ISSN 2319 – 7595
Volume 8, No.2, March - April 2019
International Journal of Information Systems and Computer Sciences
Available Online at http://warse.org/IJISCS/static/pdf/file/ijiscs29822019.pdf
https://doi.org/10.30534/ijiscs/2019/29822019

Attribute And Time Factors Combined CP-ABE and RSA based Access Control Scheme for Public Cloud

Parvathy Radhakrishnan[1],Nayana N Panicker[2],Sheedhal Susan John[3] ,Nivyamol P Varghese[4] Divya S B [5]
[1] Mangalam College of Engineering, India, pkrishnan791@gmail.com
[2] Mangalam College of Engineering, India, nayananpanicker20@gmail.com
[3] Mangalam College of Engineering, India, sheedhalsusanjohn@gmail.com
[4] Mangalam College of Engineering, India, nivyamolp@gmail.com
[5] Mangalam College of Engineering, India ,divya.sb@mangalam.in

ABSTRACT

Cloud computing a basic technology for sharing resources on the internet and is gaining popularity day by day and becoming an integral part of business because of its effective storage, data processing ,cost effectiveness and reliability. Despite of these advantages, security and privacy of data in the cloud are of critical concern. A three level security can be added to the data in the cloud with RSA as the base ,fine grained access control and time sensitivity of data can be achieved by embedding time CP-ABE (Ciphertext-Policy Attribute Based Encryption). Thus, a better level of security to the data in the public cloud can be achieved.

Key words: Fine-grained access control, Time sensitive data, CP-ABE.

1.INTRODUCTION

Cloud storage devices, a model of computer data storage devices and is accessed from many platforms like cloud computing, IP and so on. Cloud system achieving their efficiency in day-by-day. Cloud system ensure a better performance factors in terms of security and privacy. From the beginning, it’s only a simple cloud system which is used to store information and other practical applications. A collection of information called data, which is used to store that data in cloud database.

To ensure that the security policies provided is to be better in the concept on time-sensitive analysis. The encrypted message or the information can be accessed and stored on the cloud data storage based on the time. Even though CP-ABE (Ciphertext-policy Attribute Based Encryption) algorithm provide security there is a limitation that multiple copy of data are storing together and produce only one copy of data and there is a chance of data loss and may achieve insecurity. One major challenge while using with this scheme is to attaining flexible time sensitive data and fine-grained access control methods. Thus, CP-ABE system cannot provide security itself. It is a type of attribute-based encryption scheme which is used in this system. It uses access trees to encrypt data and users’ secret keys are generated within a set of attributes, CP-ABE is mainly focused on the design of the access structure. The data owners share their data to the user which preserves data security and ensures data confidentiality conditions based on time concepts. The proposed system achieves its goal.

The aim is that, all wanted secure data transformation and should be kept private. So different encryption algorithms are experimented and finally achieving the goal. Here, mainly focus on three levels of security concerns. That is by using RSA algorithm, time, attributed based concept for secure data sharing and accessing. When data owners share their data or any other posts to the clients who are a part of the specified platform then within the time limit the clients can be accessed otherwise it will be invisible to the user. Rivest–Shamir-Adleman algorithm (RSA algorithm) is one of the best cryptographic algorithms for security based concepts. Due to its asymmetric feature (used for encrypting and decrypting messages). Mainly RSA provides two types of keys: (i) one must be kept private and (ii) another is for either public or private. And this concept is embedded into the proposed system and enhances the security. Here, RSA is used for secure access control in public cloud storage devices.

Here attribute based concepts mainly focus on two types of attributes for accessing the clients. By the time of user wish to access the platform there is a concept of two attributes have to be filled ,if that two attributes are satisfying the database the user can easily login into that page and sharing photos, videos text ,audio messages respectively. The two attributes are namely, (i) on the basis of continents and (ii) on the basis of gender. By using continents, data specification space is less needed. For example by giving a country name as an attribute in that contains many number of subdivisions are came out such as states, districts, city etc. Hence it is better to us continents name as one attribute. Second, is that in terms of gender the user can access. Time based concept, within a time limit the given shared photos and other information can be viewed. It is one of the encryption methods for accessing the information stored in the cloud database. Hence, the above listed three concepts of security terms and these are embedded into a CP-ABE system for better security and confidentiality aspects.

