Security in Cloud Computing using Cryptographic Techniques

[1]Deepanshi Nanda, [2]Sonia Sharma
[1,2]Dept. of CSE, Guru Nanak Dev University, Amritsar, Punjab, India

Abstract

Cloud computing is an emerging technology for providing computing resources and storage to users. It eliminates the need of maintaining costly computing facilities by companies and institutes. But the adoption of Cloud Computing applies only if the security is ensured. So, Security is an important factor in cloud computing for ensuring clients data is placed on the secure mode in the cloud. The security issues such as Confidentiality and integrity of data in data security are essential in the cloud. This paper is mainly focused on security issues in today's cloud and several cryptographic techniques that can be used to improve the security in cloud environment.

Keywords

Cloud Computing, Security Issues, Cryptographic Techniques

I. Introduction

Cloud computing is one of the most popular technologies that allow access to information and computer resources from anywhere that a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power. The cloud is a virtualization of resources that maintain and manages itself. Cloud computing is Pay-per-Use-On-Demand model that can conveniently access shared IT resources through the Internet Where the IT resources include social networking sites, webmail, online business applications and network Services. Cloud computing can improve the availability of IT resources and thus provide thus provide the potential for cost reduction through optimized and efficient computing. Cloud also includes the major risk such as security, data integrity, network dependency and centralization. As the security is not provided in cloud many companies adopt their unique security structure [1]. For example-Amazon has its own security structure so security has become the biggest obstacle in adoption of cloud as data is completely under the control of Cloud Service Provider (CSP).

II. Architectural Components

Cloud computing can be categorize based on the services offered and deployment models. According to the different types of services offered, there are three major service models presently associated with cloud computing: Cloud Infrastructure as a Service (IaaS), Cloud Software as a Service (SaaS), and Cloud Platform as a Service (PaaS). Fig. 1 shows a cloud reference architecture [2] that makes the most important security-relevant cloud components explicit and provides an abstract overview of cloud computing for security issue analysis.

A. Software as a Service (SaaS)

In cloud-computing environment, SaaS is software that is owned, delivered and managed remotely by one or more providers and that is offered in a pay-per-use manner [3].SaaS in simple terms can be defined as "Software deployed hosted service and accessed over the Internet." [4] .One of the most common uses for SaaS is for Web- based email services, hosting commercial software suites for example (CRM),enterpriser planning (ERP), and supply chain management (SCM).

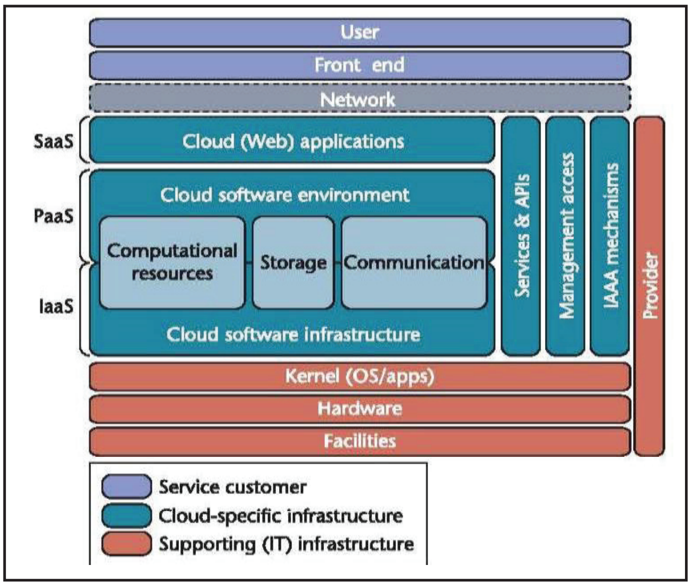

Fig. 1: The Cloud Reference Architecture [10]

B. Platform as a Service (PaaS)

PaaS is a framework to develop or customize applications. PaaS makes development, testing, and deployment of applications very fast, basic and cost-effective, eliminating the need to purchase the underlying layers of hardware and software. With PaaS, vendors still manage runtime, middleware, O/S, virtualization, servers, storage and networking, but clients manage applications and information. Examples for PaaS are Windows Azure, H Force. com and Google App Engine.

