SJIF Impact Factor: 6.260| ISI I.F.Value:1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 5 | Issue: 1 | January 2020 - Peer Reviewed Journal

CRYPTOSYSTEM BASED QUOTIENT FILTER FOR SECURED DATA ACCESS ON CLOUD STORAGE

P. Jayasree[1]
[1]Research Scholar & Assistant Professor, Department of Computer Applications, Hindusthan College of Arts and Science, Coimbatore.

Dr. V. Saravanan[2]
[2]HEAD & Professor, Department of Information Technology, Hindusthan College of Arts and Science, Coimbatore.

ABSTRACT
Cloud data storage allows users to store huge amount of data on demand in a cost-effective manner. To preserve the confidentiality of data stored in the cloud, many cryptography techniques have been developed. But, the authentication performance of existing techniques was not enough. In addition to that, the amount of memory space needed to securely store data in the cloud was more. In order to overcome such limitations, Cryptosystem Based Quotient Filter Model is proposed. The model is designed for secured data access on cloud storage with higher data confidentiality and lower space complexity. Initially, the user registers his/her detail to a cloud server (CS). After registering, the cloud server generates the endorsement public key and private key. Then, the cloud user encrypts data with their endorsement public key and sends it to the CS. During the data access, the cloud user sends the request message. After receiving the request, cloud server checks the endorsement public key of the user and allows only the authorized user to access cloud data. After verifying the endorsement public key, the user decrypts the data with help of their endorsement private key. This helps to improve the data access security on cloud storage. The Model conducts an experimental evaluation using factors such as space complexity, data confidentiality rate and authentication accuracy with respect to a diverse number of user and cloud data.

KEYWORDS: *Cloud Data, Cloud Storage, Data Access, Endorsement Public Key.*

1. INTRODUCTION

Data access control is a significant process to achieve the data security in the cloud. Securing the data access from cloud storage is a difficult problem to be resolved because of data outsourcing in un-trusted cloud servers. Several techniques are designed in existing works with help of different cryptographic techniques to perform the secure data access control on cloud storage system. However, the authentication performance of conventional techniques was not sufficient which lacks the confidentiality level of data stored in the cloud. Also, the space complexity of existing techniques was higher. In order to solve these drawbacks, NPEAKC-WHQF Model is designed. The NPEAKC-WHQF Model is designed with aim of securing cloud storage and data access with lower space complexity.

An improved CP-ABE (cipher text-policy attribute-based encryption) scheme was intended in [1] to enhance the performance of access control for mobile users in the hybrid cloud system. The confidentiality level of data using this scheme was lower. A novel Data Access Control for Multi-Authority Cloud Storage (DAC-MACS) scheme called NEDAC-MACS scheme was presented in [2] to resist attacks in the cloud. Though the communication and computation overhead was reduced, authentication was not carried out using DAC-MACS scheme. Besides, the space complexity of this scheme was higher.

The trust model was introduced in [3] to enhance the security for stored data in cloud storage systems. The time needed for achieving secured cloud storage was higher. A fair data access control scheme was designed in [4] for cloud storage. But, the

SJIF Impact Factor: 6.260| ISI I.F.Value:1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 5 | Issue: 1 | January 2020 - Peer Reviewed Journal

authentication performance of this scheme was not effective.

An attribute-based encryption technique was presented in [5] to guard data from potential data loss and an illegal access to the stored data. However, the confidentiality rate of data was not at the required level. Multi-Authority Data Access Control was developed in [6] for enhancing the security of the cloud storage system. But, the memory space needed to securely store the data was very higher.

A similarity-aware message-locked encryption algorithm called EDedup was intended in [7] to minimize metadata storage overheads and to support flexible access control with revocation in the cloud. A KPABE System with Secret Attributes was used in [8] to verify users with diverse permissions to access files with less computational cost. However, the security level of cloud storage was not adequate.

A novel technique was presented in [9] to provide a solution for secure cloud storages from EDoS attacks and resource utilization. But, computation complexity was more. A review of different cryptographic mechanisms designed for data security and privacy preservation in cloud storage environments was analyzed in [10].

In order to resolve the above mentioned existing problem, This Model is developed. The contribution of Model is described in below,

- To achieve improved security for data access and data storage on the cloud as compared to state-of-the-art works.
- To improve the cloud data storage security with minimal space complexity as compared to existing techniques.The technique is proposed with help of endorsement key generation process and cryptosystem .
- To enhance the authentication performance of data access on cloud storage as compared to conventional techniques, endorsement key verification process is employed in the existing works.

The rest of paper is formulated as follows. In Section 2, related works are described.

2. RELATED WORKS

An eXclusive-OR (XOR) homomorphism encryption scheme was introduced in [11] for secure keyword searching on encrypted data. A secure data collaboration scheme was designed in [12] for access control of data stored in the cloud.

A privacy preserving keyword search was carried out in [13] with help of Curtmola's Searchable Symmetric encryption scheme. A CP-ABE access control scheme with hidden attributes was presented in [14] for improving the security of sensitive data set constraint.