The rest of the paper is constructed as follows: first review some existing work that is similar to the data access control for time sensitive in Section II. In Section III, the proposed system and its block diagram in detail. In Section IV follows the experimentation results and its brief description. Finally conclude the paper in Section V and then follows future scope.

2.LITERATURE REVIEW

There are many researchers has been done and many methods have been proposed for secure data transmission and its privacy attributes. Here, explore few of them are as follows:

Jianan Hong, Kaiping Xue, Ying jie Xue, Weikeng Chen, David S.L. Wei, Nenghai Yu and Peilin Hong [1]have been proposed that time based access control can be improved by using CP-ABE and TRE security schemes. Hence, the overall performance of data access security based on cloud storage system can be improved.

SKan Yang, Xiaohua Jia, Kui Ren, Bo Zhang[2] have offers that an effective and secure data access control with decryption and decision-making [2] which improves both forward and backward securities. It is clear that not having an efficient security is provided while using multi-authority storage devices and due to the decryption and revocation control is less insufficient.

Dayananda RB, Prof. Dr. G.Manoj Someswar, have been proposed that in re-encryption[3]system provides the data owner is responsible for data access, data sharing and allowing attributes secret keys for user to be accessed. When the user wishes to access the information and request is sent to the server and decrypts the content and again encrypt the given contents.

Elli Androulaki, Claudio Soriente, Luka Malisaand Srdjan Capkun [4] based on location and time access control methods are used to locate the user's access control techniques and accuracy would be better achieved in terms of encryption and decryption algorithms can be improved. on-flexibility as defined in the random oracle model, under the Strong Diffie-Hellman assumption (SDH).

C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou [5] depends on storage devices can be achieved such a way that to detect the disordering server and ensure better cloud storage efficiency procedures and it consist of malicious code attacks from the given information.

Qin Liu, Chiu C. Tan, Jie Wu, Guojun Wangin [6] have proposed the formation of generated key encryption, re-encryption and decryption on the basis of synchronized clock with delays. Hence security level is reduced.

Yan Zhu, Hongxin Hu, Gail-Joon Ahn, Dijiang Huang, and ShanbiaoWangint [7] have proposed that the overall access control in cloud computing is for encrypt and decrypt the information and provide better performance in terms of flexibility, protection, and privacy terms.

Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou Fine-Grained [8]have proposed that attribute's store and access control can be improved by using key-policy attribute based encryption algorithm. It provides highly efficient and secure data privacy aspects confidentiality of the client accesses control can also be improved.

J. Li, W. Yao, Y. Zhang, and H. Qian,[9] have proposed that to set up a system on the basis of encryption, key generation algorithms. A semi anonymous privilege control scheme annoy control to address not only the data privacy, but also the user identity privacy in current access control schemes .A semi anonymous data is too applied in order to attain its goal. Does not support user revocation schema for data sharing and accessing conditions

H.Tian,Y.Chen,C-C.Chang,H.Jiang,Y.Huang,H,Y.Chen,and J.Liu, [10] have proposed that public Auditing based on hash table which provides the migration of authorized data accessing techniques. It ensure low communicational cost and computational costs. It's one of the parametric term is by using index data information.

3.PROPOSED SYSTEM

A. Overview

Cloud gives clients a virtual computing infrastructure on which they can store data and run applications. Due to the popularity of cloud, we need security schemes and algorithms to maintain its access. Cloud security is a sub-domain of computer security, network security and also information security. One of the security concerns of cloud is that the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected. Some advanced encryption algorithms applied into cloud increases the security. The three levels of security offered in this system are: 1) CP-ABE (Ciphertext-Policy Attribute -Based Encryption) along with RSA based encryption, 2)attribute based and 3)time based access control policies. The existing system consists of cloud and its basic encryption. The data stored in cloud is always in an encrypted form. This form will protect sensitive data without delaying information exchange

B. Ciphertext-Policy Attribute-Based Encryption

CP-ABE is a type of attribute-based encryption scheme which is used in this system. It uses access trees to encrypt data and users' secret keys are generated over a set of attributes used, like continent and gender. In the CP-ABE, the encryptor controls access strategy. CP-ABE is mainly focused on the design of the access structure.

