ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 6, June 2018

A Framework to Achieve Data Security and Privacy in Cloud Computing

Nivedita Tamrakar[1], Prof. Rajendra Arakh[2], Prof. Sumit Nema[3]

M.Tech Student, Department of Computer Science Engineering, Global Engineering College, Jabalpur, Madhya Pradesh, India[1]

Assistant Professor, Department of Computer Engineering, Global Engineering College, Jabalpur, Madhya Pradesh, India[2]

Assistant Professor and Head of The Department, Department of Computer Science Engineering, Global Engineering College, Jabalpur, Madhya Pradesh, India[3]

ABSTRACT: Ensuring about the security and privacy of stored data in cloud servers is one of the most challenging issues that decrease the rate of reliability in cloud computing environments. Applying cryptography algorithms is the most common solution to enhance the reliability of cloud servers and to protect resources from possible attacks and un-predictable events. However, the security of this type of protection is affected when some users are revoked by data owner from accessing to data. Hence, an efficient and reliable re-encryption model based on multi-level cryptography has been introduced in this paper to prevent un-authorized accesses from revoked users to cloudbased resources. The main aim of the proposed model is to classify data to several levels for managing the process of reencryption more efficient and reliable. Therefore, 3 levels of security have been defined to carry out this classification according to the security characteristics of stored data: TimeBased Level, High Risk Level, and Custom Level. The presented model has been evaluated according to three parameters: performance, security, and scalability. The evaluation process was done by establishing a simulated environment to investigate functionality of re-encryption procedure in each level of security. Functionality and security analysis of this model shows that, the reliability and efficiency of data protection process in cloud computing environments is improved considerably by using 3- level re-encryption model.

KEYWORDS: Cloud Computing, Re-Encryption, Security, Data Classification, Cryptography.

I. INTRODUCTION

Cloud Computing is evolving as a key technology to store and share resources via a broad network (i.e. Internet) by using emerging tools and concepts such as virtualization, processing power, storage, and connectivity [1]. The rapid growth of using cloud –based services to store resources (e.g. data, applications, etc.) and to deploy on-demand software, is an undeniable fact that have attracted attentions of IT service providers, enterprises and users to this emerging technology [2]. Despite the considerable benefits of cloud computing environments, such as quick responds, lower installation, maintenance and upgrade costs, automatic software integration and unlimited storage [3], there are some significant concerns for users to use cloud-based services. Ensuring about the security and privacy of stored data in cloud servers is one of the most challenging issues that decrease the rate of reliability in cloud computing environments. Typically, security issues in cloud-based environments are appeared regarding to weaknesses in three main levels: service providers, infrastructure, and end-user. The most important security issue that affects all of these levels is data protection. When users outsource sensitive data shared on cloud servers, many challenges crop up on data security and access control. Applying cryptography algorithms is the most common solution to enhance the reliability of cloud servers and to protect resources from possible attacks and un-predictable events [4]. However, the security of this type of protection is affected when some users are revoked by data owner from accessing to data. Therefore, a re-

DOI: 10.15680/IJIRCCE.2018.0606065

encryption model has been presented in this paper to prevent un-authorized accesses from revoked users to cloud-based resources.

II. SECURITY ISSUES IN THE CLOUD DEPLOYMENT MODELS

The three deployment models are private cloud, public cloud and hybrid cloud. The security issues of these deployment models are discussed below [6].

A. Security issues in a public cloud

In a public cloud model, the platform and infrastructure are shared among customers. The securities for these services are provided by the cloud service provider. A few of the key security issues in a public cloud include:

1) Since there is no control over the security mechanisms used by the cloud service provider, it is difficult to protect data in all its stages providing the basic requirements of confidentiality, integrity and authenticity

2) Since most service providers use a multitenant architecture, the possibility of data leakage between the tenants is very high

3) If the Cloud service provider uses a Third Party vendor for providing the services, then there is added overhead of verifying the agreements and contingency plans between them.

4) There is also a possibility of an insider attack at the service provider side. As the cloud architecture grows the number of insiders grow. Proper laws should be enforced to protect data from malicious insiders.

B. Security issues in a private cloud

A private cloud model enables the customer to have local network and storage space. They provide the flexibility to the customer to implement any kind of required services. There are certain securities issues:

1) Due to virtualization, unauthenticated and unauthorized access to system is possible

2) Malware can be used to attack the host operating system

3) In order to protect from diverse HTTP request the access point of users to access the infrastructure must be protected with standard security techniques.

