International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 5 | Issue 3 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT1953107

Block Design Key for Secure Data Sharing in Cloud Computing

Rashmi K, H. P. Mohan Kumar
Master of Computer Application, PES College of Engineering, Mandya, Karnataka, India

ABSTRACT

Sharing Data in cloud allows multiple participants to share the group of data we are gifting a distinctive block design-based key agreement protocol that supports multiple participants, in whatever the way to make the protection of the data more secure while sharing between two users. Secure data sharing is performed using a private key generated and transmitted using secure channels. A key agreement protocol is used for data transfer to make more protection compare to later communication and this protocol is applied in cloud computing to support secure and economical sharing. In addition, an AES algorithm is used to encrypt the data. We have a susceptibility to estimate Block design key for secure data sharing in cloud, based on key agreement protocol with in which TPA verifies the malicious user from the group. To protect the data more secure every time when user as to download the data the TPA generates key to user. Every time the key is generated as, an OTP to secure the data from the attacker the user must use the same key to decrypt the data. In addition to that, the owner file is also generated to user. TPA acknowledge malignant client from group and detract from group we have a tendency to blessing general recipes for creating the normal meeting key for numerous members.

Keywords : Data sharing, Key agreement protocol, cloud computing, TPA, Security, AES.

I. INTRODUCTION

Cloud computing is the process of storing all our data in remote server instead of storing all our data in local system using internet connection. Cloud is on demand availability of computer system resource. Cloud computing and cloud storage has become hot topic in recent decades each unit of measurement can-do the tactic. We have a tendency to tend to settle on to store all kinds of knowledge in cloud servers. The cloud server provides associate open and convenient storage. Cloud service providers offer single or multiple cloud service for storing and sharing data securely among users i.e. Amazon service S3, the membership in the cloud is frequently changing and because of this security –preserving are turned into a challenging issue in the cloud. Company employees in the same department can share and store files in the cloud. However, there is a significant risk to the confidentiality of those stored files. For security Purpose, it is necessary to encrypt data before uploading files in the cloud. Some systems have used techniques for securing data sharing called cryptography among multiple group members in an untrustworthy cloud. However, these systems are not supported to dynamic group concept.TPA is used as a typical tool to provide confidentiality and privacy services to the data. The data are usually encrypted before storing to the cloud. TPA handles the access control, key management, and encryption of data process. The customers to ensure the data integrity when data are shared in a group, The TPA services are capable of handling the different users, exercise the access control, and manage the keys in an effective manner to safeguard data confidentiality. The registered users are consider as a newly join group member can be proved to be an insider threats for violating the data confidentiality and the privacy Insider threats can prove to be more damaging due to the trust that they are launched by trusted entities. We focus more on the outsider attackers than insider attacker does. In spite of that, there are several issues can arise due to different users in a single group. We discuss some issues in the following discussion. Authentication attacks these types of attacks are easily occurred in the cloud the attacker easily target the server by these types of Authentication attacks. The attacker's follows the regular user's steps followed by the users are observed by the attackers and try to access the confidential data and these problems arises when in one-step of authentication mechanism is used. So to overcome from this more than one authentication mechanism is established in the environment. Man-in-middle attack can be occurred. When communication established between two servers. The attacker in the communication system modifies the message sequence, this attack permits a malicious actor to interrupt, send and receive data between two users. This type of attack is avoided by proper authentication system, the encryption is used for sender's side decryption is used for receiver side so that the attacker cannot modify the encrypted data for that purpose we are using an AES algorithm. Wrapping attacks happens at the time of translation of protocol messages between a valid user and the web server. By an exact copy the users' account and password in the login period the attacker inserts the bogus element into the communication structure, and replaces the original message with harmful content and sends the message packets to server. The attackers can violet in transport layer services. For wrapping attack, we increase the security by using Key agreement protocols while communicating with web server and web browser. The TPA is responsible for key management. The protocol will be toggled when a third party interferes with the message during the communication. A cloud framework is moreover exposed to assaults from each pernicious clients and cloud providers. In these circumstances, it is important to affirm the security of the kept data safe inside the cloud.

