Key Techniques used for Security in the Cloud

Kashyap Chetan Kotak[1] Ria Wadhwani[2] Shikha Soneji[3] Prof. Sunita Sahu[4]
[1,2,3]Student [4]Assistant Professor
[1,2,3,4]Department of Computer Engineering
[1,2,3,4]VESIT, Mumbai, India

Abstract— Since the past few years, there has been a rapid progress in the field of Cloud Computing. With the increasing number of companies applying for the various resources in the Cloud, there is a necessity for protecting the huge amount of data of various users using these centralized resources. Some of the challenges that are being faced by Cloud Computing are to secure, protect and process the data which is the property of the user. Certain techniques are applied in Cloud computing for the security and integrity of data of each user.

Key words: Cloud Computing, Security in the Cloud

I. INTRODUCTION

Cloud Computing is an upcoming new technology which provides the on-demand facility of a shared pool of resources (computing resources) (e.g., computer storage, applications and other resources), which can include rapid allocation and freedom with minimum number of efforts. Cloud computing and storage solutions provide individual users and companies with variety of capabilities to store and work on their data in data centers which are not owned by them and the location may be remote, may be across a city or across continents. Cloud computing provides sharing of resources to achieve economy of scales. The users use this cloud for sharing and the collaboration of their data with many other users in the group. Data sharing has become need in today's world and it is provided in most of the cloud storage offerings, via Drop box, Google.

Cloud is a type of platform which helps to store the data as well as helps in sharing the data. Cloud computing is the practice where multiple remote servers can be connected on a network and data is processed remotely rather locally on a computer. Cloud computing has taken Internet's era to a next level, providing the means through which everything — from computing power to Platform, Infrastructure and Service — can be delivered to you at place and time of your choice. Cloud possesses 4 characteristics: elasticity, self-service, application programming interfaces (APIs), billing and metering of service usage. This great flexibility is what is attracting everyone to move to the cloud [1].

II. ISSUES ASSOCIATED WITH CLOUD

There are various problems associated with the usage of the cloud. Some of the problems related with cloud are:

A. Authentication Issues

Authentication in cloud computing deals with the proper identity of the entity or person that is provided access to the data from the cloud service provider. When authentication is provided in the cloud, it means that the user is actually the one that he/she declares to be.

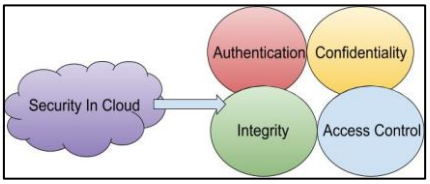

Fig. 1: Security in Cloud

B. Confidentiality in Cloud Computing

Confidentiality is among the most important mechanisms to ensure that the users' data is protected in the cloud. It includes various techniques like encryption that converts plain text into cipher text before the it is stored in remote cloud. This technique ensures protection of users' data and even cloud service providers cannot modify the content that is stored by the users.

C. Data Integrity

When a data is stored on a cloud It can be accessible from any location. But the problem is that the cloud cannot differentiate between sensitive and common data thus allowing anyone to access the sensitive data. Hence, there is a lack of data integrity [3].

D. Access Control

It is important security mechanism which helps to enable data protection in the cloud. It helps to ensure that only authorized users have access to the requested data that is stored in the cloud.

III. TECHNIQUES USED

As mentioned above, the techniques which can satisfy any of the four aspects of cloud security are described below:

A. Authentication [4]

The important point here is to deny access to unauthorized people. This ensures that the servers reject access requests from unknown people and manage the type of access of the legitimate users.

1) Authentication via username and password

Here, the user possesses a valid set of username and password registered with the cloud. Here, the password need not be stored in plaintext in the cloud as this may be exposed to hackers. They can be stored in hashed form and whenever a user logs in, a hash of entered password is computed and checked for equality. This is effective as it is not possible for recovering the original password by the hash.

2) Single sign-on (SSO)

SSO is an identity management technique where a user can be validated in a single log in and can then access other limited resources without a repeated authentication. Here, Authentication information is generated by using different programs in this method. SSO is a way to access an independent multiple software system where a user logs in to

a system and accesses all systems without a need to log in again to a program.

