Secure File Sharing System in Cloud Using AES and Time Stamping Algorithms

R.Sheeba\textsuperscript{1}, Chidambaranathan Bibin\textsuperscript{2}, Priya R Krishnan\textsuperscript{3}, R.Nishanth\textsuperscript{3}, S.Gopinath\textsuperscript{3} and K.G.Ashok\textsuperscript{4}
\textsuperscript{1}Saveetha School of Engineering, Thandalam, Chennai, Tamil Nadu.
\textsuperscript{2}RMK College of Engineering and Technology, Chennai, Tamil Nadu.
\textsuperscript{3}Cochin University College of Engineering Kuttanad, Kerala.
\textsuperscript{4}Easwari Engineering College, Chennai, Tamil Nadu.
Email: cjabbn@gmail.com

Abstract. In recent days, the growth of digital data has been increased explosively due to data-intensive applications like healthcare, education and electronic commerce. Due to the huge volume of data created and the utilization of data in emerging applications, a local storage device has to be deployed. Cloud storage services allow both the individuals and commercial users for the outsourcing of data to the cloud server and to access the data remotely with the help of the internet, so the demand for cloud storage has been raised. However, one of the critical problems of cloud data storage is security. Some researchers have used third party auditor for verifying the data stored in the cloud. This paper introduces a novel method for cloud storage and for protecting the organizations' data. The proposed system strengthens the level of authentication with the help of AES and time-stamping algorithms. The experimental results demonstrate the efficiency of the proposed method when auditing the shared data integrity.

Keywords: Cloud computing, AES, Timestamping, KDM, Data owner

1. Introduction

One of the first features of distributed computing is the utilization of the cloud \cite{1}. Additionally, the cloud offers limitless storage for the customer to store their information.
The distributed storage gives the most effective approach to remote information reinforcement, with the goal that client can able to recover the data whenever utilizing the cloud administrations. Cloud likewise lessens the money related over-burden of ventures and associations keep up their information. There are more contextual investigations that are identified with distributed storage for remote information reinforcement [2]. Additionally, people can store their individual information to the cloud utilizing Dropbox and Google Drive and then forth [3, 4]. Nowadays progressively the number of individuals groups is utilizing apparatus like Dropbox to store their information in the cloud. Nonetheless, we've to think about the safety worries in putting away the fragile information in the cloud which is maintained by third-party cloud administrations. In our defined work, two of the main security issues are considered especially. Within the first place, we've to ensure that just approved gatherings have access to the re-appropriated information in cloud through proficient key dissemination component and access strategy. Second, to confirm secure information we've to execute cryptography plans for giving security when clients transfer or download information from cloud administrations. In this paper, we utilized RSA and AES calculation for accomplishing the proposed issues and some cryptographic key activities to shield the data which is obtained from the cloud Wang et al. in [5]. Consider the dynamic storage of data in a distributed scenario. They proposed a protocol that would be capable of determining the accuracy of the data.

A few investigations [6] are identified with the insurance of re-appropriated information utilizing cryptographic strategies. S.Pawar al.[7] proposed an examining framework that empowers the clients to confirm the respectability of redistributed information. Pawar et al. [8] thought of a safe redistributed information get to the system with access rights. W.Huang [9] talked about the uprightness and security on a redistributed information utilizing hash-based component. The key offers are put away in the Hash Table in an appropriated way. RSA is the most well-known open key calculation. Rivest, Shamir and Adleman [10] imagined this calculation where both open and private key is utilized for encryption and unscrambling. All the messages are scrambled utilizing the general population key and it is sent to the beneficiary. The recipient utilizes the private key to unscramble the message. B.chor et.al [12] proposed a technique to anchor information in the cloud utilizing RSA. Cramer and JB Nielsen [11] designed AES a symmetric calculation. AES utilizes a similar key for both encryption and of messages. Sheren A. El-Booz, Gamal Attiya and Nawal El-Fishawy proposed a secure cloud storage system combining time-based one-time password and automatic blocker protocol [13].
2. Proposed work

Here the first user should register with all personal details they need to fill while registering time that individual user should select one particular group because here, we are going to divide into four groups the user should select one particular group. After selecting that, the details are stored in the database. After storing that the details of each of them are sent to admin then if admin accepts then only that individual user can log in. After accepting the user request then the user can log in and can upload the file. While uploading that file the private key will be generated for that file. Like that, if any user comes to registration after login that user can view that files in user inbox if the user needs that file they need to send an invitation to admin if that user is expounded to the identical group of that file then only that request will allow passing admin. Then if the second-hand needs the file, they send a letter of invitation to admin. In admin box admin can view what are the files available they will view and people who send request they will be viewed in the admin page. If admin accepts the request then that user can get that file with the private key while sending that file admin will allocate 30 mins time if that user wants that file within 30 means they need to enter that non-public key to induce individual file that point should be taken from our current desktop timings.

