© 2015 IJSRSET | Volume 1 | Issue 6 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

A Survey in Cloud Computing : Security Issues and Their Solutions

Chaitali Patel*, Disha sanghani
Department of Information Technology, Shantilal Shah Engineering College, Bhavnagar, Gujarat, India

ABSTRACT

In current scenario cloud computing is touching the moons. Cloud computing becomes today's hottest research area because of its ability to reduce cost of computing. Most of the companies and industries adopt cloud computing for their data storage and develop cloud computing applications. As cloud computing provide services through internet users concern more and more about security of their data stored on cloud. In this survey paper we discuss various security issues faced by cloud computing and their solution using different cryptographic algorithms based on different security parameters.

Keywords: Cloud Computing, Security, Cryptographic Algorithms

I. INTRODUCTION

A cloud is a type of parallel and distributed system consisting of a collection of interconnected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on Service Level Agreement (SLA) defining quality of service parameters under which the service is delivered [5]. Cloud Computing provides a way to store and access cloud data from anywhere by connecting the cloud application using internet. By choosing the cloud services the users are able to store their local data in the remote data server [2]. It satisfies the on-demand needs of the user. It facilitates the sharable resources "as-a-service" model. For the organization, the cloud offers data centers to move their data globally [12].

As many companies move their data to the cloud the data undergoes many changes and there are many challenges to overcome. To be effective, cloud data security depends on more than simply applying appropriate data security procedures and countermeasures. Computer based security measures mostly capitalizes on user authorization and authentication.

Cloud computing combines the data-sharing model and service statistical model. From a technical point of view, cloud computing has the following three basic characteristics [3]

- Hardware infrastructure architecture is based on the clusters, which is large-scale and low-cost. The infrastructure of cloud computing is composed of a large number of low-cost servers, and even the X86 server architecture. Through the strong performance, the traditional mainframe's prices are also very expensive.
- Collaborative development of the underlying services and the applications is to achieve maximum resource utilization. By this way, application's construction is improved. But for traditional computing model, applications to be complete dependent on the underlying service.
- The redundant problem among multiple low-cost servers is solved by the software method. Because of using a large number of low-cost servers, Failure between nodes cannot be ignored, so the issue of fault tolerance among nodes should be taken into account, when designing software [3]

Benefits

The following are some of the possible benefits for those who offer cloud computing-based services and applications:

- **Cost Savings** - Companies can reduce their capital expenditures and use operational expenditures for increasing their computing capabilities. This is a lower barrier to entry and also requires fewer in-house IT resources to provide system support.
- **Scalability/Flexibility** - Companies can start with a small deployment and grow to a large deployment fairly rapidly, and then scale back if necessary. Also, the flexibility of cloud computing allows companies to use extra resources at peak times, enabling them to satisfy consumer demands.
- **Reliability** - Services using multiple redundant sites can support business continuity and disaster recovery.
- **Maintenance** - Cloud service providers do the system maintenance, and access is through APIs that do not require application installations onto PCs, thus further reducing maintenance requirements.
- **Mobile Accessible** - Mobile workers have increased productivity due to systems accessible in an infrastructure available from anywhere.

This paper is organized as follows: section 2 describes various security issues faced by cloud service provider and users. Section 3 describes existing cryptographic algorithms used in cloud computing. In section 4 this cryptographic algorithms are compared. Conclusion and future work is described in section 5.

II. METHODS AND MATERIAL

A. Security in Cloud Computing

Cloud services are applications running somewhere in the Cloud Computing infrastructures through internal network or Internet [1]. For users, they don't know or care about the data where to be stored or services where to be provided. Confidentiality, Integrity, and Availability (CIA) are some security dimensions [4].As fast development of application of cloud computing and cloud storage, users concern more and more about security and privacy.

Security Issues in Cloud Computing

Confidentiality and privacy:

Confidentiality means keeping users' data secret in the Cloud systems. Once the client host data to the cloud there should be some guarantee that access to that data will only be limited to the authorized access. Inappropriate access to customer sensitive data by cloud personnel is another risk that can pose potential threat to cloud data. Assurances should be provided to the clients and proper practices and privacy policies and procedures should be in place to assure the cloud users of the data safety.

Data integrity:

Data integrity in the Cloud system means to preserve information integrity (i.e., not lost or modified by unauthorized users).[2]With providing the security of data, cloud service providers should implement mechanisms to ensure data integrity and be able to tell what happened to a certain dataset and at what point.

