International Journal of Scientific Research in Science, Engineering and Technology (www.ijsrset.com)
© 2020 IJSRSET | Volume 7 | Issue 1 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
DOI : https://doi.org/10.32628/IJSRSET207140

Study on Encryption Techniques Used to Secure Cloud Storage System

Athulya V S[1], Dileesh E D[2]

[1]M. Tech Scholar, M Tech Scholar, Department of Computer Science and Engineering, GEC Idukki, Kerala, India

[2]Assistant Professor, Department of Computer Science and Engineering, GEC Idukki, Kerala, India

ABSTRACT

Cloud storage is used generally to store data and realize the data sharing with others. A cloud storage system stores large number of data in its storage server. Data that are stored to the cloud have to be secured in order to avoid the data from exploiting. There are several techniques and methods that are used to secure the data before uploading it to the cloud such as cryptographic encryption techniques. In this paper, we study about different encryption technique to protect the cloud storage environment. This paper covers some of the existing cryptographic approaches that can be used to improve the security in cloud environment.

Keywords : Encryption, Cloud, Cloud Storage

I. INTRODUCTION

Cloud computing is a new computing technique that was created after grid computing, utility computing and distributed computing. The main idea of cloud computing is application hosting and service outsourcing etc.

With cloud computing technology, users do not need to spend much on the maintenance and cost of the system. In addition, strong computing and storage space makes users more willing to depend on the cloud to handle difficult tasks.

When users choose to store a large number of applications and data to the cloud platform, the cloud computing system becomes the cloud storage system. Cloud storage systems give users mass storage capacity at a very low price, and provide a platform for sharing data between users but According to the survey conducted on 2007 only 60% of the total companies uses this cloud computing platform due to privacy concerns. Thus, the secure storage of data in the cloud has blocked the use of cloud computing.

So in order to protect the data privacy, encryption techniques were introduced. Before storing data in to the cloud, these data will undergo some cryptographic encryption techniques and this additionally provides confidentiality and integrity to the data.

In this paper, we describe various cryptographic techniques that can be used to protect the data used in the cloud and prevent information from being leak and to ensure that the privacy has been maintained.

The data sharing is one of the most widely used services that the cloud storage provides. With data sharing service, users can share their data in the cloud with a group of users them in the cloud. Any error

might cause loss or damage to the data. In order to check the data integrity, some cloud storage auditing schemes for shared data are proposed. When a group

user misbehaves or leaves the group, the user should be revoked from the group.

The rest of the paper is organized as follows: background studies in section II. In section III, the survey on the various encryption techniques is presented. Section IV describes our conclusion.

II. BACKGROUND

A. Cloud Computing

Cloud computing is the availability of computer system resources especially data storage and computing power without direct access of the user. Large clouds that are found today have functions distributed between multiple locations from different servers. If the connection between user and the cloud is too close then the cloud will act as edge server.

The clouds can be limited to a single organisation or multiple organisations. The cloud can be Public or Private. The cloud computing enables the enterprises to get their applications up and running them faster with less maintenance and cost.

The Cloud Service Provider (CSP) will screen, keep up and gather data about the firewalls, action framework and information inside the system.

Worm: these are self-replicating programs that spread from one computer to another by transmitting its copy via network relying on the security failures on target computers to access, steal or delete the data.

B. Cloud Storage

Cloud storage is a model of computer data storage in which the digital data is stored in pools. The cloud storage providers are responsible for keeping the data available and accessible.

The cloud storage services may be accessed through a cloud computing services, a web service application programming interface (API) or by applications that utilize the API, such as cloud desktop storage, a cloud storage gateway or Web based content management systems. A cloud platform provides users with shared data storage services. To ensure shared data integrity, it is necessary to validate the data effectively. An audit scheme that enables group members to modify data conducts the integrity verification of the shared data, but this approach results in complex calculations for the group members.

C. Cryptographic Encryption

In cryptography, encryption is the process of changing a message or information (plaintext) to a meaningless and unreadable form (cipher text) so that only authorized parties can access it and those who are not authorized cannot. In an encryption scheme, the intended information or message, referred to as plain text, is encrypted using an encryption algorithm to generate cipher text that can be read only if decrypted. The encryption and decryption keys are the same for symmetric encryption and the encryption and decryption keys are different for asymmetric encryption.

