International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 7 | ISSN : 2456-3307

An Analysis of Cryptographic Algorithms in Cloud Computing for Security Issues

K. Gowthami[1], Dr.Jagadhesan.B[2]

[1]Research Scholar, PG and Research Department of Computer Science, D. B. Jain College (Autonomous),Thoraipakkam, Chennai, India

[2]Associate Professor PG and Research Department of Computer Science, D. B. Jain College (Autonomous),Thoraipakkam, Chennai, India

ABSTRACT

Cloud Computing is a set of IT Services, for example network, storage, hardware, software, and resources and these services are provided to a customer over a network. The IT services of Cloud Computing are delivered by third party provider who owns the infrastructure. Benefits of cloud storage are easy access means access to your knowledge anyplace, anyhow, anytime, scalability, resilience, cost efficiency, and high reliability of the data. In this research paper, the proposed work plan is to eliminate the concerns regarding data privacy using cryptographic algorithms to enhance the security in cloud as per different perspective of cloud customers.

Keywords : Cloud Computing, Cryptographic Algorithm, Infrastructure, Internet, Security Issue.

I. INTRODUCTION

Cloud computing has various security issues like data security, network security, malicious user attacks etc. Users are always concerned whether their data is secure or not. That is why many users do not want their data to be outsourced on cloud. Hardly, any organization here uses big data concepts like hadoop because data is not more than 500 TB, so it could be easily maintained using statistical analysis and tools. Cloud computing is used mainly by Facebook, Amazon and Google as their data is really huge in size which is stored in huge data centres. In future, there will be lot of advancements in this area.

II. TYPES OF CLOUDS

There are basically three types of clouds, which are described below

A. Public Cloud This is the one of the cloud in which cloud services are being available to users via a service provider over the Internet. It provides a control mechanism for them. The services may be free or offered on a pay-per usage model.

B. Private Cloud This provides many of the benefits of public, but the main difference among two is that the data is managed properly within the organization only, without the limits of network bandwidth.

C. Community Cloud This type of cloud is basically managed by group of originations that have a common objective to achieve. The members share access to the data in the cloud. D. Hybrid Cloud This is the combination of public as well as private cloud. It can also be defined as multiple cloud systems that are connected in a way that allows programs and data to be moved easily from one system to another.

III. CHARACTERISTICS OF CLOUD COMPUTING

There are several characteristics of cloud computing, which are described below

CSEIT18371 | Received : 05 Sep 2018 | Accepted : 25 Sep 2018 | September-October - 2018 [3 (7) : 175-178]

A. Virtualization Through Cloud computing, user is able to get service anywhere through any kind of terminal. User can attain or share it safely anytime.

B. High Reliability Cloud uses data fault tolerant to ensure the high reliability of the service.

C. Versatility Cloud computing can produce various applications supported by cloud, and one cloud can support different applications running it at the same time.

D. On Demand Service Cloud is a large resource pool that a user can buy according to his/her need; cloud is just like running water, and gas that can be charged by the amount that user used. E. Extremely Inexpensive The centered management of cloud make the enterprise needn't undertake the management cost of data center that increase very fast. The versatility can increase the utilization rate of the available resources compared with traditional system, so users can fully take advantage of low cost.

IV. SECURITY ISSUES IN CLOUD COMPUTING

4.1. Data breaches

A data breach might be the primary objective of a targeted attack or simply the result of human error, application vulnerabilities, or poor security practices, CSA says. It might involve any kind of information that was not intended for public release, including personal health information, financial information, personally identifiable information, trade secrets, and intellectual property. An organization's cloud-based data may have value to different parties for different reasons. The risk of data breach is not unique to cloud computing, but it consistently ranks as a top concern for cloud customers.

4.2. Insufficient identity, credential, and access management

Bad actors masquerading as legitimate users, operators, or developers can read, modify, and delete data; issue control plane and management functions; snoop on data in transit or release malicious software that appears to originate from a legitimate source, CSA says. As a result, insufficient identity, credential, or key management can enable unauthorized access to data and potentially catastrophic damage to organizations or end users.

4.3. Insecure interfaces and application programming interfaces (APIs)

Cloud providers expose a set of software user interfaces (UIs) or APIs that customers use to manage and interact with cloud services. Provisioning, management, and monitoring are all performed with these interfaces, and the security and availability of general cloud services depends on the security of APIs, CSA says. They need to be designed to protect against accidental and malicious attempts to circumvent policy.

4.4. System vulnerabilities

System vulnerabilities are exploitable bugs in programs that attackers can use to infiltrate a system to steal data, taking control of the system or disrupting service operations. Vulnerabilities within the components of the operating system put the security of all services and data at significant risk, CSA says. With the advent of multi-tenancy in the cloud, systems from various organizations are placed close to each other and given access to shared memory and resources, creating a new attack surface.

4.5. Account hijacking

Account or service hijacking is not new, CSA notes, but cloud services add a new threat to the landscape. If attackers gain access to a user's credentials, they can eavesdrop on activities and transactions, manipulate data, return falsified information and redirect clients to illegitimate sites. Account or service instances might become a new base for attackers. With stolen credentials, attackers can often access critical areas of cloud computing services, allowing them to compromise the confidentiality, integrity, and availability of those services.

