IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, October 2022
Impact Factor: 6.252

A Data Sharing Protocol to Increase Security and Privacy of Cloud Storage in Big Data Era

Mr. Manas Mandlecha, Mr. Manish Bisoi, Miss. Shraddha Sasturkar, Mr. Shubham Rajput
Department of Computer Engineering,
All India Shri Shivaji Memorial Society's Institute of Information Technology, Pune, Maharashtra, India

Abstract: *Data integrity maintenance is the major objective in big data era. This work implements protecting the data and regeneration of data if someone mishandles it. This job will be assigned to a Proxy server. The data of the users will be stored in public and private area of the cloud. So that only public cloud data will be accessed by user and private cloud will remain more secured. Cloud storage generally provides different redundancy configuration to users in order to maintain the desired balance between performance and fault tolerance. Data availability is critical in distributed storage systems, especially when node failures are prevalent in real life. This research work explores secure data storage and sharing using proposed AES 256 encryption algorithm and Role Base Access Control (RBAC) for secure data access scheme for end user. This work also carried out backup server approach it works like proxy storage server for ad hoc data recovery for all distributed data servers.*

Keywords: Data Sharing

I. INTRODUCTION

Now a day's cloud storage is used to store and retrieve data that is based on the internet, instead of local storage devices for more reliable, secure, and availability of data. But data is very important and should not be revealed to any unauthorized person, for this purpose encryption method is used to convert this plain data into cipher text and a decryption method is used to convert that cipher text into plain text to get back the original data. So, the encryption algorithm plays the most important role to make data more secure. This research work explores secure data storage and sharing using the proposed AES 256-bit encryption algorithm and SHA-256 algorithm for Role Base Access Control (RBAC) for a secure data access scheme for the end-user. This work also carried out a backup server approach it works like a proxy storage server for ad hoc data recovery for all distributed data blocks.

The system depicts the principle plan objectives of the proposed plan including key circulation, information secrecy, access control, and effectiveness as takes after: Key Distribution: The prerequisite of key transportation is that clients can competently get their personal / private keys from the gathering director without a Certificate Authorities. In other existing plans, this purpose is skilful by expecting that the communication channel is secure, on the other hand, in our plan, the system can accomplish it without this solid thought. Access control: first, gather individuals can employ the cloud asset for records stockpiling and data sharing. Second, unapproved clients can't get to the cloud asset each time, and disavowed clients can be unfitted for utilizing the cloud asset again as soon as they are renounced.

LITERATURE SURVEY

[1]. Islam, M.S.; Humaira, F.; Nur, F.N. "Control Cloud Data Access Privilege and Anonymity with Fully Anonymous Attribute-Based Encryption", IEEE transactions on information forensics and security, VOL. 10. 2020,

[2]. Shewale, A.D.; Sankpal, S.V. IOT Raspberry Pi based Smart and Secure Health Care System using BSN. Int. J. Res. Appl. Sci. Eng. Technol. 2020,

[3]. Selvaraj, S.; Sundaravaradhan, S. Challenges and opportunities in IoT healthcare systems: A systematic review. SN Appl. Sci. 2020.

[4]. Kan Yang and Xiao huaJia, "Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage", IEEE Transactions on parallel and distributed systems, VOL. 25, NO. 07, July 2020.

[5]. S. Kamara and K. Lauter, "Cryptographic cloud storage," in Proceedings of the 14th Financial Cryptography

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, October 2022
Impact Factor: 6.252

and Data Security. Springer, 2020, pp. 136-149.

[6]. Kaur, H.; Atif, M.; Chauhan, R. An Internet of Healthcare Thing (IoHT) based Healthcare Monitoring System. In Advances in Intelligent Computing and Communication, Lecture Notes in Networks and Systems; Mohanty, M.N., Das, S.,Eds.; Springer Nature: Singapore, 2020.

[7]. B. Wang, B. Li, and H. Li, "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud," IEEE Transactions on Services Computing,vol. 8, no. 1,pp. 92-106, 2018.

[8]. Deelip, S.A.; Sankpal, S.V. IOT based Smart and Secure Health Care System Analysis Data Comparison. Int. J. Res. Appl. Sci. Eng. Technol. 2020

[9]. Sanjay, S.; Shekokar, N. Toward Smart and Secure IoT Based Healthcare System. In Internet of Things, Smart Computing and Technology: A Roadmap 19 A Data Sharing Protocol to Increase Security and Privacy of Cloud Storage in Big Data Era Ahead, Studies in Systems, Decision and Control; Dey, N., Mahalle, P.N., Shafi, P.M., Kimabahune, V.V., Hassanien, A.E., Eds.; Springer Nature AG: Cham, Switzerland, 2020.