D. Integrity

Integrity is the maintenance of and the assurance of the accuracy and consistency of data over its cycle. The overall intent of any data integrity technique is the same, ensure data is recorded exactly as intended and upon later retrieval, ensures data is the same as it was originally recorded. It enables to prevent unintentional changes to information. In remote data integrity auditing schemes, the data owner firstly needs to generate signatures for data blocks before uploading them to the cloud. These signatures are used to prove the cloud truly possesses these data blocks in the phase of integrity auditing. And then the data owner uploads these data blocks along with their corresponding signatures to the cloud. The data stored in the cloud is often shared across multiple users in many cloud storage applications, such as Google Drive, Dropbox and iCloud. Data sharing as one of the most common features in cloud storage,

allows a number of users to share their data with others. However, these shared data stored in the cloud might contain some sensitive information.

III. STUDY ON ENCRYPTION TECHNIQUE USED ON CLOUD STORAGE SYSTEM

ManishKo the, Harshal Karandikar, Nikhil Wani, Sumit Ta mkhane [1] proposed Attribute-Based Encryption Method. Here a Attribute based encryption is a public-key-based one-to-many encryption that allows users to encrypt and decrypt data based on user attributes. ABE system with outsourced decryption that largely eliminates the decryption overhead for users. There are two types of ABE, they are Cipher-Text Policy Attribute Based Encryption (CP-ABE) and Key Policy Attribute Based Encryption (KP-ABE). In the Cipher text policy, the data is encrypted as cipher text and stored to the cloud. The contribution of this is that Attribute Based Encryption with Verifiable Outsourced Decryption guarantee the security property that no malicious cloud will be able to learn anything about the encrypted data. The limitations of this system is that resource limited devices the decryption is very expensive due to pairing operation. One drawback of encrypting data is that it can be selectively shared only at a coarse-grained level. Attribute based encryption is a

publickey-based one-to-many encryption that allows users to encrypt and decrypt data based on user attributes. A promising application of ABE is flexible access control of encrypted data stored in the cloud using access policies and ascribed attributes associated with private keys and cipher texts. This functionality comes at a cost. In typical implementation, the size of the cipher text is proportional to the number of attributes associated with it and the decryption time is proportional to the number of attributes used during decryption. Specially, many practical ABE implementations require one pairing operation per attribute used during decryption. One of the main efficiency drawbacks of the existing ABE schemes is that decryption involves expensive pairing operations and the number of such operations grows with the complexity of the access policy. Recently green et al. proposed an ABE system with outsourced decryption that largely eliminates the decryption overhead for users. tn such a system a user provides an untrusted server, say a cloud to translate any ABE cipher text satisfied by that users attributes or access policy into a simple ciphertext and it only incurs a small computational overhead for the users to recover the plaintext from the transformed ciphertext. Security of an ABE system with outsourced decryption ensures that an adversary will not be able to learn anything about the encrypted message; however it does not guarantee the correctness of the transformation done by the cloud. In this Project we consider a new requirement of ABE with outsourced decryption: verifiability. Informally, verifiability guarantees that a user can effectively check if the transformation is done correctly.

Liang Liu and Jun Ye [2] proposed A Homomorphic Universal Re-encryptor for Identity-based Encryption Which uses identity-based proxy re-encryption (IBPRE) scheme. The re encryptor is the method of transforming cipher text under one public key in to new cipher text in another public key. The functional Homomorphic encryption is used to protect the master secret s. But the introduction of fully Homomorphic encryption decreases the efficiency of the system. A novel identity-based proxy re-encryption (IBPRE) scheme which to the maximum extent reduces the workloads in the user side by delivering the re-encryption key (RK) generation work to the proxy server. It is not suitable for multi hop re- encryptions. It plays an important role in modern secure communication and information exchange via various kinds of network infrastructure. In addition to traditional public-key encryption scheme, re-encryption can also come into force in other cryptosystems like Identity-Based Encryption (IBE) and more advanced Functional Encryption (FE),

making the enhanced schemes more powerful as well as easy-to-use. This primitive is very useful in a scenario where the users only have limited computation or storage capability as we have explained above. Besides, the universality property features the advantage that a user can gain her re-encryption key quite easily by just issuing a re-encryption key query containing only two id's and the proxy does not need to deal with any public key or private key relevant information. This is due to the delegation of part of the master secret key s in the encrypted form under a fully homomorphic encryption (FHE) scheme.

