© 2016 IJSRSET | Volume 2 | Issue 2 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

A Review Paper on Various Security Issues and its Solutions in Cloud Computing

Neha, Mandeep Kaur

Department of Computer Engineering, RBIEBT, Mohali, Punjab, India

ABSTRACT

In this digital world, where various technologies are being used. There is a need of safe and reliable environment. It also requires considering various security issues the technology faces. As Cloud computing is emerging as a new technology and most of the organizations are moving towards this technology. But the main threat in adopting this technology is its security. There are various security issues that exist such as unauthorized access, loss of data etc. Here we will discuss various security issues and also what are the various solutions to enhance the security of cloud computing. There are various cryptographic techniques that play a major role in information security systems. In this paper, we will also compare these cryptographic techniques with their key features and drawbacks of each.

Keywords: Cloud Computing, Cloud Security, Privacy, Multitenancy, Cloning, Data Integrity

I. INTRODUCTION

Cloud Computing provides us a means by which we can access the applications as utilities, over the Internet. It allows us to create, configure, and customize applications online. Cloud computing is based on the 'reusability of IT capabilities'. It is a model for on demand network access to a shared pool of resources in a more convenient way. Cloud Computing is a computing paradigm, when a large pool of systems are connected in private or public networks, to provide dynamically scalable infrastructure for application, data and file storage.. Examples of cloud services include online file storage, social networking sites, webmail, and online business applications. It is a practical approach to experience direct cost benefits. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications.

Benefits of Cloud Computing:

- Performance
- On demand self service
- Multitenancy
- Broad network access
- Virtualization
- Resource pooling
- Rapid elasticity
- Location independence
- Low cost
- Device independent

II. METHODS AND MATERIAL

A. Service Models of Cloud Computing

Cloud computing is composed of three service models:

- Software as a Service (SaaS): Software's are provided as a service to the consumers according to their requirement, enables consumers to use the services that are hosted on the cloud server.
- Platform as a Service (PaaS): Clients are provided platforms access, which enables them to put their own customized software's and other applications on the clouds.
- Infrastructure as a Service (IaaS): Rent processing, storage, network capacity, and other basic computing resources are granted, enables consumers to manage the operating systems, applications, storage, and network connectivity.

B. Deployment Models of Cloud Computing

In Cloud computing, available deployment models are:

- Public Cloud: Public cloud allows users to access the cloud publicly. It is access by interfaces using internet browsers. Users pay only for that time duration in which they use the service, i.e., pay-per-use.
- Private Cloud: A private clouds operation is within an organization's internal enterprise data center. The main advantage here is that it is very easier to manage security in public cloud. Example of private cloud in our daily life is intranet.
- Hybrid Cloud: It is a combination of public cloud and private cloud. It provides more secure way to control all data and applications .It allows the party to access information over the internet. It allows the organization to serve its needs in the private cloud and if some occasional need occurs it asks the public cloud for some computing resources.
- Community Cloud: When cloud infrastructure construct by many organizations jointly, such cloud model is called as a community cloud. The cloud infrastructure could be hosted by a third-party provider or within one of the organizations in the community

C. Security issues

Cloud computing consists of applications, platforms and infrastructure segments. Each segment performs different operations and offers different products for businesses and individuals around the world. It suffers from various security issues. Some of them are:

- **Data Security:** To achieve the service of cloud computing, the protocol used is HTTP (Hypertext Transfer Protocol) and to ensure security, secure HTTP is used. In a traditional on-premise application, the data exists within the enterprise and it is subject to the enterprise security policies. But in case of accessing the data from outside, how one can assure the security of data. Therefore, the service provider must develop some security checks to ensure security and prevent breaches due to vulnerabilities.
- **Motility of data and data residuals:** Data is stored on a location which is unknown to users. They do not have the control over the physical access mechanisms to the data. Due to various privacy laws, data locality is of utmost importance. It can lead to various issues such as data leakage, unauthorized access to data, loss of data etc. The service provider must use some cryptographic techniques to prevent the security issues.
- **Authentication and Identity Management:** In a traditional on-premise application , the access to data is controlled and restricted the access if user is unauthorised. In clous=d computing, authentication and identity management must be conducted via the internet, increasing exposure and risk. It is extremely important to restrict administrative access to data and monitor this access to maintain visibility of changes in system control. Data access issue is mainly related to security policies provided to the users while accessing the data. There must be a multi factor authentication instead of a single password to achieve high level of security.
- **Cloning and resource Pooling:** Cloning means duplication or replicating the data on servers. It may lead to problems such as data leakage which leads to unauthorized access and loss of important data. Resource pooling is a service provided to the users to use the resources and share them. It leads to unauthorized access while sharing over the same network.
- **Data Integrity:** Data integrity is also a main aspect of cloud computing. Data Integrity must be maintained via database constraints and transactions. Loss of data integrity can lead to data corruption. So, Integrity monitoring is required at every step. It can be achieved through transaction properties (ACID i.e. Atomicity, Consistency, Isolation and Durability). It ensures the integrity of data stored on cloud computing.
- **Availability and reliability Issues:** Data availability is one of the major concern of cloud users. As the data is kept on remote servers, it can suffer from system failures of the service provider. Cloud provider must adopt multi- tier architecture and ensures the load balancing so that users must not suffer from any type of issues. Reliability means cloud provider must provide solutions to each and every problem.
- **Shared Multi-tenant Environment:** Multi-tenancy can be defined as one of the vital attribute of cloud computing, which allows multiple users to run their applications on the physical infrastructure hiding data from each other. It leads to some issues such as illegal access to some data by any other user or