[10]. Farahani, B.; Firouzi, F.; Charkabarty, K. Healthcare IoT. In Intelligent Internet of Thing, From Device to Fog and Cloud; Firouzi, F., Chakrabarty, K., Nassif, S., Eds.; Springer Nature AG: Cham, Switzerland, 2020.

[11]. Jianan Hong, Kaiping Xue and Wei Li, "Comments on "DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems"/Security Analysis of Attribute Revocation in Multi- Authority Data Access Control for Cloud Storage Systems", IEEE transactions on information forensics and security, VOL. 10, NO. 06, June 2018.

[12]. N. Attrapadung, B. Libert, and E. Pana eu, Expressive key policy attribute based encryption with constant-size cipher texts, in Proceedings of the 14th International Conference on Practice and Theory in Public Key Cryptography.Springer, 2018, pp. 90-108.

[13]. T. Jung, X. Li, Z. Wan, and M. Wan, "Privacy preserving cloud data access with multi-authorities," in Proceedings of The 32nd IEEE International Conference on Computer Communications. IEEE, 2018, pp. 2625-2633.

[14]. Wei Li, Kaiping Xue, Yingjie Xue, and Jianan Hong, "TMACS: A Robust and Verifiable Threshold Multi-Authority Access Control System in Public Cloud Storage", IEEE Transactions on parallel and distributed systems, VOL.24, NO.

[15]. 06, October 2018.

[16]. Tuli, S.; Basumatary, N.; Singh-Gill, S.; Kahani, M.; Chand-Arya, R.; Wander, G.; Buyya, R. HealthFog: An ensemble deep learning in cloud including its security. Future Gener. Comput. Syst. 2020

III. PROBLEM STATEMENT

In the proposed research work to design and implement a system which will provide the data security. The system will focus on securing and sharing the file between data owner and specific user. The TPA will make sure that the file shared is sent to the authorised user and will assign the KEY accordingly.

3.1 Related Works

Many solutions have been proposed to solve the privacy risks of cloud-based storage. Rao proposed a secure sharing schemes of personal health records in cloud computing based on cipher text policy attributed-based(CP-ABE) signcryption. It focuses on restricting unauthorized users on access to the confidential data.

Liu *et al.* proposed an access control policy based on CP-ABE for personal records in cloud computing as well. In and, only one fully trusted central authority in the system is responsible for key management and key generation.

Huang *et al.* introduced a novel public key encryption with authorized equality warrants on all of its cipher text or a specified cipher text. To strengthen the securing requirement, Wu *et al.* proposed an efficient and secure identity-based encryption scheme with equality test in cloud computing.

Xu *et al.* proposed a CP-ABE using bilinear pairing to provide users with searching capability on cipher text and fine grained access control.

He *et al.* proposed a scheme named ACPC aimed at providing secure, efficient and fine grained data access control in P2P storage cloud.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, October 2022
Impact Factor: 6.252

Xue *et al.* proposed a new framework, named RAAC, to eliminate the single-point performance bottleneck of the exiting CP-ABE based access control schemes for public cloud storage. While these schemes use identity privacy by using attribute-based techniques which fail to protect user attribute privacy.

IV. THE PROPOSED PROTOCOL

In this section we describe more about the proposed protocol model and algorithm.

4.1 Protocol Model

A. Data Sharing Model

Consider a cloud storage data sharing system with multiple entities and the data sharing model as shown in Fig 1. The protocol model consists of three types of entities: cloud provider, data owner and group members. The cloud provider: provides a public platform for data owners to store and share their encrypted data. The cloud provider doesn't conduct data access control for owners. The encrypted data can be download freely by any users.

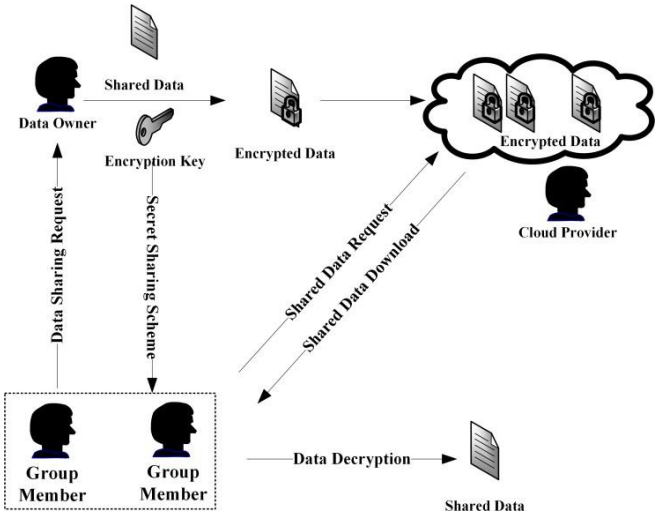

Figure 1: Protocol Model

Data owner: defines the access policy and encrypts its data with a symmetric encryption algorithm using a group key. The group members who satisfied the access policy constitute a sharing group. Then secret sharing scheme is used by the owner to distribute the encryption key to the sharing group.