3) Public Key Infrastructure (PKI)

Old authentication systems are mainly based on a system using hidden key that supports traditional old asymmetric encryption algorithms, eg. RSA. Private key is used to confirm user identity. PKI has been adopted in the new design of security protocols like SSL/TSL and the use of SET mainly to provide authentication. Success of PKI depends on the control of access to the user's private keys similar to other encryption schemes. PKI should provide confidentiality, data comprehensiveness, strong authentication, and undesirability

B. Data Confidentiality

Cryptography algorithms are the efficient tool to ensure the security of data storage in the cloud. Indeed, there are many encryption algorithms that can encrypt the data and convert them into incomprehensible format, in order to ensure their confidentiality. These algorithms are divided into two categories: symmetric and asymmetric key.

1) Asymmetric Techniques:

The asymmetric key techniques performance is very slow, and used in general to exchange the keys of symmetric key algorithms

2) Symmetric Techniques:

The symmetric key algorithms are a one form of encryption that use same key to encrypt and decrypt the data, and which are divided into block ciphers and stream ciphers. The input of block cipher when the data is encrypted or decrypted is in block of the fixed data size. In this section, we mainly focus on symmetric key algorithms which can be adopted by cloud providers to ensure the confidentiality of the data storage [5]. The table below (fig. 2) presents the some popular symmetric key algorithms:

Algorithms	Cipher type	Key Size	Algorithm Structure	Attacks
DES	Block (64 bits)	56 bits	Fiestel Network	Brute force attack
3DES	Block (64 bits)	K1,k2,k3 168 bits	Fiestel Network	Theoretically possible
RC4	Stream	8- 2048 bits	Fiestel Network	Fluhrer mantin and shamir attack
Blowfish	Block (64 bits)	32-448 bits (128 by default)	Fiestel Network	Differential Attack , Weak key
AES	Block (128, 192 or 256 bits)	128,192 or 256 bits	Substitution Permutation Network	Side channel attacks
Twofish	Block (128 bits)	128, 192 or 256 bits	Fiestel Network	Truncated differential cryptanalysis

Fig. 2: Symmetric key Algorithms

C. Confidentiality of Data Storage and Data Treatments

In an unsafe environment like the public cloud, highly sensitive data must be secured. Regarding the storage service, data can be encrypted before sending them to the cloud server, using the symmetric key cryptosystems such as: Blowfish, etc. But, to ensure the confidentiality of data storage and their treatments, the cloud providers must adopt techniques that can ensure the confidentiality of this type of service. Indeed, researchers stressed a useful encryption technique in this type of environment: Homomorphic Encryption (HE). This technique enables to confirm the confidentiality of data storage and their treatments, located in cloud servers The Homomorphic Encryption cryptosystems are asymmetric key, which use different keys for data encryption and decryption. In this section, we will define first Homomorphic Encryption technique and secondly introduce different operations types.

IV. Data Integrity

A. Homomorphic linear Authentication (HLA) - Based Solution Algorithm

HLA which allows TPA to perform auditing without requesting for user data. It reduces communication & computation overhead [16]. In this, HLA with random masking protocol is used which does not permit TPA to learn data content HLA Based Solution. It supports effective way of public auditing without retrieving data block. It is aggregated and required constant bandwidth. HLA has potential to compute an aggregate HLA which authenticates a linear combination of distinct data blocks.

B. MAC-Based Solution Algorithm

It is used to authenticate the data. In this, user upload data blocks and MAC to CS provide its secret key SK to TPA.[17] The TPA will randomly retrieve data blocks & Mac uses secret key to checked rightness of stored data on the cloud.

Problems with this system are listed below as:

1) It introduces added online burden to users due to limited use (i.e. Bounded usage) and stateful verification.
2) Communication & computation complexity
3) TPA requires knowledge of data blocks for verification
4) Limitation on data files to be audited as secret keys are fixed
5) After usages of all possible secret keys, the user has to download all the data to recomputed MAC & republish it on CS.
6) TPA should maintain & update states for TPA which is very difficult
7) It supports only for static data not for dynamic data.

C. Privacy Preserving Public Auditing Proposed by Cong Wang (Third Party Based)

Public auditing lets Third Party Auditor and user to check the integrity of the outsourced data stored on a cloud & Privacy Preserving allows TPA to do auditing without requesting for local copy of the data.

Through this scheme [14], TPA can audit the data and cloud data privacy is maintained. It contains 4 algorithms as

1) Keygen

It is a key generation algorithm used by the user to set up the scheme.

2) Singen

It is used by the user to generate verification metadata which may include digital signature.

3) GenProof

It is used by CS to generate a proof of data storage correctness.

