A Survey of Encryption Techniques and Security Issues in Cloud Computing

K. Uma*, Thanooj S
Department of IT, VIT University,vellore-632 014, India
***Corresponding author: E-Mail: drumakphd@gmail.com**

ABSTRACT

Cloud computing is now seen as the next generation architecture of IT enterprise. The cloud computing hypothesis, the advantages and its potential for diminishing costs and reducing the time for a deal that favours towards the security issues. Cloud Computing is also an aggregation of IT services that is offered to the customers based on leasing. Though a large number of security issues are addressed, still some are not addressed and several algorithms are proposed for security issues. Clouds are extraordinarily complex systems. They can be condensed to plain primitives, that ca be replicated thousands of times, and universal functional units. The intricacy of cloud computing produce many issues connected to security as well as all the aspects of Cloud computing. One of the key issues is data security. Since Clouds characteristically have single security architecture but has numerous customers with diverse demands. This paper presents a strong view on cloud computing technologies, vital features, classifications, delivery models and different encryption mechanisms. A relative study made on numerous encryption techniques are used for maintaining the discretion of data in the cloud. Finally, the most important data security issues present in cloud computing are discussed.

KEY WORDS: Cloud Computing, Encryption Techniques, Classification, Data security, Authentication, Security in Cloud.

1. INTRODUCTION

Cloud Computing is a combination of IT services provided by many service providers. The term cloud was originated from the internet and is also a platform that gives people the opportunity for sharing resources, services and information globally. In general, cloud computing has diverse definitions obtained by several important organizations. The National Institute of Standard and Technology (NIST) defines cloud computing as “a model for enabling expedient, on demand network access to a shared pool of configurable computing resources that can be swiftly provisioned and released with very less management effort or service provider interaction”. Users will not know where the information will be stored in the cloud. Most of the users only care about the privacy of their information. Privacy is the important constraint in all cases of deployment. Privacy/ Confidentiality can be categorized into two types, i.e. weak confidentiality and strong confidentiality. In weak confidentiality only authorized users and cloud providers get the meaningful data from cloud storage (Mell, 2011).

Strong confidentiality means cloud providers will not be able to access the data. For example confidential and classified business information, government secret information, etc. Applications that execute in the cloud can poise several factors including load balancing, bandwidth, size of data and security. One of the key obstacles to cloud approval is data security and privacy, because the user and the service provider are not contained in the same trusted domain. Security issues are increasingly significant in lower layer Infrastructure as a Service (IaaS) to higher Platform as a Service (PaaS). These cloud layers are deployed (public, private, community, and hybrid) in high end MCC (Mobile Cloud Computing). Users vacillate to shift into the cloud because of certain ambiguities in its architecture that makes cloud computing insecure (Anwar, 2013).

Essential Characteristics of Cloud Computing

On-demand Self Service: The consumers of cloud will expect on demand services from the cloud environment. Self-service access must be allowed by the service provider according to their request. So that consumers can appeal personalized, pay and use services without the intrusion of human operators (Maneesha Sharma, 2012).

Broad Network Access: The resources from cloud are internationally available and accessed through a standard benchmark mechanism that endorses the customer by a heterogeneous platform.

Resource Pooling: The resources are pooled together by the providers and grant services to multiple clients by means of multiple tenant models.

Rapid Elasticity: The cloud will be scalable and flexible to suit consumer business needs. Customers can simply add or eliminate users, resources, software features, etc.

Measured Service: The resource usage of cloud computing can be measured, controlled and also provides transparency to the provider and also to the consumer of the utilized service.

Classification Of Cloud Computing: Depending on the consumer service and their usage, the cloud can be categorised as public, private, community, and hybrid (Krogstie, 2012).

Public Cloud: Public or the external cloud infrastructure is available and can be accessed by the general owned by an organization for selling cloud services on pay and use basis. For example Windows Azure services platform, Google App Engine, etc.

Private Cloud: Private or internal cloud infrastructure is managed, maintained and controlled by a single group or organization. For example Sun Cloud, IBM Blue clouds, Google App Engine, etc.

Community cloud: Community cloud is a different type of private cloud. The infrastructure of the cloud is shared by a number of organizations, characteristically with mutual concerns. It may be maintained and controlled by a cluster of organizations or by a third party premise.

Hybrid Cloud: The cloud infrastructure might consist of two or more public, private or community clouds. The idea of hybrid cloud is to offer extra services and resources to consumers to handle their demands (Wan, 2012).

Encryption Techniques for Data Security in Cloud: Encryption Techniques are used for protecting the sensitive information. They are classified into two different techniques that are used commonly. The Symmetric Key Encryption makes use of a Single key that is implicated in data security. The same key is used by both the sender and the receiver to encrypt and decrypt. The Asymmetric Key Encryption involves two different keys. The receiver acquires a secret key which is private whereas the other key is public and is available to everyone. Usually, the Classical Encryption algorithms are categorized into two principles:

- Substitution Cipher (replaces a character with another)
- Transposition Cipher (transposes the characters).