Group members: every group member including the data owner is assigned with an unique and a pair of keys. The group members can freely get any interested encrypted data from the public cloud. However, the user can decrypt the data if and only if it gets the data decryption key from the data owner.

B. Security Model

We have the following assumptions:

The data owner is totally trusted and will never be corrupted by any adversaries. Cloud provider is semi-trusted, it correctly executes the task assigned to them for profits, but they would try to find out as much secret information as possible based on the data owners uploaded data. We now describe the security model by listing possible attacks. The group key is distributed by running the secret sharing scheme. Parts of the group members can gather their sub secret shares to reconstruct the group key.

C. Definitions and Notations

Definition 1 ((t ,n)VSS): A verified secret sharing scheme contains four steps:

Sharing Generation Algorithm: An algorithm that, on input a security parameter K and a random polynomial $f(x)$ of degree t - 1, output n sub-shares and a verified value v; Distribution: The dealer distributes each sub-share and v to every scheme participant secretly;

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, October 2022
Impact Factor: 6.252

Verify: A verification algorithm that, on input a sub-share and *v*, output whether the sub-share is tempered during distribution;

Secret Reconstructed: For any *t* sub-shares, the security parameter *K* can be reconstructed.

Definition 2 (Equity and Availability): Verified secret sharing scheme guaranteeing equity and availability with two conditions: Any participant set in the share group, where the size of the set is less than the total quantity, the participants in the set cannot get any information about *K*; Only with cooperation of all the legitimate participants, *K* could be reconstructed.

Definition 3 (Confidentiality): Verified secret sharing scheme guarantees confidentiality if any users outside the sharing group cannot get any information of *K* even with the knowledge of enough interactive messages.

Definition 4 (Integrity): Once the interactive messages are tempered during VSS, any information about *K* could be gotten by participants. We said that verified secret sharing scheme guarantees integrity. The notations are used throughout the remainder of this paper.

D. Protocol Details

The scene describes as a protocol participant *O* wishes to share data *D* with the legitimate participants *Pi*; *i* D 1; 2; : : : ; *n*. Firstly, *O* generates a secret key *K* and uses *K* to encrypt *D*, then *O* stores the encrypted data *cipher*(*D*) to the cloud. Secondly, *O* shares *K* with the legitimate participants and all participants work together to certify and reconstruct *K*. Finally, every participant gets *K* and download *cipher*(*D*) from the cloud.

4.2 Data Sharing

The data owner *O* creates the secret key and encrypts the data using symmetric encryption algorithm AES. Then secret sharing scheme is used by *O* to distribute the secret key. As the public channel is available for communications between every pair of participants, an asymmetric encryption algorithm RSA is used to protect the key sub-shares from known by unauthorized users. The distribution protocol is summarized as followed steps.

Step 1: When the Owner O shares file with a specific user U, a key is generated

Step 2: The key is secure with TPA and TPA also gets the information about the data that's been transferred/ shared.

Step 3: The User U, sends request for key to the TPA.

Step 4: TPA crosschecks the information and verifies it and shares the key with the user U only when every detail is correct.

Step 5: The user U, then uses the key to gain access to the file and downloads it.

4.3 System Architecture

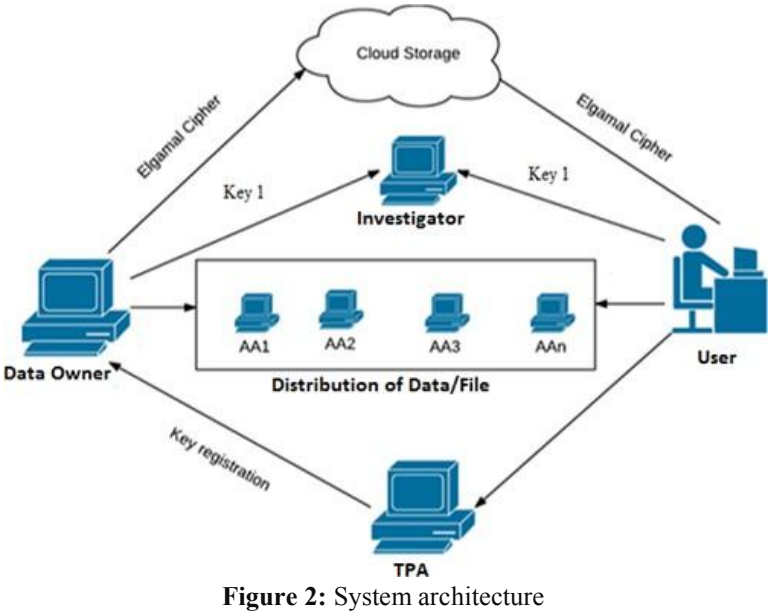

Figure 2: System architecture

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, October 2022
Impact Factor: 6.252

V. CONCLUSION

In this paper we propose a model/ platform for an organisation to share data on a very secure network. We use TPA in this model to provide extra security as it gets the information about the file shared and also can cross verify if it's been accessed by authorised user.