Data location and Relocation:

Cloud Computing offers a high degree of data mobility. Consumers do not always know the location of their data. However, when an enterprise has some sensitive data that is kept on a storage device in the Cloud, they may want to know the location of it. They may also wish to specify a preferred location (e.g. data to be kept in India). This, then, requires a contractual agreement, between the Cloud provider and the consumer that data should stay in a particular location or reside on a given known server.

Another issue is the movement of data from one location to another. Data is initially stored at an appropriate location decide by the Cloud provider. However, it is often moved from one place to another.

Data Availability:

The goal of availability for Cloud Computing systems (including applications and its infrastructures) is to ensure its users can use them at any time, at any place.

Customer data is normally stored in chunk on different servers often residing in different locations or in different Clouds. In this case, data availability becomes a major legitimate issue as the availability of uninterruptible and seamless provision becomes relatively difficult.

Storage, Backup and Recovery:

When you decide to move your data to the cloud the cloud provider should ensure adequate data resilience storage systems. At a minimum they should be able to provide RAID (Redundant Array of Independent Disks) storage systems although most cloud providers will store the data in multiple copies across many independent servers. In addition to that, most cloud providers should be able to provide options on backup services which are certainly important for those businesses that run cloud based applications so that in the event of a serious hardware failure they can roll back to an earlier state.

B. Solution: Analysis of Existing Cryptographic Algorithms

Fig 1 shows some of the symmetric & asymmetric algorithms [6].

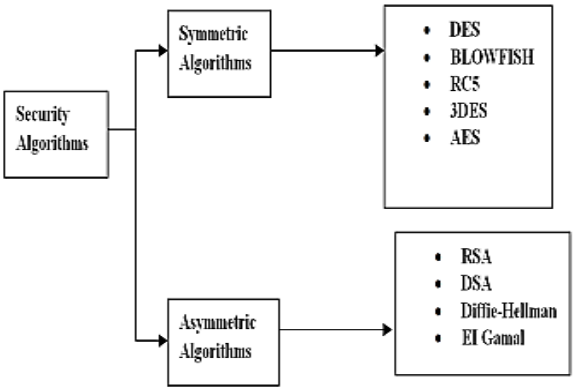

Figure 1: Existing Security Algorithms

Symmetric Algorithms:

DES: This stands for Data Encryption Standard and it was developed in 1977. It was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology). DES is 64 bits key size with 64 bits block size. Since that time, many attacks and methods have witnessed weaknesses of DES, which made it an insecure block cipher [7].

BLOWFISH: This was developed in 1993. It is one of the most common public algorithms provided by Bruce Schneider. Blowfish is a variable length key, 64-bit block cipher. No attack is known to be successful against this. Various experiments and research analysis proved the superiority of Blowfish algorithm over other algorithms in terms of the processing time. Blowfish is the better than other algorithms in throughput and power consumption [8].

3-DES: This was developed in 1998 as an enhancement of DES. In this standard the encryption method is similar to the one in original DES but applied 3 times to increase the encryption level. But it is a known fact that 3DES is slower than other block cipher methods. This is an enhancement of DES and it is 64 bit block size with 192 bits key size. 3DES has low performance in terms of power consumption and throughput when compared with DES. It requires always more time than DES because of its triple phase encryption characteristics [8][10].

AES: (Advanced Encryption Standard), is the new encryption standard recommended by NIST to replace DES. Brute force attack is the only effective attack known against it, in which the attacker tries to test all the characters combinations to unlock the encryption. Both AES and DES are block ciphers. It has variable key length of 128, 192, or 256 bits; default 256. It encrypts data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices. Also, AES has been carefully tested for many security applications [9][10].

Asymmetric Algorithms :

RSA: This is an Internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is the most commonly used encryption. Till now it is the only algorithm used for private and public key generation and encryption. It is a fast encryption [11].