Attribute based encryption is a type of public-key encryption in which the secret key of a user and the ciphertext are dependent upon attributes. In this system, security is improved using attribute-based encryption. In such a system, the decryption of a ciphertext is possible only if the set of attributes of the user key matches the attributes of the ciphertext.

C. System Model

The cloud enables us to login anywhere with internet access to retrieve or share files and images based on the attributes such as location and gender. For attribute location, continent is preferred. If country list is taken, it will be difficult because there are almost 195 countries in the world. So for simplicity, continental concept is taken. Another attribute is based on gender (male/female). This is because all can access this platform and all has these attributes in common(fig 1). So encryption can be done on its basis. The file and images shared in the cloud should be in the encrypted form. For this an encryption tool based on RSA along with CP-ABE is introduced. This will apply passwords and encryption to files and images, so that they are encrypted before uploading into cloud.

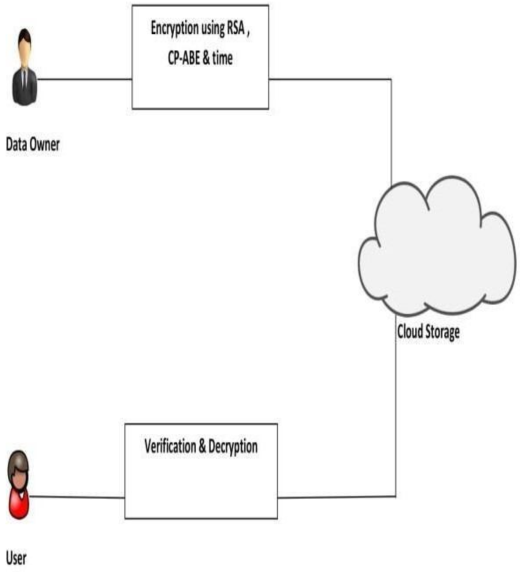
Encryption using RSA , CP-ABE & time
Data Owner
Cloud Storage
Verification & Decryption
User

Figure 1: Basic Process

D. RSA based Encryption

RSA algorithm is used to improve security and is named after Ron Rivest, Shamir, and Leonard Adleman. It is an algorithm for public-key cryptography. It involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. But ABE (Attribute-Based Encryption) systems mainly suffer from two drawbacks: non-efficiency and non-existence of attribute revocation mechanisms. Revocation is even more challenging in ABE systems, given that each attribute possibly belongs to multiple different users, whereas in traditional PKI systems public/private key pairs are uniquely associated with a single user. To incorporate the revocation feature, a simple but constrained solution is to include a time attribute. The user is given a specific time to access the files in the cloud.

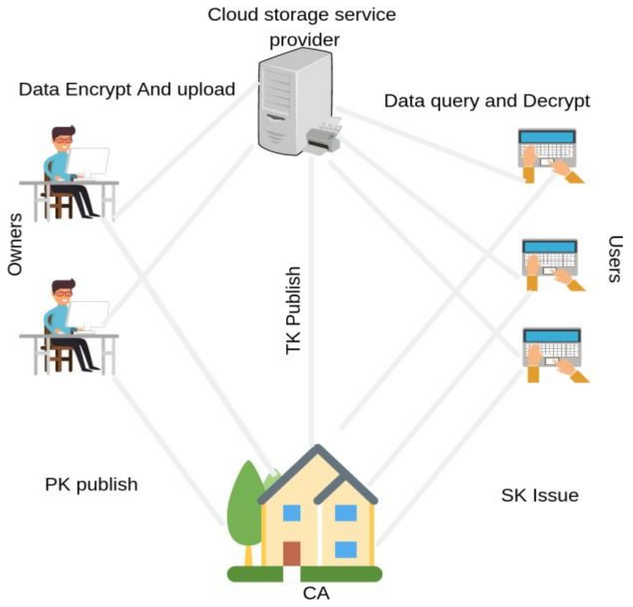

Figure 2: System Architecture

E. Construction

The proposed system uses CP-ABE and RSA algorithm to generate encryption when user upload the text files or images in the cloud storage and inverse of these algorithms to generate decryption when user download files or images from cloud storage. All are allowed to share the text files and images in the cloud(fig 2). Only those users having matching key, attributes and allowed time can access the shared data. The text can be anything like doc, program etc. which is written in common notepad. Thus the system is proposed to maintain security and provides privacy. It is highly efficient and satisfies the security requirements for time-sensitive data storage in public cloud.