If any kind of corruption takes place during entering the key during decryption the file gets locked and new key is generated immediately. Also the TPA and investigator are informed about it. So basically this model will provide highest security while sharing data. And avoid all kinds of corruptions. It will also help the owner to store his/ her data on the cloud which he can access anytime.

REFERENCES

[1]. Islam, M.S.; Humaira, F.; Nur, F.N. "Control Cloud Data Access Privilege and Anonymity with Fully Anonymous Attribute-Based Encryption", IEEE transactions on information forensics and security, VOL. 10. 2020,

[2]. Shewale, A.D.; Sankpal, S.V. IOT Raspberry Pi based Smart and Secure Health Care System using BSN. Int. J. Res. Appl. Sci. Eng. Technol. 2020,

[3]. Selvaraj, S.; Sundaravaradhan, S. Challenges and opportunities in IoT healthcare systems: A systematic review. SN Appl. Sci. 2020.

[4]. Kan Yang and Xiao huaJia, "Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage", IEEE Transactions on parallel and distributed systems, VOL. 25, NO. 07, July 2020.

[5]. S. Kamara and K. Lauter, "Cryptographic cloud storage," in Proceedings of the 14th Financial Cryptography and Data Security. Springer, 2020, pp. 136-149.

[6]. Kaur, H.; Atif, M.; Chauhan, R. An Internet of Healthcare Thing (IoHT) based Healthcare Monitoring System. In Advances in Intelligent Computing and Communication, Lecture Notes in Networks and Systems; Mohanty, M.N., Das, S.,Eds.; Springer Nature: Singapore, 2020.

[7]. B. Wang, B. Li, and H. Li, "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud," IEEE Transactions on Services Computing,vol. 8, no. 1,pp. 92-106, 2018.

[8]. Deelip, S.A.; Sankpal, S.V. IOT based Smart and Secure Health Care System Analysis Data Comparison. Int. J. Res. Appl. Sci. Eng. Technol. 2020

[9]. Sanjay, S.; Shekokar, N. Toward Smart and Secure IoT Based Healthcare System. In Internet of Things, Smart Computing and Technology: A Roadmap 19 A Data Sharing Protocol to Increase Security and Privacy of Cloud Storage in Big Data Era Ahead, Studies in Systems, Decision and Control; Dey, N., Mahalle, P.N., Shafi, P.M., Kimabahune, V.V., Hassanien, A.E., Eds.; Springer Nature AG: Cham, Switzerland, 2020.

[10]. Farahani, B.; Firouzi, F.; Charkabarty, K. Healthcare IoT. In Intelligent Internet of Thing, From Device to Fog and Cloud; Firouzi, F., Chakrabarty, K., Nassif, S., Eds.; Springer Nature AG: Cham, Switzerland, 2020.

[11]. Jianan Hong, Kaiping Xue and Wei Li, "Comments on "DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems"/Security Analysis of Attribute Revocation in Multi- Authority Data Access Control for Cloud Storage Systems", IEEE transactions on information forensics and security, VOL. 10, NO. 06, June 2018.

[12]. N. Attrapadung, B. Libert, and E. Pana eu, Expressive key policy attribute based encryption with constant-size cipher texts, in Proceedings of the 14th International Conference on Practice and Theory in Public Key Cryptography. Springer, 2018, pp. 90-108.

[13]. T. Jung, X. Li, Z. Wan, and M. Wan, "Privacy preserving cloud data access with multi-authorities," in Proceedings of The 32nd IEEE International Conference on Computer Communications. IEEE, 2018, pp. 2625-2633.

[14]. Wei Li, Kaiping Xue, Yingjie Xue, and Jianan Hong, "TMACS: A Robust and Verifiable Threshold Multi-Authority Access Control System in Public Cloud Storage", IEEE Transactions on parallel and distributed systems, VOL.24, NO. 06, October 2018.

[15]. Tuli, S.; Basumatary, N.; Singh-Gill, S.; Kahani, M.; Chand-Arya, R.; Wander, G.; Buyya, R. HealthFog: An ensemble deep learning in cloud including its security. Future Gener. Comput. Syst. 2020