Caihui Lan , Haifeng Li , Shoulin Yin, and Lin Teng [3] proposed a A New Security Cloud Storage Data Encryption Scheme Based on Identity Proxy Re-

encryption which uses i dentity proxy re-encryption here Computational Overhead is present. When a data is shared with many users the scalability is weak. Plain text encryption scheme to cipher text security encryption scheme is used. The system consists of control all the other keys. Here secret shares are generated then deduplication is done and the hash valus are checked which is used to check the integrity and this hash values are uploaded in to the cloud.

Cong Wang, Sherman S.-M. Chow, Qian Wang,Kui Ren and Wenjing Lou[4] proposed Privacy-Preserving Public Auditing for Secure Cloud Storage, Here a homomorphic linear authenticator with random masking technique is proposed. In this paper a securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to user. In this paper. scheme is the first to support scalable and efficient public auditing in the Cloud Computing.A public auditing scheme consists of four algorithms(KeyGen, SigGen ,Gen Proof ,Verify Proof). KeyGen is a key generation algorithm that is run by the user to setup the scheme. Sig Gen is used by the user to generate verification metadata, which may consist of MAC ,signatures, or other related information that will be used for auditing. Gen Proof is run by the cloud server to generate a proof of data storage correctness, while Verify Proof is run by the TPA to audit the proof from the cloud server. r, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to a third party auditor (TPA) to check the integrity of

outsourced data and be worry-free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to user. In this paper, we propose a secure cloud storage system supporting privacy-preserving public auditing.

Mohammad Ubaidullah Bokhari and Qahtan Makki Shallal[5] proposed Hybrid Encryption Technique to Secure Data during Transmission in Cloud Computation. Here it uses hybrid encryption and decryption process based on AES-128 and RSA algorithm. This is mainly used for the integrity and Confidentiality. The limitation of this method is that Decryption and encryption time consumption is more. The plaintext is converted to cipher by using AES algorithm, the key used for this AES is got from RSA algorithm. And in order to check the integrity an HMAC algorithm is also used. The technology of Cloud computing is permit the subscribers to store their own data in its infrastructure. The subscribers will be able to use their stored data whenever they required. Since the data are stored outside their boundary, it needs to use a strong encryption during transmission process to be protected well. Thus, in this paper we have proposed a model to use a hybrid encryption and decryption process based on AES-128 and RSA algorithm.

Avinash Shukla, Sanjay Silakari and Uday Chourasia[6] proposed A Secure Data Storage over Cloud using ABE where Enhanced lockbox algorithm with more secure algorithm AES is performed. It has Less computation time and cost. The concept behind the research is taken a secure and reliable algorithm, approach which can find the solution for security as well as de-duplication redundancy optimizationover data. Cloud computing is an emerging area of research, where most of the IT infrastructure is moving to make their service and delivery more efficient. Cloud computing make it more scalable, more reliable, secure and accessible with plenty of option to perform its best. In this paper our work approach leads behind the data ownership and security providing over the user session. The existing technique based on key generation for the user session and further the extension is performed on Enhanced lockbox session concept for file sharing and management. The concept behind the research is taken a secure and reliable algorithm, approach which can find the solution for security as well as de-duplication redundancy optimization over the data store. The existing base paper discussed about the file level distribution where as to transmit and store the data AES (Asymmetric encryption system) algorithm is used to provide data security.