II. RELATED WORK

In [1] proposed a common conference key to communicate with all the members in the group. It works when all the group members are honest but does not work when any one offs the conference are malicious and try to delay or destruct the conference. In [2,3] proposed a Enabling cloud storage auditing with key-exposure resistance to compromised keys has been taken into consideration, which is an important issue in the context of cloud computing enabling cloud storage auditing with verifiable outsourcing of key updates which not only imparts a burden to the TPA but also introduces some security problems.

In[4] proposes a trust enhanced cryptographic role-based access control for secure cloud data storage attempts to protect the privacy of data stored in the cloud, cryptographic role-based access control schemes have been developed to safeguard from threats however these cryptographic approaches do not address the issues trust.

In [5,6] introduces author provably authenticated group diffie-hellman key exchange In this protocol, to manage the complexity of definitions and proofs for the authenticated group Diffie-Hellman key exchange, a formal model was presented, where two security goals of the group Diffie-Hellman key exchange were addressed. Cryptanalysis of simple three-party key exchange protocol proposes public key infrastructure is used to circumvent man-in-the-middle attacks. However, these protocols are not suitable for resource-constrained environments since they require executions of time-consuming modular exponentiation operations.

Xu et al. [7] proposed authorized proxy reencryption scheme for sharing the data securely within the group in the public cloud. It encrypts the data with symmetric key afterwards it encrypts with public key both encrypted key and data are uploaded to the cloud. Again, the encrypted key is reencrypted by the cloud to decrypt the users private key .Private key generated is not based on the certificates, as it was bilinear pairing so it has some security issues based on the private key.

Seo et al [8] introduced a certificateless encryption approach for sharing data in public cloud to reduce bilinear pairing. The user public –private key is partially decrypted in the cloud due to which threats can easily decide to attack. From the perspective of security issues it is not suitable to shift the key generation process to share data in public or private cloud.

Chen and Tzeng [9,10] proposed a methodology based on the shared key derivation method for secure data sharing among the group. It uses the binary tree for calculations of keys so it not smart for public cloud to perform certain operations Similarly the RSA based approach proposes which is unsafe against the complicity attacks

III. PROPOSED SYSTEM

The proposed method ensures intended to keep confidential data on the cloud by using Symmetric key encryption. The system quality of predicted protocol linearly can increase with the quantity of users. The framework is really a mix of various frameworks comprising of SQL server, The SQL server stores the client data also, access to the gathering in its database.

A. Contributions

In this paper, we present a methodology called Block Design Key for secure data sharing in cloud computing that has four modulus:

1) Data Owner
2) Cloud server
3) TPA
4) Data User

The Data Owner uploads the data or submits the data to cloud server the list of Data users and parameter required for generating the access control list to TPA. Moreover, we are presenting a key agreement protocol that allows multiple participants to share their data in the cloud, which will flexibly extend the quality to contribute in equating the cloud setting in step with the structure of the block model. Supported the predicted mass of information sharing model. We have a tendency to present general formulas for generating the common convention key for multiple users.

In addition, the fault tolerance property of our protocol permits the bundle of information sharing in the cloud computing to set about to all totally different key attacks. A key agreement protocol is used to return up with a conventional key for multiple users to create positive security of their later communication and this protocol is applied in cloud computing to support secure and economical information sharing. Therefore, TPA is a trusted third party and is responsible of verifying the users, key management, and encryption of data. In addition to this, an OTP is generated to users every time when the user wants to access and download the information. Access control is used to security purpose to verify the user's authentication and is verified by TPA. The Key agreement protocol is used to generate the Common communication key between TPA and user, which is used to secure the data from later communication problem. In Addition to that the File uploaded to the cloud by owner is going to upload the File Key for each file. When user want to download the file.TPA is going to verify the user.TPA generates the encrypted key and the file key to the user. The user should use the same to keys to decrypt the data and can access the data. Thus, the secure data sharing in cloud among the group of users is safeguarded from Diffie-Hellman Key exchange protocol.