C. Infrastructure as a Service (IaaS)

Infrastructure as a service delivers a platform virtualization outsourced service. The Consumer can control the environment as a service. Instead of purchasing servers, software, data center space or network equipment, consumers instead buy those resources as a fully operating system, storage, deployed applications and possibly networking components such as firewalls and load balancers, but not the cloud infrastructure beneath them.

III. Deployment Models

The cloud environment is subdivided into public, private, hybrid and community clouds as shown in Fig. 2.

A. Public Cloud

In Public Cloud, systems and services are easily accessible by everyone therefore, it is less secure due to its openness and needs a mechanism to make it secure .Public clouds provide an elastic, cost- effective means to deploy solutions and take care of deploying, managing, and securing the infrastructure. Companies can use it on demand, and with pay-as-peruse e.g. Amazon EC2, Microsoft Azure, Google Cloud etc.

B. Private Cloud

Private cloud is used by an organization and therefore accessibility to systems and services is limited only to that particular organization. Furthermore, its more secure than public cloud due to its private nature.

C. Hybrid Cloud

Hybrid cloud is a amalgamation of public and private cloud in which the non critical activities are performed in public cloud while the critical activities are performed in private cloud. For example if some of the data being stored is of a very sensitive nature. In such condition the organization may choose to store few data on its dedicated server and less sensitive data in the cloud. Hybrid clouds is also used when the organization needs more processing power than is available in-house and obtains extra requirement in the cloud. This is referred to as cloud bursting. Furthermore hybrid clouds environments are used in situations where customer is moving from a completely private to public cloud setup.

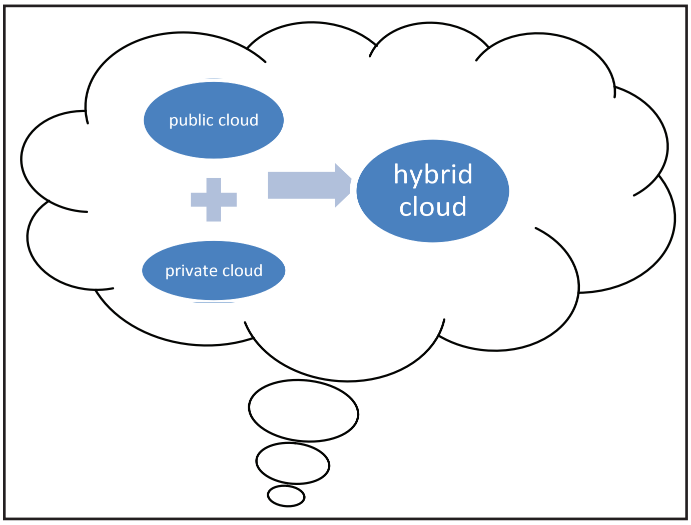

Fig. 2: Types of Cloud

D. Community Cloud

The community cloud is not really a deployment model since it's like a private cloud only in which systems and services are accessible to a group of organization. Community clouds are often designed for businesses and organizations working on joint projects, applications or research, which requires a central cloud computing facility for building, managing and executing projects.

IV. Security Issues in Cloud Computing

Cloud computing can provide infinite computing resources on demand which reduces capital costs,improves accessability,improve fleaxibility .Despite of its merits,one of the most significant barrier preventing companies from entering into the cloud is security Security is a continuous consideration in IT-related projects There are several security issues for cloud computing as it encompasses many technologies inclusive of networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management [5]. For example, the interconnection the system by network in a cloud has to be secure. In addition, virtualization paradigm in cloud computing results in several security concerns. Data security involves encrypting the data and ensuring that appropriate policies are enforced for data sharing [6].

