International Journal of Progressive Research in Science and Engineering
Volume-1, Issue-8, November-2020
www.ijprse.com

An Overview of Providing Privacy for Cloud Data and Its Users Using Signature Keys

***Hiral Asna Kumar*[1], Sheeja Beevi S [2]**

[1]*Student, Computer Science and Engineering, Lourdes Matha College of Science and Technology, Thiruvananthapuram, India.*

[2]*Assistant Professor, Computer Science and Engineering, Lourdes Matha College of Science and Technology, Thiruvananthapuram, India*

Corresponding Author: hiralasna@gmail.com

Abstract: - Cloud computing is an emerging technology in IT industries. Since resources remotely shared and processed by third party, there is a need to provide privacy for data and users. For that, different encryption methods and policies are used. This paper overviews different method for providing privacy for users and data in cloud, how they shared in cloud and analysed different algorithms used for encryption. It also provides different access schemes like signature keys in order to access the cloud.

Key Words: — ***Cloud, encryption algorithm, privacy***

I. INTRODUCTION

Cloud computing is one of the trending developments in IT industries. Cloud refers to an on-demand availability of computer resources, where data and programs are stored over the internet and can be access remotely. Data distributed at different location in cloud as resources. Cloud can be categorize as private cloud, public cloud and hybrid cloud.

Private cloud- this infrastructure works for only one organization, which managed by only by the company itself. It improves security and optimize the access between user and network.

Public cloud – a platform provides services to everyone and belongs to a provider of cloud service.

Hybrid cloud – it is a mixture of two or more cloud model.

Cloud computing is an essential low maintenance way to share resources [1]. In cloud computing privacy is one of the most important issue because sharing data, processing and transferring data in third party is vulnerable to various attack, such as attacks on client profile, synchronize cookies etc. Moving data in cloud makes the data and client information riskier. By providing privacy, data access is restricted to only authorize users. Access control based on encrypted data is a common privacy method. Access control to any system depends on the providers of the system who support basic authentication. Some of the access control methods includes providing key id, signature keys in order to authenticate users and use the services of the cloud. In Cloud, computing set of computers used to provide different accounts and service. Cloud computing providers focus on providing secure environments for organizations, flexible service, cost effective IT infrastructure. Privacy of data and user is the main issue in cloud computing because it's processing and the third party does usage. Therefore, it is important for clients, data owners to guarantee privacy for the information stored in cloud.

II. LITERATURE SURVEY

Anwar Chitheer Jasim proposed access control by signature keys to provide privacy for cloud and big data [1]. In order to provide privacy for data stored in cloud various privacy techniques applied followed by the upload of that data into cloud. It consists of cloud, transaction manager, and client. This based on the base of zero trust. Here the transaction manager will create a list of roles and groups, and generate keys. When a user wants to access cloud, He should first register his information and obtain signature keys. If the user has an ID in the list of 〖ID_u , then the user will be verified based on the key received from the transaction manager. If he is a valid user, he will be added to the authentication list. Group signature is also provided for each group. Based on the attributes present in the Group signature, he will be added to a particular group. In case of any dispute transaction manager has the power to exclude particular member from the group. Attribute based encryption algorithm is used for encryption.

Jian Shen proposed Anonymous and traceable group data sharing in cloud computing [2], that provides secure and efficient data sharing in cloud. To provide privacy key agreement and group signature is used so that group members can communicate without revealing the real identity of group members. Common conference key derived based on SBIBD structure and group signature to support secure group data sharing and to protect the outsourced data. Group member can dynamically change. By taking the advantage of key agreement and efficient access control, computational complexity and communication complexity for updating the

data are relatively low. However, the disadvantage is that the attacker tries to reveal the common conference key to decrypt the outsourced data.

T.A Mohanprakash proposed a novel privacy preserving system for cloud data security using signature-hashing algorithm [3]. Here, in a huge organization with cloud storage framework there is a chance of delicate information being breached. For preserving the privacy in Electronic Health Record (EHR) framework reviewing of shared information is done. So, hash signature is created for each record using the hashing algorithm. The hashed value and file are stored in the local storage and also send a copy to the public cloud. An auditing mechanism at the cloud hashes file and the hashed value is compared with the hash value sent by the data owner. If there is a mismatch, data owner will replace the file with the original file, otherwise there is no need to send the file thus preserving the integrity of data and privacy. The advantage of hashing using SHA-256 is that it is not prone to hash collision because of increased bit length. But it can degrade the security mechanism of SHA-256 with the bit length and hashed value output.

Yujiao Song proposed an efficient Attribute Based Encryption with privacy preserving key generation and its application in industrial cloud [4]. To provide confidentiality encrypt the data before uploading it and access control is based on Attribute Based Encryption (ABE). Here Key Generation Centre (KGC) generates keys and Attribute Auditing Centre (AAC) provides blind token. To provide privacy functionality of AAC and KGC are separated so that KGC cannot know the user attributes and AAC cannot obtain users secret key, thus information about the user attributes and private key is not leaked. To protect user's privacy during key generation phase Oblivious transfer protocol is used. In Attribute Based Encryption a user whose attributes satisfies the access policy set by the encryptor can decrypt the cipher text. The advantage of blind token is that, it will give evidence for user's owning attributes.