DSA: The Digital Signature Algorithm (DSA) is a Federal Information Processing Standard for digital signatures. It was proposed by the National Institute of Standards and Technology (NIST) in August 1991 for

use in their Digital Signature Standard (DSS) and adopted as FIPS 186 in 1993. Four revisions to the initial specification have been released: FIPS 186-1 in 1996, FIPS 186-2 in 2000, FIPS 186-3 in 2009, and FIPS 186-4 in 2013. With DSA, the entropy, secrecy, and uniqueness of the random signature value *k* is critical [10]. It is so critical that violating any one of those three requirements can reveal the entire private key to an attacker. Using the same value twice (even while keeping *k* secret), using a predictable value, or leaking even a few bits of *k* in each of several signatures, is enough to break DSA. [11]

Diffie-Hellman Key Exchange (D-H): Diffie–Hellman key exchange is a specific method of exchanging cryptographic keys. It is one of the earliest practical examples of key exchange implemented within the field of cryptography. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

EI Gamal: In cryptography, the ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie–Hellman key exchange. It was described by Taher Elgamal in 1984. ElGamal encryption is used in the free GNU Privacy Guard software, recent versions of PGP, and other cryptosystems. The Digital Signature Algorithm is a variant of the ElGamal signature scheme, which should not be confused with ElGamal encryption. ElGamal encryption can be defined over any cyclic group. Its security depends upon the difficulty of a certain problem in related to computing discrete logarithms.

III. RESULTS AND DISCUSSION

In this section we compare the existing symmetric algorithms on the basis of different parameters as shown in table1, which includes Block Size, Key Length, Security, and Speed.

Table 1: Comparison of Existing Algorithms on the basis of different parameters

Characteristics	DES	Blowfish	RC5	3-DES	AES
Developed	1977	1993	1994	1998	2000
Block size	64	64	32, 64, 128	64	128, 192, 256
Key length	56	32-448	MAX 2040	112,168	128, 192, 256
Security	Proven Inadeq-uate	Consider-ed Secure	Consid-ered Secure	Consid-ered Secure	Consid-ered Secure
Speed	Very slow	Fast	slow	slow	Very fast

IV. CONCLUSION

Although there has been some increase in security of cloud computing world, there is no straight solution applied under cryptographic implementation. Various cryptographic techniques used to overcome the security issues faced by cloud service provider and users. In this paper, we discussed security issues and its solutions using number of symmetric and asymmetric Algorithms. Our future work will be considering some problems related to existing security algorithms and implement a better version of DES, 3DES, AES, RSA, IDES, Blowfish.

V. REFERENCES

[1] Chunming Rong a, Son T. Nguyen a, Martin Gilje Jaatun, Beyond lightning: A survey on security challenges in cloud computing" Computers and Electrical Engineering xxx (2012) xxx–xxx elsevier

[2] Minqi Zhou, Rong Zhang, Wei Xie, Weining Qian, Aoying Zhou "Security and Privacy in Cloud Computing: A Survey", 2010 Sixth International Conference on Semantics, Knowledge and Grids

[3] Dr. Chander Kant and Yogesh Sharma, "Enhanced Security Architecture for Cloud Data Security" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013, pp.571-575.

[4] Pratyush Ranjan, Preeti Mishra, Jaiveer Singh Rawat, Emmanuel S. Pilli, and R.C. Joshi"

Improved Technique for Data Confidentiality in Cloud Environment" © Springer International Publishing Switzerland 2014

[5] R. Buyya, C. Vecchiola, S.T. Selvi, Mastering Cloud Computing (McGraw-Hill, New Delhi, 2013)

[6] Kashish Goyal, Supriya Kinger" Modified Caesar Cipher for Better Security Enhancement" International Journal of Computer Applications (0975 – 8887) Volume 73– No.3, July 2013.

[7] Yogesh Kumar, Rajiv Munjal and Harsh Sharma,"Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures" IJCSMS International Journal of Computer Science and Management Studies, Vol. 11, Issue 03, Oct 2011.

[8] Mr. Gurjeevan Singh, Mr. Ashwani Singla and Mr. K S Sandha "Cryptography Algorithm Comparison For Security Enhancement in Wireless Intrusion Detection System" International Journal of Multidisciplinary Research Vol.1 Issue 4, August 2011.

[9] D. S. Abdul. Elminaam, H. M. Abdul Kader and M. M. Hadhoud, "Performance Evaluation of Symmetric Encryption Algorithms", Communications of the IBIMA Volume 8, 2009.

[10] Gurpreet Singh, Supriya Kinger"Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security "International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013.

[11] Uma Somani, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing," 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).

[12] M.B. Mollah, K.R. Islam, and S.S. Islam. Next generation of computing through cloud computing technology, in: 2012 25th IEEE Canadian Conference on Electrical Computer Engineering (CCECE), May 2012.p.1-6.