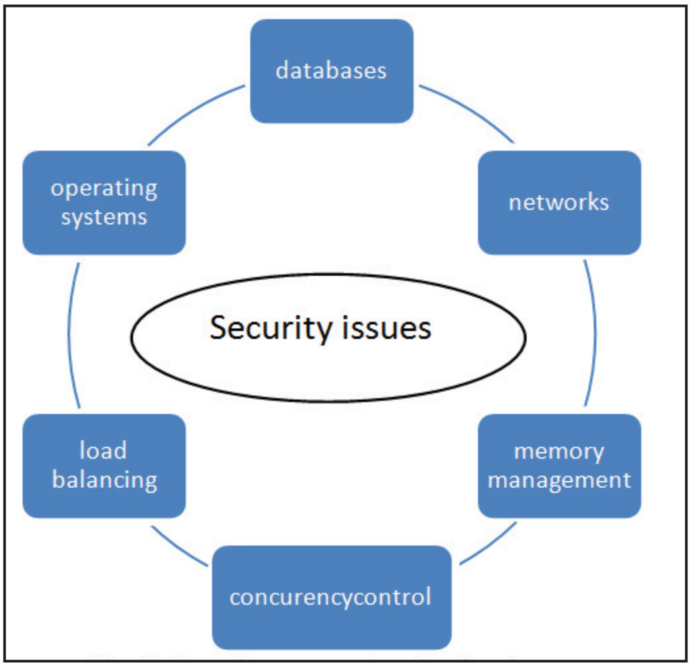

Fig. 3: Security Parameters in Cloud

To maintain security data integrity, confidentiality,availabilty audit control are very important so that any third person or intruder cannot sniff into the messages sent by two parties. Hence, more concerns on these issues, should be taken into account[7].

A. Data Confidentiality

Data confidentiality means only authorized user can get access the owner's data. A key component of protecting information confidentiality would be that only the encryption. Encryption ensure right people can read the information.

B. Data Integrity

In cloud system integrity means to protecting information from being modified by unauthorized parties. Data integrity can be obtained by techniques such as RAID like strategies and digital signature.

C. Availability

The objective of availability for cloud computing systems (including applications and its infrastructures) is to make sure its users will use them at any time at anywhere. As its web-native nature, cloud system allows its users to access the system (e.g., applications, services) from anyplace. Two methods, say hardening and redundancy, are mainly used to enhance the availability of the cloud system or applications hosted on it.

D. Control

Within the cloud system control means to regulate the use of the system, together with the applications, its infrastructure and the data.

E. Audit

It intends to watch what occurred in the cloud framework. Audit ability could be included as an extra layer in the virtualized operation framework (or virtualized application environment) facilitated on the virtual machine to provide facilities watching what occurred in the framework. It is substantially more secure than that is incorporated with the applications or into the software themselves, since it is able watch the entire access duration.

V. Cryptographic Techniques in Cloud Computing

Many security methods for cloud use various cryptographic techniques. Cryptographic techniques have become essential for security in cloud. Cryptography refers to the technique widely used in computer networks to provide security to the data and messages communicated over the network. The plain text message being sent from sender is encrypted in to a special format called as "Cipher Text" by applying some cryptographic algorithm and then communicated over the network. At the receiver's end, the Cipher text message is decrypted in the original plain text again by applying some decryption algorithm. Thus only the sender & receiver of the communication can read the encoded message and no one else.

Following figure describe the basic components of cryptography

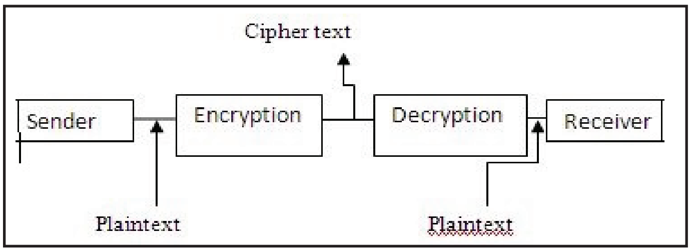

Fig. 4: Cryptography

- **Plaintext** is the original message before being transformed,
- **Cipher text** is the output of an encryption process i.e. encrypted text or message in its coded human readable form.
- **Encryption algorithm:** An encryption algorithm transforms the plaintext into cipher text. The sender uses an encryption algorithm.
- **Decryption algorithm:** An decryption algorithm transforms the cipher text back into plaintext. The receiver uses a decryption algorithm
- **Key:** A key is a number (or set of numbers) that the cipher, as an algorithm, operates on it.

At present various cryptographic algorithms are there which belong to two major Categories

1. Private-Key or Symmetric Algorithms

In symmetric key encryption, the person who is sending the data and the person who is receiving the data share a key which is kept secret. This is used to encrypt and decrypt the messages. Some examples of are DES, AES, Triple DES.