The Homomorphic encryption theory originates from mysterious world of abstract algebra. The word Homomorphic means same shape or same effect on two unlike sets of objects can be transformed (Balamurugan, 2014).

The Fully Homomorphic Encryption (FHE) explains that there are no boundaries on what manipulations can be performed. The following section analyses the various symmetric encryption techniques, which effectively handle large amount of data.

Attribute Based Encryption (ABE): ABE is a public key cryptography technique that uses one-to-many encryption. ABE uses attributes as identities for both encryption and decryption of data. The cipher text and the user's private key depend on attributes. If the features of a user key counterpart to those of the cipher text, then decryption is permitted. For instance, assume that there are three features {std, fac, cs} and that the threshold value is 3, then the private key will need at least three descriptive features to decrypt data. This idea was first anticipated by Sahai and Waters to deliver fine-grained admittance control, scalability, and flexibility in access control mechanisms in the cloud. ABE utilizes four algorithms: encryption, decryption, setup and key generation. Their limitations are as follows:

- The threshold value lacks an express ability
- Diverse categories of consumers create a computational overhead.

Hierarchical Identity-Based Encryption (HIBE): HIBE is a protracted form of IBE. In ordered identity-based encryption patterns, each private key is circulated by a single private key originator, and public keys are their Primitive ID (PID), which is also called 1- HIBE. One of the dynamic shortcomings of this procedure is its vital management overhead. To minimalize this, a 2-HIBE pattern was introduced that provided a accurate definition of the privacy. The 2-HIBE pattern consists of a domain Private Key Generator (PKG), a root PKG, and users, all of which are associated with an indiscriminate string of PID. A user's public key is the mixture of PID and domain PID, which is also called address. The domain PKG can calculate any private user key from users' domain, provided they have previously requested their domain secret key from the root PKG. The cryptosystem includes a root certificate authority called a trusted third party that allows a hierarchy of certificates. HIBE can ominously shrink the workload on the root server (Sarvesh Kumar, 2013).

Hierarchical Attribute-Based Encryption (HABE): The HABE pattern was idealized by Wan et al. This scheme compromises fine-grained access control, scalability and full delegation by combining the features of HIBE and CP-ABE. HABE works in a dynamic division fashion and shoulders all attributes in one conjunctive item and are directed by the same domain chief. Fig.1 shows a three level HABE. The limitations of HABE are stated below:

- Even though the same feature is directed by multiple domain chiefs, it is problematic to implement in practice.
- It cannot proficiently sustain compound features.
- The multiple-value assignments are not supported.

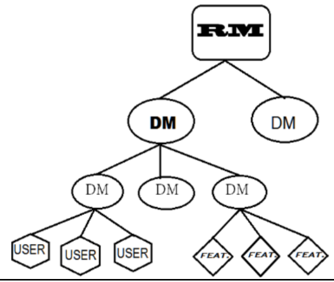

Figure.1. Three level HABE

Fully Homomorphic Encryption: We have projected an application of a technique to implement actions on encrypted data without decrypting them, which will deliver us with the same outcomes after the computations as if the authors have operated directly on the raw data. Homomorphic Encryption method is able to perform operations on encrypted data without decrypting. Homomorphic Encryption schemes are used to accomplish actions on encrypted data without the Secret Key; the client is the only owner of the private key. We have also proposed a Fully Homomorphic Encryption (FHE) that allows a user who does not have the private decryption key to compute any outcome of the data. The technique the author focussed is based on a FHE algorithm with key designation to ensure data secrecy, verification, reliability and accessibility of multi-level hierarchical order. Their projected framework solution is the using of homomorphic cryptography with Attribute Based Encryption.

Cloud Data Encryption Standard DES Algorithm: The DES algorithm ensures data security in cloud. The security design architecture of the system is planned by using DES cipher block chaining, which eradicates the hackers. The data which is sent, being interrupted and replaced has no danger. The system with encryption is adequately secure but for that, the level of encryption has to be amplified, as computing power upsurges. To secure the results, a symmetric key is used to encrypt the communication system between the modules. The cloud data security must be utilized to analyse the data security requirements, the data security risk, the data security process through encryption and disposition of security functions.

This encryption algorithm is used to address the security and privacy issues in cloud storage to shield the data from illicit access. The anticipated technique is converting plain text into the equivalent ASCII code value of each alphabet and the key value varies between 1 to 256. This method improves orthodox encryption techniques by assimilating substitution cipher and transposition cipher. Symmetric encryption has the promptness and computational effectiveness to handle encryption of great volumes of data files in cloud storage. This algorithm is used to encrypt the user data in cloud storage and it can’t be accessed by administrators or attackers (Cecil A Donald, 2014).

Data Security Issues In Cloud Computing

Data Authentication: Any user can access the LAN by feeding a cloud identification and password, which may be acknowledged by a cloud verification mechanism. If the authentication mechanism validates the certification, the user identification and password are stored locally for subsequent authentication requests. The authentication mechanism may be distributed in both domain and Workgroup LAN and may function simultaneously with other users who may have a LAN or client authorizations which may not be authenticated from the cloud (Mell, 2009).