4) Verifyproof

Used by TPA to audit the proofs It is divided into two parts as setup phase and audit phase.

a) Setup Phase

Public and secret parameters are initialized by using keygen and data files f are preprocessed by using singen to generate verification metadata at CS & delete its local copy. In preprocessing user can alter data files F.

b) Audit Phase

TPA generates an audit message to CS. The CS will derive a response message by executing Genproof. TPA validates the response using F and its verification metadata.

TPA is stateless i.e. no necessity to maintain or update the state information of audit phase. Public key based homomorphic linear authentication with random masking method is used to achieve privacy preserving public auditing. TPA checks the integrity of the outsourced data stored on a cloud without retrieving actual contents. Existing research work of proof of retrievability (PoR) [15] or Proofs of Data Possession (PDP) technique doesn't consider data privacy problem. PDP scheme first proposed by Ateniese et al. used to identify large amount corruption in outsourced data. For auditing the cloud data and randomly sample a few blocks uses the RSA based Homomorphic authentication.A Second technique proposed by Juels as Proofs of retrievability (PoR) allows user to retrieve files without any data loss or corruptions. It uses spot checking & error correcting codes are used to ensure both "Possession" and "Retrievability". To achieve Zero knowledge privacy, researcher [14] proposed Aggregatable Signature Based Broadcast (ASBB). It provides completeness, privacy and soundness. It uses three algorithms as Keygen, Gentag and Audit.

D. Boneh–Lynn–Shacham

The BLS system uses bilinear pairing for verification, and signatures are grouped under an elliptic curve. It's an undeniable signature scheme that helps users verify that a signer is trusted. Furthermore, it can work with any scheme in gap Diffie–Hellman (GDH) group G. [11]The arrangement requires a hash function derived from the message space on G This scheme can also be utilized in cloud-auditing techniques. Let G = of the GDH group of prime order p, with hash function H: {0, 1}*G, be considered as a random oracle. Any block of data can be encrypted using the following algorithm:[11]

- Key generation will be executed by the cloud client. Select a random variable, x←Zp and compute v¬ gx. The public and private keys are vG and xZp, respectively.
- Signing uses a private key and message M {0, 1}*, determined as h ¬ H(M), where hash value h G and s ¬hx.
- Verification computes h ¬ H(M) from a public key x, a block of data, and a signature. Hence, (g,v, h, s) is verified as a valid tuple.

These schemes are further extended to support dynamic data as well as public auditability. The Merkle hash tree is one scheme that achieves these goals. Based on the binary tree concept, its leaves are hashes of authenticated data values, as Qian Wang and his colleagues discuss. [12] In the sense that it audits dynamic data, this work extends that of Ateniese and his colleagues[13] and Ari Juels and Burton Kaliski,[12] who considered signatures with respective file indexes. Hence, once a file is updated, its previous file indexes should also be recomputed. To reduce the overhead of keeping an index of files, Qian Wang and his colleagues discarded the index information for files and created tags for each data block to support data dynamics.

E. Elliptic curve cryptography [9]

When talking about the application of ECC to cloud computing, Tirthani and Ganesan [10] propose a simple architecture based on the Diffie-Hellman Key Exchange and Elliptic Curve Cryptography to make a cloud system secure. In this section we present their proposed architecture for a client/cloud server system, which uses a four step procedure that consists of connection establishment, account creation, authentication and data exchange.

Establishing the connection to the remote system and the creation of an account for a first-time user consists of the two first steps. When a new user tries to access the system for the first time, a new initial connection can be made by means of HTTPS and SSL protocols. During this process, the remote cloud server will generate a unique user ID and the public/private key pair necessary for Elliptic Curve Cryptography encryption.

The third step is authenticating a user that logs on to the system. This is done by requiring the user to provide the user ID that was created initially during account creation process mentioned above.

In the final step, the data exchange, is done by using the Diffie-Hellman key exchange protocol. When the client user wants to retrieve data from the remote server, the client's fired query is stored in a special file which is encrypted with the remote server's public key and the client user's private key. The encrypted file is then sent to the remote server, where the file is then decrypted by using the remote server's private key to retrieve and process the client fired query. Thereafter, the server encrypts the resulting data with the server's private key and the client's public key, and sends this back to the requesting client who can retrieve the queried data returned by server by decrypting the package with his/her own generated private key.

V. ACCESS CONTROL [7]

Access Control allows an application to trust another application's identity. The traditional model for this is application-centric, where each application tracks its own collection of users and manages them, but it is not feasible in cloud based architectures. Because here, we need a lot of memory for storing the user details such as username and password. Therefore cloud needs to have a user-centric access control mechanism so that each user request to a remote service provider will be packed with the user identity and entitlement information.