4.RESULT

The security properties of attribute and time based factors are analyzed. The system provides users the capacity to define access policies according to specified attributes and time. A user can decrypt the ciphertext to access the data only if his/her attribute set and time factors satisfy the conditions. Therefore, based on the performance analysis of CP-ABE along with RSA algorithm, we can conclude that the system can provide flexible and fine-grained access control for time-sensitive data in public cloud.

5.CONCLUSION

This paper mainly focuses on secure storage of data in public cloud. It provides facility for fine-grained access control of time-sensitive data. To achieve this by integrating CP-ABE and RSA algorithm mechanism. Based on this scheme the data owners can decide the user able to access data and provide relevant access privilege releasing time points according to the well defined access policy over attribute and releasing time. And also it provides a lightweight overhead on both central authority and data owners. A rigorous security proof that is given to validate the proposed scheme is secure and effective. This mechanism is highly applicable for large scale access control system for cloud storage.

REFERENCES

[1]. Jianan Hong, Kaiping Xue, Ying jie Xue, Weikeng Chen, David S.L. Wei, Nenghai Yu and Peilin Hong," TAFC: Time and Attribute Factors Combined Access Control for Time-Sensitive Data in Public Cloud",IEEE Transactions on Services Computing,2017.
https://doi.org/10.1109/TSC.2017.2682090

[2]. SKan Yang, Xiaohua Jia, Kui Ren, Bo Zhang "DACMACS: Effective data access control for multi-authority cloud storage systems," IEEE Transactions on Information Forensics and Security, vol. 8, no. 11, pp. 1790–1801, 2013.
https://doi.org/10.1109/TIFS.2013.2279531

[3].Dayananda RB, Prof. Dr. G.Manoj Someshwar"Time-based proxy re encryption scheme for secure data sharing in a cloud environment," Information Sciences, vol. 258, no. 3, pp. 355–370, 2014.
https://doi.org/10.1016/j.ins.2012.09.034

[4]. Elli Androulaki, Claudio Soriente, Luka Malisaand Srdjan Capkun "Enforcing location and time-based access control on cloud-stored data," in Proceedings of the 2014 IEEE 34th International Distributed Computing Systems (ICDCS '14), pp. 637–648, IEEE, 2014.
https://doi.org/10.1109/ICDCS.2014.71

[5]. C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward secure and dependable storage services in cloud computing," IEEE Transactions on Services Computing, vol. 5, no. 2, pp. 220–232, 2012.
https://doi.org/10.1109/TSC.2011.24

[6]. Q. Liu, C. C. Tan, J. Wu, and G. Wang, "Reliable re-encryption in unreliable clouds," in Proceedings of the 2011 IEEE Global Communications Conference (GLOBECOM '11), pp. 1–5, IEEE, 2011.
https://doi.org/10.1109/GLOCOM.2011.6133609

[7]. Yan Zhu, Hongxin Hu, Gail-Joon Ahn, Dijiang Huang, and ShanbiaoWanging, "Towards temporal access control in cloud computing," in Proceedings of the 31st IEEE International Conference on Computer Communications (INFOCOM '12),pp. 2576–2580, IEEE, 2012.
https://doi.org/10.1109/INFCOM.2012.6195656

[8]. Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou"Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proceedings of the 29th IEEE International Conference on Computer Communications (INFOCOM '10), pp. 1–9, IEEE, 2010.

[9] . J. Li, W. Yao, Y. Zhang, and H. Qian, "Flexible and fine grained attribute-based data storage in cloud computing," IEEE Transactions on Services Computing, Available online, 2016.

[10].H.Tian,Y.Chen,CC.Chang,H.Jiang,Y.Huang,Y.Chen,and J.Liu, "Dynamic-hash-table based public auditing for secure cloud storage," IEEE Transactions on Services Computing, Available online, 2016.
https://doi.org/10.1109/TSC.2015.2512589