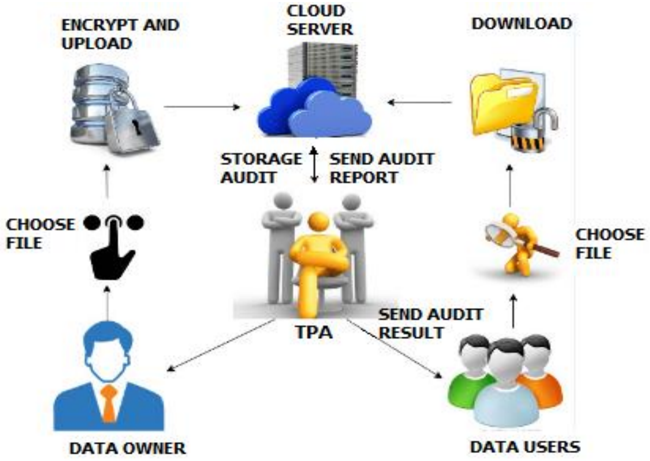

Figure 1 : System Architecture

B. Algorithm

AES algorithm is used by current Computers to encrypt and decrypt the data. It is a symmetric key algorithm, which uses the private key to encrypt and decrypt the data. And transmitted through secure communication channels.

AES Algorithm steps:

Step 1: Start

Step 2: Round keys are obtained from the cipher key. No of rounds performed by AES depends on the bit keys.AES uses 10 rounds for 128-bit and 12 rounds for 192 bit and 14 rounds for 256 bit.

Step 3: Initialize the 128 bits cipher key is stored in four columns and four rows for processing as a matrix.

Step 4: Add a round key where each byte of the state is combined with a block of the round key.

(i)Sub Bytes

An element in the matrix is replaced by an element of sub matrix this results in a matrix of four rows and four columns.

(ii)Shift Rows

In this steps the rows and cylindrically shifted to the left direction.

1. The first row is not shifted
2. The second row is shifted to left by one place
3. The third row is shifted to left by two places
4. The fourth row is shifted to left by three places

This result in 16 bytes of matrix but are shifted with respect to each other

(iii)Mix Columns

It is the main part of the algorithm. During this matrix each row is multiplied by single column of fixed matrix where this result into another new matrix consisting of 16 new bytes

(iv)Add round Key

The 16 bytes of matrix is now considered as 128 bits and are XORed to the 128bits of the round key. If this is the last round then the output is the secret text. Otherwise, the produced 128 bits are translated as 16 bytes and we start another similar round.

Step 5: Perform the tenth and final round of the position used.

Step 6: Copy the final text of array where data as encrypted is considered as the output.

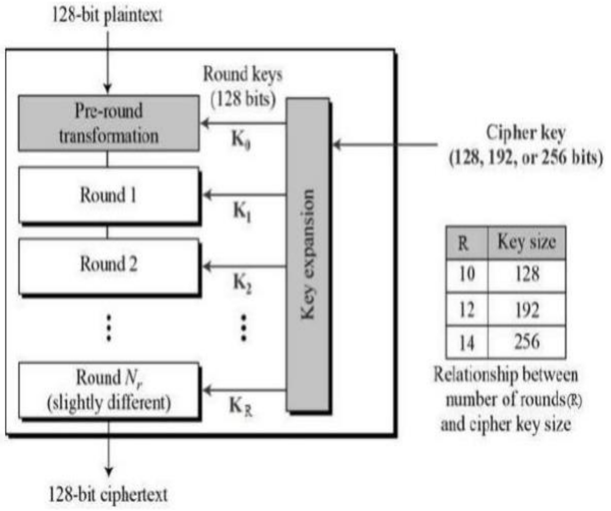

Figure 2 : Advanced Encryption standard encryption process

IV. EXPERIMENTAL RESULTS

The Block Design Key for secure data sharing in cloud presents the following services to the data uploaded by the Data Owners:

(i) The proposed method ensures intended to keep secret data on the cloud by using Symmetric Key encryption.
(ii) The secure data sharing in cloud among the group of users is safeguarded from Diffie-Hellman Key exchange protocol.
(iii) Secures the data against of access control that arrives due to inner threats.
(iv) The Key agreement protocol is used to generate the Common communication key between TPA and user which is used to secure the data from later communication problem
(v)The TPA generates OTP to the user when user wants to download the file.