A novel two-server authentication and key agreement protocol were introduced in [15] for accessing secure cloud services. A privacy-preserving data access control scheme depends on Ciphertext-Policy ABSC was introduced in [16] to attain a fine-grained control and attribute privacy protection simultaneously in a multi-authority cloud storage system.

Hierarchical attribute-set-based access control scheme was presented in [17] for flexible access control, privacy-preserving, efficient data utilization in the cloud. A task-oriented multilevel cooperative access control scheme was developed in [18] to get improved security isolations between tasks in the cloud.

An identity based secure authentication scheme was introduced in [19] with the application of quantum cryptography for authenticating the user in the cloud. A Rijndael Encryption Algorithm was intended in [20] for achieving cloud data security.

3. CRYPTOSYSTEM BASED QUOTIENT FILTER MODEL

The Cryptosystem Based Quotient Filter Model is developed to improve thesecurity of data storage and access in a cloud environment. This technique is designed in the Model by combining endorsement key generation process in a conventional Paillier cryptosystem. The designed technique is called non-deterministic cryptography as the encryption of the same plaintext under the same endorsement public key outputs a different ciphertext. Besides to that, Endorsement public key and the private key is used in order to increases the authentication performance of user when access the data stored on a cloud server.

In this Model comprises three main processes as below,

- Registration
- Data Encryption
- Data Decryption

3.1 Registration

The user's required to register their personal information's with cloud server for authentication purpose. The users in the cloud environment transmit their personal information's for example first name, last name, age, date of birth, e-mail Id, etc to the cloud server. After receiving user information's, cloud server stores it in the database and issue endorsement public key and private key for each user in a cloud computing environment. The endorsement public key is an encryption key which is shared between the sender and

SJIF Impact Factor: 6.260| ISI I.F.Value:1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 5 | Issue: 1 | January 2020 - Peer Reviewed Journal

the receiver. Besides, endorsement private key is a secret key which kept secret by the user. With supports of provided endorsement public key, To ensures the authenticity of each user who accesses the cloud data. The endorsement private key is employed to decrypt the ciphertext.

3.2 Data Encryption

Before storing the data on the cloud, encryption is carried out to attain the security and confidentiality rate. Few cryptography techniques were designed in existing works to perform secured cloud data storage. But, the security and confidentiality rate of conventional techniques were not sufficient.

The technique is developed by applying Endorsement key generation process in existing Paillier cryptosystem on the contrary to state-of-the-art works. The technique is an asymmetric algorithm for public key cryptography. The technique is also called as non-deterministic cryptography because the encryption of the same data under the same endorsement public key provides diverse ciphertext as output. The technique is a type of key pair-based cryptography as where each user gets an endorsement public and a private key, and data encrypted with their endorsement public key can only be decrypted with their endorsement private key.

3.3 Data Decryption

During the data access, the cloud user transmits the request message to the cloud server. After receiving the user request, cloud server authenticates the user is an authenticated or not with help of their endorsement public key. The endorsement public key used in this model on the contrary to state-of-the-art works as it helps for accurately verifying the cloud users with minimal time complexity. During the processes of user authentication, the user entered endorsement public key is matched with the keys of the corresponding user stored in cloud server database. If both endorsement public key is the same, model allows the user to carry out the Data Decryption. Otherwise, the data decryption process through that user is declined.

4. CONCLUSION

The goal of the model is to attaining higher security for data access on cloud storage. And also obtained with application of endorsement key generation. The generation of endorsement key pairs helps to improve the authentication performance of users who access cloud data as compared to existing works. With the support of processes this technique ,enhances the security of data on cloud storage when compared to conventional works. By using the endorsement key generation, permits only legitimate users to get the data stored on the cloud. This assists to increases the confidentiality of data on cloud storage as compared to existing works. The performance of the Model is estimated in terms of space complexity, authentication accuracy, and data confidentiality rate and compared with two state-of-the-art works.