Xiaodong Yang proposed privacy- preserving cloud auditing for multiple users' scheme with authorization and traceability [5]. Here, inorder to solve issues like identity disclosure, denial of service attack and single manager abuse of a power cloud auditing scheme is provided. Certificate less signature technology is used to provide privacy for multiple users with authentication and traceability. It also uses identity authentication process between third party auditor (TPA) and cloud service provider (CSP) to prevent denial of service attack. This scheme consists of key generation centre, group users, group manager, CSP and TPA. KGC generates private keys, public keys, tags of shared data and public keys and are stored in cloud. Group users send their requests to the TPA for auditing the integrity of shared data. After receiving requests, TPA sends challenge to the CSP for getting the auditing proofs and sends it to TPA. If it is valid, CSP generates proofs. TPA checks the effectiveness of the proof from the CSP and gives the result about the shared data integrity of group users. The advantage of certificate less cryptography ensures that this scheme does not involve certificate management problem and escrow problem.

Amog Santosh Pai Raiturkar proposed an efficient and secure cloud data distribution and sharing scheme in groups [6]. In this scheme data will be stored in cloud in groups. Group-Signature verification and encryption-decryption technique are used to secretly share data with other users. Trusted third party as a data centre is used to activate and deactivate a new user to reveal the real identity of a user in case of disputes. The architecture consists of four major components: data custodian, data centre, private key generator (PKG) and cloud. Data centre has the privilege to perform creation of group, activate or deactivate members. PKG grants private keys for each group created by admin, Data custodian using his information will register and then join the group after successful verification using group signature. Cloud is the data storage. AES algorithm is used to encrypt large amount of unrestricted data. ID based ring signature algorithm is used to check data authenticity, anonymity and data sharing to a large number of group members. The custodian will choose the group in which he wishes to upload data in a ring topology. Key exposure is a serious issue in ring signature scheme.

III. Analysis Of Different Algorithms

A. RSA Algorithm

RSA algorithm is an asymmetric algorithm. It uses exponentials for encryption and decryption.

At encryption side, C=M^d mod n

At decryption side, M=C^e mod n

Where C is the cipher text, M is the plain text, d is the public key used for encryption and e is the private key used for decryption.

RSA algorithm is used to encrypt small data and it will take maximum execution time. Here only users are secured.

B. AES Algorithm

AES is a symmetric key algorithm used for encryption and decryption. It uses different keys 128/192/256 bits. For 128 bits about 2^128 attempts are needed to break. It can encrypt large amount of data of unlimited or unrestricted size and takes lesser execution time. Both users and providers are secured using AES algorithm.

C. ABE Algorithm

Attribute based encryption is a public key encryption algorithm, in which encryption and decryption is based on user attributes. Decryption is possible if the user key matches with set of attributes.

D. Sha 256

SHA 256 (Secure hash algorithm) is a cryptographic hash function that has digest length of 256 bits. It is used to provide signature for text or data. SHA-256 algorithm is prone to length extension attack.

IV. CONCLUSION

Cloud computing is an emerging technology in IT industries. The privacy of data and users in cloud are the most important issues, because sharing, processing and transferring of data are processed by third party. Various encryption techniques and algorithms used to provide privacy are analyzed here. Different methods of providing signature keys are analyzed here. To provide more privacy members are provided with signature keys.

REFERENCES

[1]. Anwar Chitheer Jasim, Nicolae Tapus, Imad Ali Hassoon," Access Control by Signature-Keys to Provide Privacy for Cloud and Big Data", 2018 5th International Conference on Control, Decision and Information Technologies, April 10-13, 2018.

[2]. ian Shen, Tianqi Zhou, Xiaofeng Chen, Jin Li, Willy Susilo "Anonymous and traceable group data sharing in cloud computing" IEEE, April 2018.

[3]. T.A Mohanprakash, Dr.J.Andrews "Novel privacy preserving system for cloud data security using Signature Hashing Algorithm", IEEE, 2019.

[4]. Yujiao Song, Hao Wang, Xiaochao Wei, Lei Wu, "Efficient Attribute-Based Encryption with Privacy-Preserving key generation and its application in industrial cloud", May 2019.

[5]. Xiaodong Yang, Meiding Wang, Ting Li, Rui Liu, Caifen Wang, "Privacy Preserving Cloud Auditing for Multiple Users Scheme with Authorization and Traceability", IEEE, July 2020.

[6]. Amogh Santosh Pai Raiturkar, Sonia Fernandes, Anusha Pai," Efficient and Secure Cloud Data Distribution and Sharing Scheme in Groups", Second International Conference IEEE, 2018.