Data Integrity: Data Integrity emphasizes on complete and consistent data. The cloud data might suffer damages due to data integration. The client must be made sure by the cloud service provider that they are aware of what data that is outsourced in the cloud, the native and the integrity mechanisms put in place (Ning, 2015).

Data Privacy and Confidentiality: The clients must be assured that the data outsourced by them into the cloud must be accessed only by the authorized users. Securing the customers data is the key role of the cloud computing service provider and make sure that the customer’s personal data is well protected from other service providers and users. The best solution for data privacy is authentication because the service provider must make sure who is accessing the data and also who is maintaining the server, so that the customer’s private data is sheltered. The cloud consumer must be assured that data stored in the cloud will be classified.

Data Location: The exact location and methodology used for storing the data in the cloud remains quite anonymous to most of the cloud users, in fact they also don’t know where the data will be hosted. This requires a special contractual agreement and contract between the users that the data must stay in a particular location.

Data Storage, Backup and Recovery: The cloud consumers who choose to move their data to the cloud provider should make sure adequate resilience storage systems. The process of improving and backing up data is simplified. The cloud providers will store the data in a distributed fashion i.e. several places across many free and independent servers (Shamir, 1985; Sugumaran, 2014).

Data Availability:_Data provided by the consumer is usually stored in different servers frequently placing in different locations or in different clouds. Data availability and accessibility becomes a key legal issue due to the availability of corrupted and relatively difficult servers (Xiaojun, 2010).

4. CONCLUSION

Attribute Based Encryption is an extensively used technique for access control in cloud computing. The main advantage of ABE is that it gives users access to stronger encryption and allows key strength distribution. This paper has analyzed several different ABE techniques and categories, and reviewed their functionality and limitations. That is why it is the most commonly used encryption algorithm in cloud computing.

We extended the survey to weighted attribute based encryption techniques that perform better by offering fine-grained access control. Cloud computing is a versatile technology, widely studied in recent years. The providers and the clients must make sure that the cloud is safe from all the internal threats, external threats and mutual understanding between the customer and provider when it comes to the security of cloud. The major issues in cloud computing is data security and it has many aspects like confidentiality, surveillance, integrity, availability, anonymity, reliability, security, telecommunications capacity, government and backup & recovery. But the most important issue in data security is privacy and security for shielding and protecting the data in cloud storage.

This paper analyses the importance of the data security in the cloud. Reason for choosing symmetric encryption algorithms are efficient to handle encryption for large amount of data, and effective speed of storing data in the cloud.

REFERENCES

Anwar J, Alzaid, Eng, Jassim M, Albazzaz, Cloud Computing, An Overview, International Journal of Advanced Research in Computer and Communication Engineering, 2(9), 2013.

Balamurugan B and Venkata Krishna P, Extensive survey on usage of attribute based encryption in cloud, Journal of Emerging Technologies in Web Intelligence, 6(3), 2014, 263–272.

Cecil A Donald and Arockiam L, Article, Securing Data with Authentication in Mobile Cloud Environment, Methods, Models and Issues, International Journal of Computer Applications, Published by Foundation of Computer Science, New York, USA, 94(1), 2014, 25-29.

John W, Rittinghouse James F, Ransome, Cloud Computing Implementation, Management, and Security, CRC Press, 2010.

Krogstie J, Model-Based Development and Evolution of Information Systems, a Quality Approach. Springer, 2012.

Maneesha Sharma, Himani Bansal, Amit Kumar Sharma, Cloud Computing, Different Approach & Security Challenges, International Journal of Soft Computing and Engineering (IJSCE), 2(1), 2012.

Mell P and Grance T, Cloud computing definition, NIST, 2009

Mell P and Grance T, The NIST Definition of Cloud Computing, 2011.

Ning H and Liu H, Cyber-physical-social-thinking space based science and technology framework for the Internet of Things, SCIENCE CHINA Information Sciences, 58(3), 2015, 1–19.

Sarvesh Kumar, Jahangeer Ali, Ashish Bhagat, Jinendran P.K, An Approach to Creating a Private Cloud for Universities and Security Issues in Private Cloud, International Journal of Advanced Computing, 36(1), 2013.

Shamir, Identity-based cryptosystems and signature schemes, in Advances in Cryptology, Blakley G.R and Chaum D, eds. Springer Berlin Heidelberg, 1985.

Sugumaran, BalaMurugan B, Kamalraj D, An Architecture for Data Security in Cloud Computing, IEEE World Congress on Computing and Communication Technologies, 2014.

Wan Z, Liu J.E and Deng R.H, A hierarchical attribute based solution for flexible and scalable access control, IEEE Transactions on Information Forensics and Security, 7(2), 2012, 743–754.

Xiaojun Y, Qiaoyan Wen, a View about Cloud Data Security from Data Life Cycle, IEEE, 2010.