4) Security policies must be designed to protect attacks from insiders.

The hybrid cloud model is a combination of both public and private cloud and hence the security issues discussed with respect to both are applicable in case of hybrid cloud model. Each of the three ways in which cloud services can be deployed has its own advantages and limitations. And from the security perspective, all the three have got certain areas that need to be addressed with a specific strategy to avoid them [6].

III. SECURITY MECHANISM IN PUBLIC CLOUD

Despite of increased hacking of data in public cloud, data security in public cloud can be achieved with the use of high-quality cloud security. The three issues need to be addressed to provide security in cloud computing are: Availability, Confidentiality and Integrity known as the ACI triad [3].

1) Availability

Availability is a mechanism by which data will be available to the user in a manner irrespective of location of the user. It can be achieved by providing authentication and network security.

2) Integrity

Integrity provides security to data in the means that the data sent and the data received is always the same and it cannot be changed while transmitting. Integrity will be affected if the data gets affected. It can be achieved by using firewalls and intrusion detection.

3) Confidentiality

Confidentiality is a way to avoid unauthorized expose of user data to the unauthorized user. Providing security protocols and data encryption services confidentiality can be achieved.

Client's data in the cloud can be accessed by other clients. So there arise security issues on client's data. To achieve security on cloud data many techniques and algorithms are available. Some of these are [4]:

Authorization practices – Provides authorization to clients, who can access data stored on cloud system.

Authentication processes - which creates a user name and password to access the data.

Encryption - A technique which uses complex algorithm to hide the original information with the help of encryption key.
Many of the techniques used in physical data centers have to be used in the cloud environment too. The best cloud service providers build these techniques into their clouds. Some of the security mechanisms used in public cloud:

Implicit storage security mechanisms use the scheme of data partitioning to store data in online. The data is simply partitioned and stored instead of encrypting the data. The data can be divided and stored on different servers on the network. The location of the data where it is stored will be known only to the user. In order to obtain the data back for use, the user has to have the knowledge about where data is residing. There are several different mechanisms available for storing data online, one of which is to store the encryption key. The access to all the servers is given only to the user thus providing more security. It involves the roots of a polynomial in finite field.

A. Security for Implicit Data Storage in Online[5]

Implicit storage security mechanisms use the scheme of data partitioning to store data in online. The data is simply partitioned and stored instead of encrypting the data. The data can be divided and stored on different servers on the network. The location of the data where it is stored will be known only to the user.
In order to obtain the data back for use, the user has to have the knowledge about where data is residing. There are several different mechanisms available for storing data online, one of which is to store the encryption key. The access to all the servers is given only to the user thus providing more security. It involves the roots of a polynomial in finite field.

B. Dynamically Storage in Cloud [5]

A Flexible Distributed Storage Integrity Auditing Mechanism (FDSIAM) is a mechanism used to dynamically store data in cloud. It uses a protocol using the data reading protocol algorithm to check the data integrity. This mechanism uses homomorphism tokens, blocking erasure, unblocking factors and distributer erasure coded data. These concepts to provide secure data storage. It also used to check the data security provided by the service providers.

C. Identify –Based Authentication[5]

The security is provided with the help of private and public key pair without the need for certificates and deployment. The key is generated using the unique identity. The private key is generated using the public identity of each entity.
A identify based encryption (IBE) and Identity Based Signature (IBS) are used to provide authentication based on identity. When SSH Authentication Protocol (SAP) is a very complex and hence an alternative to SAP is a new authentication protocol based on identity. It is hierarchical model with particular signature and encryption scheme.

D. Third Party Auditing (TPA)[5]

The small and medium enterprise may have huge amount of data. It is difficult and expensive for those data owners to check for the data correctness in a cloud environment. A trusted auditing organization works in the between to provide secure storage to the cloud users.
To achieve data storage security, BLS (Bonch-Lynn- Sachems) algorithm is used to sign the data blocks before outsourcing data into cloud. Reed Solomon technique is used to provide error correction and to support data storage correction. It is homogeneous in nature.