The following discussion briefly describes the above-mentioned services are achieved. In the case of Block design key for secure data sharing in cloud, first, the data is encrypted with the key and that key is generated by TPA and deleted after the utilization of the user .TPA or user cannot reconstruct the key alone. For Security purpose, the data cannot be leaked unless the attacker get the key .Key is completely not stored anywhere. Therefore trying to access for key is difficult task. Moreover, if the insider threats try to access the file with the absence of key the user will be blocked for the security purpose and will not be able to access the data. For safety purpose, it will not allow for the reencryption with multiple keys of the data only the single symmetric key is used for encryption of the data. Therefore the raised of Block Design Key for Secure Data Sharing in Cloud methodology is fairly less as compared to RAS encryption.

V. CONCLUSION

We proposed the block design key for secure data sharing in cloud, where we are providing security for cloud storage. The implemented methodology provides the data are kept safe, secure data sharing with encryption, access control. Additionally the Block design key for secure data sharing provides encryption and decryption features are performed at the TPA that is the trusted third party and is responsible of various operations. The implementation of block design key for secure data sharing in cloud is determined based on the time consumption during key generation, file upload, and file download operations. The output displays that the methodology can be practically used in cloud for secure data sharing among the group.

VI. REFERENCES

[1]. X.Yi, “identity –based fault tolerant conference key agreement”, IEEE transactions on dependable and secure computing,vol.1,no.3,pp 170-178,2004.

[2]. J.Yu, K.Ren, and C.Wang,”Enabling cloud storage auditing with verifiable outsourcing of key updates” IEEE transactions on

information forensics and security,vol.11,no.6,pp.1-1,2016.

[3]. J.Yu,K. Ren, C.Wang and V.Varadharajan,"Enabling cloud storage auditing with Key-exposure resistance," IEE Transactions on information forensics and security,vol.10,no.6,pp.1-1,2015.

[4]. L.Zhou,V.Varadharajan and M.Hitchens, "Cryptographic rolebased access control for secure cloud data storage systems" information forensics and security IEEE transactions on,vol.10,no.11,pp.2381-2395,2015

[5]. H.Guo, Z.Li, Y.Mu, and X.Zhang,"Cryptanalysis of simple three-party key exchange protocol" computers and security,vol.27,no.1-2,pp.16-21,2008.

[6]. W.Diffie and M.E.Hellman, "New directions in cryptography," IEEE Transactions on information theory,vol.22,no.6,pp.644-654,1976.

[7]. L.Xu,X.Wu, and X.Zhang,"CL-PRE: A certificateless proxy reencryption scheme for secure data sharing with public cloud," in proc 7th ACM symp. Inf,comput.commun security,2012,pp.87-88.

[8]. S.Seo,M.Nabeel,X.Ding and E.Bertino,"An Efficient Cerficate-less encryption for secure data sharing in public clouds",IEEE Transactions Data Eng,vol.26,no.9,no.9,pp.2107-2119,sep.2013.

[9]. Y.Chen and W.Tzeng,"Efficient and provably-secure group key management scheme using key derivation," in proc. IEEE 11th intconf trustcom,2012,pp.295-302.

[10]. Y.Chen,J.D.Tygar, and W.Tzeng, "Secure group management using uni-directional proxy re-encryption schemes" IEEE INFOCOM, pp.1952-1960.

Author Details:

Rashmi K received his Bachelor's degree in Computer Science from Mysore University, India, and she is currently pursuing MCA in PES College of Engineering, Mandya, and Karnataka, India.

Mohan Kumar H P received the MCA, M.ScTech and Ph.D from University of Mysore. He is currently professor in computer application department at PES College of engineering, Mandya. His research interest includes computer vision, Machine's intelligence Data mining, Artificial intelligence and cloud computing.

Cite this article as :

Rashmi K, H. P. Mohan Kumar, "Block Design Key for Secure Data Sharing in Cloud Computing", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 3, pp. 369-374, May-June 2019. Available at doi : https://doi.org/10.32628/CSEIT1953107
Journal URL : http://ijsrcseit.com/CSEIT1953107