4.6. Malicious insiders

While the level of threat is open to debate, the fact that insider threat is a real adversary is not, CSA says. A malicious insider such as a system administrator can access potentially sensitive information, and can have increasing levels of access to more critical systems and eventually to data. Systems that depend solely on cloud service providers for security are at greater risk.

4.7. Advanced persistent threats (APTs)

APTs are a parasitical form of cyber attack that infiltrates systems to establish a foothold in the IT infrastructure of target companies, from which they steal data. APTs pursue their goals stealthily over extended periods of time, often adapting to the security measures intended to defend against them. Once in place, APTs can move laterally through data center networks and blend in with normal network traffic to achieve their objectives, CSA says.

4.8. Data loss

Data stored in the cloud can be lost for reasons other than malicious attacks, CSA says. An accidental deletion by the cloud service provider, or a physical catastrophe such as a fire or earthquake, can lead to the permanent loss of customer data unless the provider or cloud consumer takes adequate measures to back up data, following best practices in business continuity and disaster recovery.

V. CRYPTOGRAPHY: SECURITY PRINCIPLES & ALGORITHMS

Cryptography is the science of storing messages securely by converting the raw data into forms which is not readable. Cryptography is considered as a collection of three algorithms.

a) Symmetric-key algorithms,
b) Asymmetric key algorithm and
c) Hashing

Symmetric key algorithms

Symmetric uses single key, which works for both encryption and decryption. The symmetric systems provide a two channel system to their users. It ensures authentication and authorization. Symmetric-key algorithms are those algorithms which uses only one and only key for both. Symmetric-key algorithms are divided into two types: Block cipher and Stream cipher. Some popular Symmetric-key algorithms used in cloud computing includes: Data Encryption Standard (DES), TripleDES, and Advanced Encryption Standard (AES). a) Advanced Encryption Standard (AES) In cryptography, the Advanced Encryption Standard [3] is type of symmetric-key encryption algorithm. Each of the ciphers has a 128-bit block size and having key sizes of 128, 192 and 256 bits, respectively. AES algorithm assures that the hash code is encrypted in a secure manner. AES has a block size of 128

a) **RSA Cryptosystem**

This cryptosystem is one the initial systems and oldest of asymmetric cryptosystem. This algorithm is used for public-key cryptography and not private key cryptography. It is the first and still most commonly used asymmetric algorithm. It involves two keys namely a public key and a private key. The public key is used for encrypting messages. Messages encrypted with the use of public key can be decrypted only by using the private key. In this verification process, the server implements public key authentication by signing a unique message with its private key, which is called as digital signature? The signature is then returned to the client. Then it verifies using the server's known public key.

b) **Diffie-Hellman Key**

In this key exchange protocol sender and receiver will manage to set up a secret key to their symmetric key system, using an unsafe channel. The important concepts on which the security of the Diffie-Hellman Protocols defend upon DDH, DHP, DLP like etc

c) **Hashing Algorithms**

MD5-(Message-Digest algorithm A widely used hash function algorithm in cryptography with a 128-bit hash value and possesses a variable length message into a fixed-length output of 128 bits. First the input message is divides up into lump of 512- bit blocks then the message is padded so that its total length is divisible by 512. The sender of the data uses the public key to encrypt the message and the receiver uses its private key to decrypt the message.

VI. CONCLUSION

Cloud computing is growing as a new thing and it is the new trend indeed and many of the organizations and big companies are moving toward the cloud but lagging behind because of some security problems. Cloud security is an ultimate concept which will crush the drawbacks the acceptance of the cloud by the big MNCs, companies and organizations. DES and AES are mostly used symmetric algorithms as they are relatively more secure. DES is quite simple to implement than AES. RSA and Diffie-Hellman Key Exchange is the asymmetric algorithm. RSA and Diffie-Hellman Key Exchange is used to generate encryption keys for symmetric algorithms in cloud. But the security algorithms which allow linear searching on decrypted data are required for cloud computing, which will take care about the safety of the data. For example, Cryptography can be used for maintaining cloud data access control, cloud data trust management, verifiable computing, cloud data authorization and authentication and safe data storage.

VII. REFERENCES

[1]. Sanjoli Singla, Jasmeet Singh ,"Cloud computing security using encryption technique", IJARCET, vol.2, ISSUE.

[2]. R. Bala Chandar, M. S. Kavitha , K. Seenivasan," A proficient model for high end security in cloud computing", International Journal of Emerging Research in Management &Technology, Vol.5, Issue 10.

[3]. Bokefode Jayant.D, Ubale Swapnaja A, Pingale Subhash V., Karane Kailash J. , Apate Sulabha S. ,"Developing Secure Cloud Storage System by Applying AES and RSA Cryptography Algorithms with Role bases Access Control Model", International Journal of Computer Applications, Volume 118-No.12, May2015

[4]. Douglas R. Stinson," Cryptography: Theory& Practice", Chapman and Hall Publications.