Swati V.Thakre, Prof. K.K.Chhajed and Prof. V. B. Bhagat [7] proposed Key Based Encryption Scheme for Secure Data Sharing on Cloud here a Key Based Encryption scheme is used and one of the to distribute a single key to a user when sharing lots of documents with the user. Cloud storage makes it possible for users to remotely store their data and enjoy the ondemand high quality cloud applications without the any burden of local hardware and software management, which boasts an array of advantages like unlimited storage capability, anywhere accessibility etc. Since Cloud computing environment is constructed on open architectures and interfaces; it has the potential to incorporate multiple internal and external cloud services together to provide high interoperability. Sowmya P , Revathi P , Dr. Thirumala Rao [8] proposed POLICY BASEDDATA DEDUPLICATION IN CLOUD STORAGE were The Deduplication techniques like file level block level and byte level data Deduplication mechanism is used. The Deduplication technology has gained more popularity in cloud storage system with the increase in growth rate of digital data. Deduplication techniques minimizes the redundant data by using data Deduplication techniques like file level, block level, byte level and identifies duplicate copy by calculating the hash values. Now a day's maintaining the data reliability and the confidentiality to the stored data becomes a curial part in the cloud storage. The Deduplication technology has gained more popularity in cloud storage system with the increase in growth rate of digital data. Deduplication techniques minimizes the redundant data by using data Deduplication techniques like file level, block level, byte level and identifies duplicate copy by calculating the hash values. Now a day's maintaining the data reliability and the confidentiality to the stored data becomes a curial part in the cloud storage. Dekey Ramp Secrete key and Dupless are used methods here. The deduplication is used in orde to reduce the system traffic. A master key is generated and it is used to control all the other keys. Here

secret shares are generated then deduplication is done and the hash valus are checked which is used to check the integrity and this hash values are uploaded in to the cloud.

Abiodun Esther Omolara [9] proposed Security and Verification of Data in Multi-Cloud Storage with Provable Data Possession were Cooperative Provable Data Possession Scheme is used and the advantage of this system is that This technique gives astrong proof of data integrity.Support Block less verification. The This paper looked into the Cloud storage and different techniques that are used to store data securely to cloud. The Encryption was said to provide security to

data in the cloud. A cloud storage system stores large number of data in its storage server. Data that are stored to the cloud have to be secured in order to avoid the data from exploiting. There are several techniques and methods that are used to secure the data before uploading it to the cloud such as cryptographic encryption techniques with Sensitive Information Hiding for Secure Cloud Storage here sensitive data is only hided it does not use any encryption techniques, The hiding is done by using blinding and sanitizer. One of the advantage is that no encryption is used here. And it is more secure than any other above techniques.

Wenting Shen, Jing Qin, Jia Yu, Rong Hao, and Jiankun Hu, Senior Member[10] proposed Enabling Identity- Based Integrity Auditing and Data Sharingwith Sensitive Information Hiding for Secure Cloud Storage here sensitive data is only hided it does not use any encryption techniques, The hiding is done by using blinding and sanitizer. One of the advantage is that no encryption is used here. And it is more secure than any other above techniques. Group users compute their new private keys SKID;RN by using the identity key IDKID and the partial key TKID;RN. The user revocation is realized by a key update technique. The number of user revocations RN plays an important role in the key update. RN is a value set by the group manager, and also known by group users and the cloud. When the system is initialized, set RN = 0. When users are revoked, set RN = RN + 1. The group manager generates a new partial key corresponding to this new value of RN, and sends it to all of the non-revoked group users. Then the non-revoked group users update their private keys using the new partial key. In this way, the revoked user cannot get the current private key related to the newest RN.

IV. CONCLUSION

This paper looked into the Cloud storage and different techniques that are used to store data securely to cloud. The Encryption was said to provide security to data in the cloud. A cloud storage system stores large number of data in its storage server. Data that are stored to the cloud have to be secured in order to avoid the data from exploiting. There are several techniques and methods that are used to secure the data before uploading it to the cloud such as cryptographic encryption techniques.

V. REFERENCES

[1]. ManishKo the,Harshal Karandikar, NikhilWani, SumitTamkhane "Attribute-BasedEncryptionwithVerifiableOutsourced

[2]. Decryption" 2016,International Research Journal of Engineering and Technology.

[3]. Liang Liu and Jun Ye "HoneyGen: "A Homomorphic Universal Re-encryptor for Identity-based Encryption", 2016,International Journal of Network Security.

[4]. Cong Wang, Sherman S.-M. Chow, Qian Wang,Kui Ren and Wenjing Lou"Privacy-Preserving Public Auditing for Secure Cloud Storage" 2013,IEEE Transactions on Computers.

[5]. Mohammad Ubaidullah Bokhari and Qahtan Makki Shallal "Hybrid Encryption Technique to Secure Data during Transmission in Cloud Computation " 2017,International Journal of Computer Applications.

[6]. Avinash Shukla, Sanjay Silakari and Uday Chourasia "A Secure Data Storage over Cloud using ABE Approach " 2017,International Journal of Computer Applications.

