: 2013 , Page(s): 118 - 126

[8]. Yanchao Zhang ; Yanchao Zhang ; Chi Zhang, "*Secure top-k query processing via untrusted location-based service providers*", INFOCOM, 2012 Proceedings IEEE, DOI: 10.1109 /INFCOM. 2012.6195476, Publication Year: 2012 , Page(s): 1170 - 1178

[9]. Linke Guo ; Chi Zhang ; Hao Yue ; Yuguang Fang, "*PSaD: A Privacy-Preserving Social-Assisted Content Dissemination Scheme in DTNs*", Mobile Computing, IEEE Transactions, Volume: 13 , Issue: 12, DOI: 10.1109/TMC. 2014.2308177, Publication Year: 2014 , Page(s): 2903 – 2918

[10]. Yan Zhu ; Di Ma ; Shanbiao Wang, "*Secure Data Retrieval of Outsourced Data with Complex Query Support*", Distributed Computing Systems Workshops (ICDCSW), 2012 32nd International Conference,

DOI: 10.1109/ICDCSW. 2012.91, Publication Year: 2012 , Page(s): 481 - 490

[11]. Varalakshmi, P. ; Shajina, A.R. ; Soniya, V.S., "*SMOADS - Secured Multi-Owner Attribute-based DataSharing in cloud computing*", Advanced Computing (ICoAC), 2013 Fifth International Conference, DOI: 10.1109/ICoAC. 2013.6921970, Publication Year: 2013 , Page(s): 318 - 324

[12]. Liu, H. ; Ning, H. ; Xiong, Q. ; Yang, L.T., "*Shared Authority Based Privacy-preserving Authentication Protocol in Cloud Computing*", Parallel and Distributed Systems, IEEE Transactions, Volume: PP , Issue: 99, DOI: 10.1109/TPDS.2014.2308218, Publication Year: 2014 , Page(s): 1

[13]. Shuaishuai Zhu ; Xiaoyuan Yang ; Xuguang Wu, "*Secure Cloud File System with Attribute based Encryption*", Intelligent Networking and Collaborative Systems (INCoS), 2013 5th International Conference, DOI: 10.1109/INCoS. 2013.22, Publication Year: 2013 , Page(s): 99 - 102

[14]. Tenglong Wang ; Hong Liang ; Bisheng Wei ; Hongzhen Shi, "*The study of urban drainage network information system space framework data standards in kunming based on GIS*", Software Engineering and Service Science (ICSESS), 2013 4th IEEE International Conference, DOI: 10.1109 /ICSESS .2013. 6615266, Publication Year: 2013 , Page(s): 107 - 111

[15]. Jadliwala, M. ; Maiti, A. ; Namboodiri, V., "*Social Puzzles: Context-Based Access Control in Online Social Networks*", Dependable Systems and Networks (DSN), 2014 44th Annual IEEE/IFIP International Conference, DOI: 10.1109/DSN. 2014.38, Publication Year: 2014 , Page(s): 299 - 310

[16]. Xin Dong ; Yu Jiadi ; Yuan Luo ; Yingying Chen ; Guangtao Xue ;Minglu Li, "*P2E: Privacy-preserving and effective cloud data sharing service*", Global Communications Conference (GLOBECOM), 2013 IEEE, DOI: 10.1109 /GLOCOM.2013.6831152, Publication Year: 2013 , Page(s): 689 – 694

[17]. Ling-Hua Chang ; Behl, S. ; Shieh, T.-H., "*Amazing of Using ISG on Implementing a Web-BasedSystem*", Parallel and Distributed Computing, Applications and Technologies (PDCAT), 2013 International Conference, DOI: 10.1109 /PDCAT. 2013.14, Publication Year: 2013 , Page(s): 44 - 49

[18]. Dutta, R. ; Annappa, B., "*Privacy and trust in cloud database using threshold-basedsecret sharing*", Advances in Computing, Communications and Informatics (ICACCI), 2013 International Conference, DOI: 10.1109 / ICACCI.2013.6637278, Publication Year: 2013 , Page(s): 800 - 805

About Author:-

Rahila Fatima Mir Asif Ali- I am pursuing Master degree in computer Science & engineering from Dr. Seema Quadri Institute of Tech, Aurangabad, My area of interest is C#.net, Database, Networking.

Mrs. Seema Singh Solanki-She is currently working as Assistant Professor in the Department of Computer, Dr. Seema Quadri Institute of Tech, Aurangabad, India. Her research area includes Reusability of software components.

Zafar Ul Hasan-
Qualification ME(Comp), MBA(Mkg), LMISTE
Institute: Intellisense Research & Development (IRD) Consultancy, Aurangabad.