2.1 The Cloud

Data redistributing and Data reinforcement are completed in the cloud by the knowledge proprietor. To shield the knowledge from the unapproved client, information is put away in an exceeding sort of encryption in the cloud. Classification is accomplished by putting away the knowledge in an exceedingly scrambled frame. The cryptographic activity and the transfer and download document activity are finished utilizing our proposed strategy. So, there's not much association of cloud explicit activity in our work.

2.2 Key Distribution Manager

The Key Distribution Manager (KDM) acts as confided in outsider where all the cryptographic related activities are done here. ACL is additionally maintained in KDM for the arrangement of individual records. At whatever point the client must transfer or download the document in the cloud, first, the client must enlist with KDM and KDM confirms for validation. KDM will be maintained by the association itself to make a trust for the client who is getting to the information.
2.3 Data Owner

Data proprietor will transfer the scrambled information to the cloud with the help of KDM. Information Owner sends the Access Approach (AP_i) which is expounded with the document alongside the rundown of clients who can get to the present record to KDM. This arrangement of access approaches is maintained in ACL document which could be a piece of a KDM. All entrance approaches are related with each document and also the approved clients are permitted to urge to the documents.

![Figure 1. Proposed System Architecture](image)

2.4 User Registration

Information Owner and every other individual client must first enrol with KDM. KDM monitors rundown of the client and their Gathering ID (ID_i) which is given by the gathering individuals while enlistment. Amid the procedure of encryption and unscrambling, KDM confirms and verify the rundown of clients who wish to induce to its document.

2.5. Key Generation

The KDM is to blame of RSA key age of our strategy which has both Symmetric and Asymmetric calculations. In our proposed work, we use RSA calculation to form the key combination which is open and personal key.

1. Two prime number a and b chosen randomly.
2. Compute \( c = a \times b \)
3. Calculate the function $f(c)$ i.e.,
$$f(c) = (a-1) \times (b-1)$$

4. Variety $e$ is chosen randomly such the range as
$$1 < e < f(c)$$
and also $\text{GCD}(e, f(c)) = 1$.

5. With these parameters private key $(d)$ is generated using the equation
$$d = e^{-1} \mod f(c) \quad (1)$$

### 2.6 Encryption

Data Owner sends the document to KDM for encryption. Encryption is conveyed our utilizing the Symmetric calculation AES using below equation.

$$D_1 = \text{EAES}(\text{File, Rk}) \quad (2)$$

The KDM creates the irregular key $(R_k)$ of the length required for record encryption. Presently the document is an encoded frame. The knowledge is put away within the cloud by Data proprietor after receiving from KDM. After the procedure of record encryption, the AES key created is scrambled utilizing people normally key of RSA.

$$D_2 = \text{ERSA}(R_k, K_{Pu}) \quad (3)$$

### 2.7 Decryption

At the purpose when the gathering part must get to the record, either the client can download the scrambled document from the cloud or the demand will be made to KDM for recovering the scrambled document. The KDM sends the scrambled record and therefore the private key combine $(K_{Pr})$ to the information Owner. After confirming the legitimacy of the client, the KDM sends the Encrypted record to the gathering individuals. When the record is acquired by the client, at that time a requirement is sent to the data proprietor for AES key to unscramble the record. The information owner utilizes the private key $(K_{Pr})$ and $D_2$ esteem get from KDM to recover the AES key $(R_k)$ using the equation.

$$K_{AES} = \text{DRSA}(D_2, K_{Pr}) \quad (4)$$

As per the request provided by the user and also with relevance to user access policy, the generated AES key $(K_{AES})$ is shipped to the group of users. The group members after receiving the AES key will ready to decrypt the file using the equation (5)
2.8 Policy-Based Data Access

Each document and also the clients are related to single access arrangement. Amid the record transfer, the data proprietor sends the record alongside the arrangement related with the document and rundown of clients who can get to the document. Each client’s necessities to induce to the record is with the constant or distinctive arrangement because it is chosen by the data proprietor. The KDM validates the clients amid the record download activity. The arrangement can shift with diverse applications. Assume when some representatives are working in an association and each one engaged with the distinctive venture, we can relate a client-based strategy will be the documents for the client. At whatever point the representative leaves the association the KDM will create diverse RSA key match furthermore, will re-scramble the AES key utilizing the new open key. AES secrets likewise recovered before encryption by RSA open key if important. At that time KDM will send the new private key to the knowledge proprietor. The knowledge proprietor will send the recently created private key to the gathering individuals who approach strategy to urge thereto record. The individual from gathering who left won't have any entrance thereto information and also the arrangement related with the clients may be additionally erased from ACL which is a piece of KDM. The new client first registers with the KDM. While joining the client presents his personality for confirmation. At the purpose when the client has to join the present gathering, he sends a requirement to KDM by giving the group ID for confirmation. The new part has been sent by the knowledge proprietor, at that time KDM adds the part to the gathering which is referenced by gathering Id. Likewise, ACL refresh the new client data and therefore the strategy is expounded to the client with the record that has to be caught. At the purpose when the knowledge proprietor has to recharge with the new approach, sends a requirement to KDM to refresh the approach related to the record. The KDM refreshed the ACL list as indicated by the new approach and if necessary, it yet again recovers the new match of RSA open and a personal key. At the purpose when a client is expounded with various document and since each record is connected with a solitary arrangement, KDM will make utilization of the Boolean mixture of approaches for that client.