2. Public-Key Or Asymmetric Algorithms

In asymmetric key encryption, two keys are involved where in one is used for encryption (this is publicly available) and the other is used for decryption (this is kept secret) such as RSA, Diffie-Hellman, ECC, etc

A. Identity Based Encrytion

In identity based encryption (IBE), identity of user plays an vital role. In IBE the public key of a user is some unique information about the identity of the user. It allows any party to generate a public key from a known identity value such as an ASCII string. A trusted third party, called the Private Key Generator (PKG), creates the corresponding private keys. This type of encryption reduces the complexity of the encryption process for both users and administrators. Email Encryption is one of the real applications for Identity Based Encryption.

B. Attribute Based Encryption

It is type of encryption in which a control authority will create a secret key for the users(like in IBE) based on attributes/policies for the each user. In this encryption, data owner uses a set of attributes to encrypt the data and only the authorized users who has the predicted or certain attributes can decrypt the information. This encryption scheme makes more secure cloud environment.

C. Fully Homomorphic Encryption

Homomorphic Encryption method is able to perform operations on encrypted data without decrypting. Homomorphic Encryption systems are used to perform operations on encrypted data without knowing the private key (without decryption), the client is the only holder of the secret key.

Hu da et al [8] proposed fully homomorphic encryption (FHE) allows a user that does not have the secret decryption key to compute any result of the data. The author focused technique is based on a FHE algorithm with key delegation to ensure data confidentiality, authentication, integrity and availability of multi-level hierarchical order. Their proposed framework solution is the using of homomophic cryptography with Attribute Based Encryption.

D. Cloud DES Algorithim

Neha Jain et al[9] have introduced the concept of Data security using the DES algorithm in cloud computing. This approach is applicable for securing both the server and the clients. DES cipher block chaining is constructed for security architecture to eliminate the fraud that is taken place in stealing the data. The data forwarded to the receiver which is hacked is replaced with no danger. The system with encryption is adequately secure, but the level of encryption has to be stepped up as, computing power increases. Symmetric key are used to encrypt the model to result in better secure communication system. The cloud data security must be considered to analyze the data security risk, the data security prerequisites, deployment of security functions and the data security process through encryption. The main view of their paper is the new view of data security solutions with encryption which is also important and it can be applied as reference for designing the complete security solution.

VI. Conclusion

Cloud computing is broad and 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 thus data security on the cloud would be the major concern for all the service providers and data security has many issues like confidentiality, Integrity, surveillance, reliability, availability, Security. The paper discussed various cryptographic techniques that can be used in cloud computing environment so that the data can be securely shared with the authorized users by adopting the cryptographic techniques.

References

[1] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou, Jin Li, "Toward Publicly Auditable Secure Cloud Data Storage Services‖, IEEE Network, 2010.

[2] B. Grobauer, T. Walloschek, E. Stöcker,"Understanding Cloud Computing Vulnerabilities", 2011 IEEE Security and Privacy, pp. 50-57, 2011.

[3] Mertz SA, Eschinger C, Eid T, Pring B.,"Dataquest Insight: SaaS Demand Set to Outpace Enterprise Application Software

Market.

[4] Growth. Gartner RAS Core Research Note, (2007) Moxie Marlinspike,"New Tricks for Defeating SSL In Practice", 2009.

[5] Meiko Jensen, Jörg Schwenk, Nils Gruschka, Luigi Lo Iacono,"On TechnicalSecurity Issues in Cloud Computing", In IEEE ICCC, Bangalore, pp. 109-116, 2009.

[6] Security Issues and their Solution in Cloud Computing Prince Jain International Journal of Computing & Business Research.

[7] M. Q. Zhou, R. Zhang, W. Xie, W. N. Qian, A. Zhou, "Security and Privacy in Cloud Computing: A Survey," 2010 Sixth International Conference on Semantics, Knowledge and Grids (SKG), pp. 105-112, Nov. 2010

[8] Huda Elmogazy, Omaima Bamasak,"Towards Healthcare Data Security in Cloud Computing", IEEE 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)

[9] Jain N, Kaur G.,"Implementing DES Algorithm in Cloud for Data Security, VSRD- IJCSIT 2012; 2(4), pp. 316–21.

[10] Cloud Computing – Research Issues, Challenges, Architecture, Platforms and Applications: A Survey by Santosh
Kumar and R. H. Goudar International Journal of Future Computer and Communication,