The main types of access control models are [7],

- Mandatory Access Control (MAC)
- Discretionary Access Control (DAC)
- Role Based Access Control (RBAC)

1) Mandatory access control (MAC) is a security strategy that restricts the ability individual resource owners can deny or grant access to resource objects in a remote cloud file system. MAC criteria are defined by the cloud/server

system administrator, strictly enforced with the help of operating system (OS) or kernel security, and are unable to be altered by end users.

2) In cloud security,[8] Discretionary Access Control (DAC) is a type of access control in which a user possesses complete control over all the programs it executes and owns, and also is able to determine the permissions other users can have to those files and programs. Because DAC requires permissions to those who need access to be assigned explicitly, DAC is commonly referred to as a "need-to-know" access model.
3) In cloud systems security, Role-Based Access Control (RBAC) is an approach to restricting system access to authorized users. It is used by the majority of enterprises with more than 500 employees, and can implement mandatory access control (MAC) or discretionary access control (DAC).

VI. CONCLUSION

The main goal of this work is to list the security techniques for data protection, data integrity, access control and authentication in the cloud computing scenario. For that purpose we listed the most important security techniques for data protection that are already accepted from the cloud computing providers. Apart from this, the most popular (and secure) techniques from the 4 sections are:

- Authentication: Sinsle Sign On (SSO)
- Confidentiality: 3DES
- Integrity: Privacy Preserving Cloud Auditing
- Access Control: Role Based Access Control

We classified them in four sections according to the security mechanisms that they provide: authentication, confidentiality, access control and Integrity.

REFERENCES

[1] Kashyap, Ria, Shikha. "Survey on Privacy Preserving Cloud Auditing For Shared Data", International Journal Of Engineering Sciences and Research Technology 6(2), (February 2017):22-27
[2] Jakimoski, Kir-e. "Security Techniques for Data Protection in Cloud Computing.", International Journal of Grid and Distributed Computing 9.1 (2016): 49-56.
[3] https://www.slideshare.net/ronak2454/issues- in-cloud-computing-9710875
[4] Dejamfar, Najafzadeh. "Authentication Techniques in Cloud Computing: A Review", International Journal of Advanced Research in Computer Science and Software Engineering, (January 2017): 95-99
[5] Khalid El Makkaoui,Abdellah ezzati, Abderrahim Beni-Hssane, Cina Motamed:"Data Confidentiality in the world of Cloud" in 29 february 2016 vol 84 No 3
[6] K. Sathish 1 , Y. Jansi, M.Tech2 , Dr. M. GiriMulti-User Setting For Dynamic Data Invocation for Privacy Preserving In Public Cloud Storage, M.Tech,Ph.D 3 in IOSR Journal of Computer Engineering (IOSR-JCE)
[7] Onanakunju, "Access Control In Cloud Computing" International Journal of Scientific and Research Publications, Volume 3, Issue 9, September 2013.
[8] http://www.webopedia.com/TERM/D/Discreti onary_Access_Control.html
[9] Gopinathan, Nygard, Aune "Elliptic curve cryptography in cloud computing security", Koclab, December 2015.
[10] Tirthani, Ganesan: Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography. Web: https://eprint .iacr.org/2014/ 049.pdf. 2014.
[11] A. Juels and B.S. Kaliski Jr., "PORs: Proofs of Retrievability for Large Files," Proc. 14th ACM Conf. Computer and Communications Security, 2007, pp. 584–597.
[12] Q. Wang et al., "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 5, 2011, pp. 847–859.
[13] G. Ateniese et al., "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Communications Security (CCS 07), 2007, pp. 598–609
[14] D. Boneh et al., "A Survey of Two Signature Aggregation Techniques," RSA CryptoBytes, vol. 6, no. 2, 2003, pp. 1–10.
[15] D. Boneh, B. Lynn, and H. Shacham, "Short Signatures from the Weil Pairing," Proc. 7th Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT 01), 2001, pp. 514–532.
[16] Bowen, Janine Anthony. (2011). Cloud Computing: Issues in Data Privacy/Security and Commercial Considerations. Computer and Internet Lawyer Trade Journal. 28 (8), 8.
[17] Jun Tang, Yong Cui (2016). "Ensuring Security and Privacy Preservation for Cloud Data Services" (PDF). ACM Computing Surveys.