3. Performance Evaluation
This segment assesses the execution of our proposed framework. The proposed strategy is tested and actualized in java. For our investigation, we utilized Google App Motor as distributed storage. We utilized Google Cloud SQL as a database to store and recover information whenever and at anyplace. In our proposed work, we utilize both symmetric and kilter key for look after security Utilizing RSA key pair created, AES key is encoded. The testing has been done with various key lengths. Fig.2 and Fig.3 demonstrate that the time taken to create the private key and open key increments with admiration to the expansion in the key length. Our evaluation is based on the time taken to upload and download the file.

![Figure 2. Time taken for private key generation](image)

![Figure 3. Time taken for public key generation](image)
4. Future Enhancements

Based on our analysis, categorization of dynamical networks prevention mechanisms and we identify some possible directions. Future works embrace investigations of cybersecurity management for systems with state and input delays. In real applications, due to completely different environmental influences or enforced equipment's, it's conjointly vital and sensible to consider the heterogeneous case wherever A, B, C and performance D are completely different for the followers. Moreover, since input saturation nonlinearities are omnipresent in physical and engineering systems. It is necessary to explore the implications of input saturation in these Publications/privacy security.pdf systems in presence of cyber-attacks on their communication channels. Distributed intrusion detection and resilient distributed estimation are fascinating topics for complicated cyber-physical networks.

5. Conclusion

This paper dealt with the protection of privacy while maintaining public auditing. A new secure cloud storage system is proposed to ensure that the details of companies are secure from all data operator and third-party inspector, respectively by protected sharing of information utilizing RSA and AES calculation to keep up security inside the cloud server. KDM will be in charge of all key age and key appropriation process in our proposed plan. The execution is assessed what's more; the outcomes are acquired dependent on RSA key age and AES encryption process. From the outcome, it is seen that our proposed strategy will be pertinent for sharing information in the cloud safely. We use approaches-based access instrument to give security with the information in the cloud and to give validation. In future, we can utilize different KDM to deal with the information with various access strategies to maintain a strategic distance from insider attacks.

References

[1] A. G. Dimakis, P. B. Godfrey, Y. Wu, M. J. Wainwright, and K. Ramchandran, “Network coding for distributed storage systems,” IEEE Transactions on Information Theory, vol.56, no. 9, Sep. 2010.
[2] J. A. Garay, R. Gennaro, C. Jutla, and T. Rabin, “Secure distributed storage and retrieval,” Theoretical Computer Science, vol. 243, no. 1-2, pp. 363-389, Jul. 2000.
[3] A. Parakh and S. Kak, “Space efficient secret sharing for implicit data security,” Information Sciences, vol. 181, no. 2, pp. 335-341, Jan. 2011.
[4] N. B. Shah, K. V. Rashmi, K. Ramchandran, and P. Kumar, “Privacy-preserving and secure distributed storage codes,” http://www.eecs.berkeley.edu/ retrieval,” Journal of Computer and Systems Sciences, vol. 71, no. 2, pp. 213-247, Aug. 2005.

[5] C. Wang, Q. Wang, K. Ren, W. Lou, Privacy preserving public auditing for secure cloud storage. IEEE Transactions on Computers 62(2), 362–375 (2011)

[6] N. B. Shah, K. V. Rashmi, and P. Kumar, “Information-theoretically secure regenerating codes for distributed storage,” in Proc. IEEE Global Communications Conference (GLOBECOM), Houston, TX, Dec. 2011.

[7] S. Pawar, S. Rouayheb, and K. Ramchandran, “Securing dynamic distributed storage systems against eavesdropping and adversarial attacks,” IEEE Transactions on Information Theory, vol. 57, no. 10, pp. 6734-6753, Oct. 2011.

[8] O. O. Koyluoglu, A. S. Rawat, and S. Vishwanath, “Secure cooperative regenerating codes for distributed storage systems,” IEEE Transactions on Information Theory, vol. 60, no. 9, pp. 5228-5244, Sep. 2014.

[9] W. Huang and J. Bruck, “Generic secure repair for distributed storage,” arxiv preprint arXiv: 1706.00500, Jun. 2017.

[10] A. Shamir, “How to share a secret,” Communications of the ACM, vol. 22, no. 11, Nov. 1979.

[11] R. Cramer, I. B. Damgard, and J. B. Nielsen, Secure Multiparty Computation and Secret Sharing, Cambridge University Press, 2015.

[12] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan, “Private information retrieval,” in Proc. the 36th Annual Symposium on Foundations of Computer Science, Wisconsin, USA, pp. 41-50, Oct. 1995.

[13] Sheren A. El-Booz*, Gamal Attiya and Nawal El-Fishawy,” A secure cloud storage system combining time-based one-time password and automatic blocker protocol”, EURASIP Journal on Information Security, 2016.