[7]. Swati V.Thakre, Prof. K.K.Chhajed and Prof.V.B.Bhagat "Key Based Encryption Scheme for Secure Data Sharing on Cloud' ,International Research Journal of Engineering and Technology.

[8]. Caihui Lan , Haifeng Li , Shoulin Yin, and Lin Teng. "A New Security Cloud Storage Data Encryption Scheme Based on Identity Proxy Re-encryption". 2016, International Journal of Network Security.

[9]. Abiodun Esther Omolara "Security and Verification of Data inMulti-Cloud Storage with

Provable Data Possession " 2015,International Journal of Computer Applications.

[10]. Wenting Shen, Jing Qin, Jia Yu, Rong Hao, and Jiankun Hu, Senior Member "Enabling Identity-Based Integrity Auditing and Data Sharing with Sensitive Information Hiding for Secure Cloud Storage" IEEE Transaction 2018.

[11]. C. Erway, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in ACM Conference on Computer and Communications Security, 2009, pp. 213–222.

[12]. Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," IEEE Transactions on Parallel and Distributed Systems, vol. 22.

[13]. J. Yu, K. Ren, C. Wang, and V. Varadharajan, "Enablingcloud storage auditing with key-exposure resistance," IEEE Transactions on Information Forensics and Security, vol. 10, no. 6, pp. 1167–1179, 2015.

[14]. 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. 1362–1375, June 2016.

[15]. J. Yu and H. Wang, "Strong key-exposure resilient auditing for secure cloud storage," IEEE Transactions on Information Forensics and Security, vol. 12, no. 8, pp. 1931–1940, Aug 2017.

[16]. J. Yu, R. Hao, H. Xia, H. Zhang, X. Cheng, and F. Kong, "Intrusion-resilient identity-based signatures: Concrete scheme in the standard model and generic construction," Information Sciences, vol. 442-443, pp. 158 – 172, 2018.

[17]. B. Wang, B. Li, and H. Li, "Oruta: Privacy-preserving public auditing for shared data in the cloud," in 2012 IEEE Fifth International Conference on Cloud Computing, June 2012, pp. 295–302.

[18]. G. Yang, J. Yu, W. Shen, Q. Su, Z. Fu, and R. Hao, "Enabling public auditing for shared data in cloud storage supporting identity privacy and traceability," J. Syst. Softw., vol. 113, no. C, pp. 130–139, Mar. 2016.

[19]. A. Fu, S. Yu, Y. Zhang, H. Wang, and C. Huang, "Npp: A new privacy-aware public auditing scheme for cloud data sharing with group users," IEEE Transactions on Big Data, 2017. [Online]. Available: DOI:10.1109/TBDATA.2017.2701347

[20]. B. Wang, B. Li, and H. Li, "Panda: Public auditing for shared datawith efficient user revocation in the cloud," IEEE Transactions on Services Computing, vol. 8, no. 1, pp. 92–106, Jan.-Feb. 2015.

[21]. Y. Luo, M. Xu, S. Fu, D. Wang, and J. Deng, "Efficient integrity auditing for shared data in the cloud with secure user revocation," in Proceedings of the 2015 IEEE Trustcom/BigDataSE/ISPA - Volume 01, ser. TRUSTCOM '15, 2015, pp. 434–442.

[22]. H. Wang, "Identity-based distributed provable data possession in multicloud storage," IEEE Transactions on Services Computing, vol. 8, no. 2, pp. 328–340, 2015.

[23]. H. Wang, D. He, and S. Tang, "Identity-based proxyoriented data uploading and remote data integrity checking in public cloud," IEEE Transactions on Information Forensics and Security, vol. 11, no. 6, pp. 1165–1176, June 2016.

[24]. Y. Yu, M. H. Au, G. Ateniese, X. Huang, W. Susilo, Y. Dai, and G. Min, "Identity-based remote data integrity checking with perfect data privacy preserving for cloud

Cite this article as :

Athulya V S, Dileesh E D , "Study on Encryption Techniques Used to Secure Cloud Storage System", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 7 Issue 1, pp. 238-244, January-February 2020. Available at doi : https://doi.org/10.32628/IJSRSET207140
Journal URL : http://ijsrset.com/IJSRSET207140