REFERENCES

1. *Wen-Min Li, Xue-Lei Li, Qiao-Yan Wen, Shuo Zhang, Hua Zhang, "Flexible CP-ABE Based Access Control on Encrypted Data for Mobile Users in Hybrid Cloud System", Journal of Computer Science and Technology, Springer, Volume 32, Issue 5, Pages 974–990, September 2017*
2. *Xiang long Wu, Rui Jiang, and Bharat Bhargava, "On the Security of Data Access Control for Multi-authority Cloud Storage Systems", IEEE Transactions on Services Computing, Volume 10, Issue 2, Pages 258 – 272, March-April 2017*
3. *Lan Zhou, Vijay Varadharajan, Michael Hitchens, "Trust Enhanced Cryptographic Role-Based Access Control for Secure Cloud Data Storage", IEEE Transactions on Information Forensics and Security, Volume 10, Issue 11, 2015*
4. *Hai Liu, Xinghua Li, Mengfan Xu, Ruo Mo, Jianfeng Ma, "A fair data access control towards rational users in cloud storage", Information Sciences, Elsevier, Volumes 418–419, Pages 258-271, December 2017*
5. *Jongkil Kim, Surya Nepal, "A Cryptographically Enforced Access Control with a Flexible User Revocation on Untrusted Cloud Storage", Data Science and Engineering, Springer, Volume 1, Issue 3, Pages 149–160, September 2016*
6. *Jianan Hong, Kaiping Xue, Wei Li, "DAC-MACS: Effective Data Access Control for Multiauthority Cloud Storage Systems"/Security Analysis of Attribute Revocation in Multiauthority Data Access Control for Cloud Storage Systems", IEEE Transactions on Information Forensics and Security, Volume 10, Issue 6, Pages 1315 – 1317, June 2015*
7. *Yukun Zhou, Dan Feng, Yu Hu, Wen Xi, Min Fu, Fangting Huang, Yucheng Zhang, "A similarity-aware encrypted deduplication scheme with flexible access control in the cloud", Future Generation Computer Systems, Elsevier, Volume 84, Pages 177-189, July 2018*
8. *Eissa Tameem, Gihwan Cho, "Providing Privacy and Access Control in Cloud Storage Services Using a KPABE System with Secret Attributes", Arabian Journal for Science and Engineering, Volume 39, Issue 11, Pages 7877–7884, November 2014*

SJIF Impact Factor: 6.260| ISI I.F.Value:1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)
Volume: 5 | Issue: 1 | January 2020 - Peer Reviewed Journal

9. *Kaiping Xue, Weikeng Chen, Wei Li,Jianan Hong, Peilin Hong, "Combining Data Owner-Side and Cloud-Side Access Control for Encrypted Cloud Storage", IEEE Transactions on Information Forensics and Security, Volume 13, Issue 8, Pages 2062 – 2074, 2018*
10. *Nesrine Kaaniche, Maryline Laurent, "Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms", Computer Communications, Elsevier, Volume 111, Pages 120-141, October 2017*
11. *Shu Qin Ren, Benjamin Hong Meng Tan, Sivaraman Sundaram, Taining Wang, Yibin Ng, Chang Victor, and Khin Mi Mi Aung, "Secure Searching on Cloud Storage Enhanced by Homomorphic Indexing", Future Generation Computer Systems, Elsevier, Volume 65, Pages 102-110, December 2016*
12. *Qinlong Huang, Yixian Yang and Mansuo Shen, "Secure and efficient data collaboration with hierarchical attribute-based encryption in cloud computing", Future Generation Computer Systems, Elsevier, Volume 72, Pages 239-249, July 2017*
13. *Md Iftekhar Salam, Wei‐Chuen Yau, Ji‐Jian Chin, Swee‐Huay Heng, Huo‐Chong Ling, Raphael C‐W Phan, Geong Sen Poh, Syh‐Yuan Tan and Wun‐She Yap, "Implementation of searchable symmetric encryption for privacy-preserving keyword search on cloud storage", Human-centric Computing and Information Sciences, Springer, Volume 5, Issue 19, Pages 1-16, December 2015*
14. *Nurmamat Helil, and Kaysar Rahman, "CP-ABE Access Control Scheme for Sensitive Data Set Constraint with Hidden Access Policy and Constraint Policy", Hindawi, Security and Communication Networks, Volume 2017, Article ID 2713595, Pages 1-13, 2017*
15. *Durbadal Chattaraj, Monalisa Sarma, Ashok Kumar Das, "A new two-server authentication and key agreement protocol for accessing secure cloud services", Computer Networks, Elsevier, Volume 131, Pages 144-164, February 2018*
16. *Qian Xu, Chengxiang Tan, Zhijie Fan, Wenye Zhu, Ya Xiao, Fujia Cheng, "Secure Multi-Authority Data Access Control Scheme in Cloud Storage System Based on Attribute-Based Signcryption", IEEE Access, Volume 6, Pages 34051 – 34074, 2018*
17. *Rohit Ahuja, Sraban Kumar, Mohanty, Kouichi Sakurai, "A scalable attribute-set-based access control with both sharing and full-fledged delegation of access privileges in cloud computing", Computers & Electrical Engineering, Elsevier, Volume 57, Pages 241-256, January 2017*
18. *Jian Dong, Hui Zhu,Chao Song, Qiang Li, and Rui Xiao, "Task-Oriented Multilevel Cooperative Access Control Scheme for Environment with Virtualization and IoT", Hindawi, Wireless Communications and Mobile Computing, Volume 2018, Article ID 5938152, Pages 1-11, 2018*
19. *Geeta Sharma and Sheetal Kalra, "Identity-based secure authentication scheme based on quantum key distribution for cloud computing", Peer-to-Peer Networking and Applications, Springer, Pages 1–15, November 2016*
20. *Sanjoli Singla and Jasmeet Singh, "Cloud Data Security using Authentication and Encryption Technique", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 2, Issue 7, Pages 2232- 2235, 2013*