E. Secure and Dependable Storage Service[5]

The storage service provides a way to store data which can be used later for well qualified applications. A distributed auditing mechanism is used for storage service by utilizing the homomorphism token and distributed coded-data. They help us to utilize the available data which has been stored without worrying about security concerns. The proposed system support efficient dynamic operation on outsource data which includes block modification, deletion and append.
trusted auditing organization works in the between to provide secure storage to the cloud users.
To achieve data storage security, BLS (Bonch-Lynn- Sachems) algorithm is used to sign the data blocks before outsourcing data into cloud. Reed Solomon technique is used to provide error correction and to support data storage correction. It is homogeneous in nature.

F. Secure and Dependable Storage Service[5]

The storage service provides a way to store data which can be used later for well qualified applications. A distributed auditing mechanism is used for storage service by utilizing the homomorphism token and distributed coded-data. They help us to utilize the available data which has been stored without worrying about security concerns. The proposed system support efficient dynamic operation on outsource data which includes block modification, deletion and append.
Both encryption and decryption requires encryption/decryption algorithm and a key (ki).
- Cryptographic algorithm is the mathematical function or functions used for encryption (E)/ decryption (D).
- A Key is a numeric or alpha numeric text or may be a special symbol. The selection of key in Cryptography is very important since the security of encryption algorithm depends directly on it.
- Cryptology is the science of both cryptography and cryptanalysis.
- Cryptographer is the person dealing with cryptography.
- Cryptanalyst is the person dealing with cryptanalysis.
- Attack is the cryptanalytic attempt.
- Cryptosystem is the system where an encryption/decryption process takes place.
- Steganography is the technique of hiding secret messages into innocuous messages, such that every secret message is hidden (invisible).

There are three types of techniques

1) Symmetric Key Cryptography – Private-key cryptography, also known as symmetric cryptography, a single key or private key is used for both encryption and decryption process. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data.

2) Asymmetric Key cryptography - Public-key cryptography, also known as asymmetric cryptography, requires two separate keys, one to encrypt the plaintext, and one decrypt the cipher text. One of these key is public and the other is kept private. Although, the two different parts of this key pair are mathematically linked.

3) Hash function Cryptography - The hash function cryptography (One way cryptography) offers a way of creating a fixed-size blocks of data by using entry data with variable length. It is also known as taking the digital fingerprint of the data, and the exit data are known as message digest or one- way encryption. If the data is modified after the hash function was generated, the second value of the hash function of the data will be different. Even the slightest alteration of the data like adding a comma into a text, will create huge differences between the hash values. The hash values solve the problem of the integrity of the messages.

Encryption algorithms review: A. Symmetric Encryption:

1) Blowfish [7]

Blowfish is a fast, compact and simple block size of 64 bits encryption algorithm with variable key length from 32 to 448 bits. It is a 16-roundFeistel cipher and uses large key dependent permutation in P-Box and substitution in S-Boxes. Each S-box contains 32 bits of data. This algorithm consists of two sub parts, one is key expansion part and the other is data encryption part. In which the key expansion part converts a key of at most 448 bits into 4168 bytes of sub keys and the data encryption is done by completing 16 rounds fiestel network which can be implemented on 32 or 64-bit microprocessor. This algorithm is suitable when the key is not changing frequently in any other applications.

Advantages:

1. Provides high level of security to cryptanalysis.
2. It is considerably faster than most encryption algorithms.

3. Blowfish is invulnerable against differential related- key attacks.

Limitations:
1. Blowfish has some classes of weak keys.
2. The reliability of Blowfish is questionable due to the large no. of weak keys.

2) Data Encryption Standard [8]

The Data Encryption Standard (DES) is a symmetric-key algorithm for the encryption of data. DES is a block cipher that enciphers 64-bit blocks of data with a 56-bit key. The remaining eight bits are used for checking parity. Decryption uses the same structure as encryption but with the keys used in reverse order.

Advantages:
1. The same hardware or software can be used in both directions.

Disadvantages:
1.Small key size which offers less security.
2.Its encryption speed which is very slow.

3.Advanced Encryption Standard [7]

AES is a symmetric key block cipher and is fast in both software and hardware. AES has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits with variable 10, 12, or 14 rounds. The AES algorithm holds a 4 by 4 array of bytes called the state, which is initialized to the input of 128 bits (i.e., 16 bytes) to the cipher. The substitution and permutation operations are all applied to the state array. There are four stages in every round of AES. It also contains a single S- box and same algorithm is used in reversed for decryption. Its symmetric and parallel structure provides great flexibility for implementers, with effective resistance against cryptanalytic attacks. AES can be implemented and well adapted on processors such as Pentium, RISC and parallel processors.

Advantages:
1.AES is compact cipher and it works fast by using variable key length.
2.It provides resistance against certain collision attacks.

Disadvantages:
1.AES has no serious weakness.
2.The mathematical property of the cipher might be vulnerable into an attack.

B. Asymmetric Encryption:

1) RSA [8]

RSA (stands for Rivest, Shamir Adleman) is a public-key cryptography and is widely used for secure data transmission. In RSA, one of the key can be shared with everyone and another key must be kept private. The public key consists of the modulus n and the public (or encryption) exponent e. The modulus n is the product of two large prime numbers p and q. The private key consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q, and φ(n) must also be kept secret because they can be used to calculate d . Anyone can use the public key to encrypt a message, but in some cases if the public key is large enough, only someone with knowledge of the prime factors can get the possible decode of the message. The decryption of message does not take excessive time to get the original text.

Advantages:
1.Its security is based on the difficulty of factoring large integers.
2.The RSA scheme can be used for security and authenticity.

Disadvantage:
1.Slow compared to existing encryption algorithms.

V. CONCLUSION

In this paper, a 3-level re-encryption model was presented to ensure data protection in cloud computing environments. In the proposed model data was classified to three main levels: Time-Based Level, High Risk Level, and Custom Level. This classification improved the efficiency of re-encryption process in stored data regarding to the characteristics and level of risk for a specific resource. Furthermore, the presented model was evaluated according to three parameters: performance, security, and scalability. The evaluation process was done by establishing a simulated environment to investigate functionality of re-encryption procedure in each level of security. In overall, the results showed that this re-encryption model met the objectives of this research to increase the rate of efficiency and security during the process of data protection in cloud computing environments.

REFERENCES

[1] P. Kalagiakos, and P. Karampelas, “Cloud Computing Learning,” in Proc. of 5th International Conference on Application of Information and Communication Technologies (AICT), Baku, 2011, pp. 1-4.

[2] F. Fatemi Moghaddam, A. Hakemi, N. Memari, and H. Latifi, “A Reliable E-Service Framework based on Cloud Computing Concepts for SaaS Applications,” in IEEE Conference on eLearning, e-Management and e-Services (IC3e), 2013, pp. 100– 104.

[3] F. Fatemi Moghaddam, I. Ghavam, Sh. Dabbaghi Varnosfaderani, and S. Mobedi, “A Client-Based User Authentication and Encryption Algorithm for Secure Accessing to Cloud Servers,” in Proc. of IEEE Student Conference on Research and Development (Scored), Putrajaya, Malaysia, 2013, pp. 175-180.

[4] F. Fatemi Moghaddam, O. Karimi, and M. T. Alrashdan, “A Comparative Study of Applying Real-Time Encryption in Cloud Computing Environments,” in 2nd International Conference on Cloud Networking (CloudNet), San Francisco, USA, 2013, pp. 185–189.

[5] J.M. Do, Y.J. Song, and N. Park, “Attribute Based Proxy Reencryption for Data Confidentiality in Cloud Computing Environments,” in Proc. of First ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering (CNSI), Jeju Island, South Korea, 2011, pp.248- 251.

[6] Q. Liu, C.C. Tan, J. Wu, and G. Wang, “Reliable Re-Encryption in Unreliable Clouds,” in Proc. of IEEE Global Telecommunications Conference (GLOBECOM), Houston, USA, 2011, pp.1-5.

[7] L. Xiong, and Z. Xu, “Re-Encryption Security Model Over Outsourced Cloud Data,” in Proc. of International Conference on Information and Network Security (ICINS), Beijing, China, 2013 , pp.1-5.

[8] P.K. Tysowski, and M.A. Hasan, “Hybrid Attribute- and ReEncryption-Based Key Management for Secure and Scalable Mobile Applications in Clouds,” IEEE Transactions on Cloud Computing, vol.1, no.2, pp.172-186, December 2013.

[9] C. Sur, Y. Park, S.U. Shin, K.H. Rhee and C. Seo, “CertificateBased Proxy Re-encryption for Public Cloud Storage,” in Proc. of Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), Taichung, 2013, pp. 159-166.

[10] J. Daemen, and V. Rijmen, “AES Proposal: Rijndael”. National Institute of Standards and Technology, p. 1-10. Apr 2001.

DOI: 10.15680/IJIRCCE.2018.0606065