when any tenant consumes unequal amount of resources. This can be due to priority requirements or any hack attacks.

- **Backup and Storage:** The cloud vendor must ensure that data will not be lost i.e. it must ensure the regular backup of data so that in case of any failure, data should not be lost. But It can also lead to some issues such as misuse of data by unauthorized parties. Data de-duplication is one of the solution to reduce backup and offline storage volumes.
- **Network Security:** Networks are classified into many types like shared and non-shared, public or private, small area or large area networks and each of them have a number of security threats to deal with. Problems associated with the network level security comprise of Sniffer Attacks, SQL Injection attack, Intruder attack, Denial of Service attack etc which are explained in details as follow.

Sniffer attacks are launched by applications that can capture packets flowing in a network and if the data that is being transferred through these packets is not encrypted, it can be read and there are chances that vital information flowing across the network can be traced or captured. A sniffer program, through the NIC (Network Interface Card) ensures that the data/traffic linked to other systems on the network also gets recorded. It can be achieved by placing the NIC in promiscuous mode and in promiscuous mode it can track all data, flowing on the same network.

A Denial-of-Service or DoS attack in virtualization takes place when one VM occupies all the obtainable physical resources such that the hypervisor cannot hold up more VMs and accessibility is endangered. The most excellent move towards preventing a DoS attack is to bound resource allocation using correct configurations. Additionally, it is advisable to have the Service Level Agreement (SLA). This legally identifies responsibilities of the service provider and the user.

SQL Injection attacks - These attacks are malicious act on the cloud computing in which a spiteful code is inserted into a model SQL code. This allows the invader to gain unauthorized access to a database and eventually to other confidential information.

D. Cryptographic Techniques

To overcome these security issues, there are various cryptographic techniques. The goal of Information security is to achieve confidentiality by cryptography, integrity by hashing, and availability by access control. To make the data inaccessible to unauthorized users, various cryptographic techniques are used. There are two cryptographic techniques: Symmetric and Asymmetric techniques.

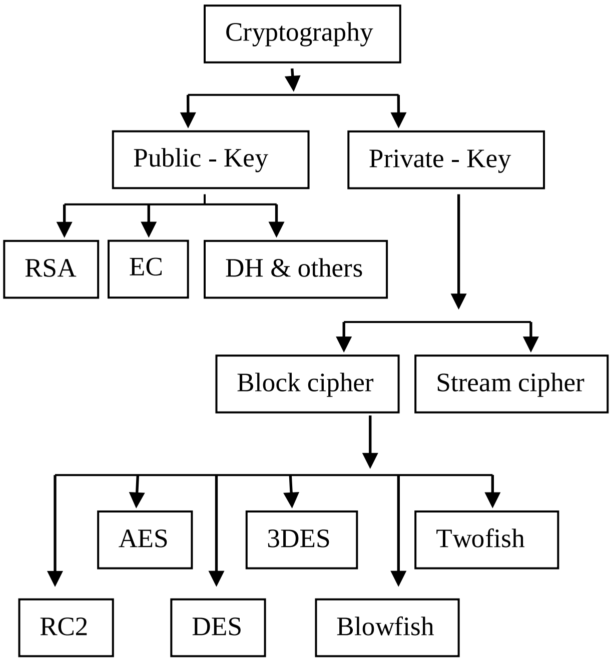

Figure 1. Classification of Cryptographic techniques

III. RESULTS AND DISCUSSION

A. Symmetric Techniques

It is also known as private–key cryptography. In symmetric encryption algorithm, encryption and decryption requires that the same algorithm and key are used to both encipher and decipher the message. There is a private key that is used to encrypt and decrypt the message at both ends. Symmetric encryption key method is extremely fast and efficient for processing encrypts and decrypt message. Symmetric encryption algorithm provides confidentiality, integrity and availability but it fails to provide authenticity and non-repudiation.

Table 1. Comparison among Symmetric Techniques

Techniques	Block Size	Key Size	Cycles	Features	Drawbacks
DES	64	56	16	Resistant to all forms of cryptanalysis	Increased computational power
3DES	64	56, 112, or 128	48	Increase the encryption level	More complex and consumes a lot of time
AES	128	128, 192 or 256	10,12 or 14	More secure	Sometimes it becomes complex
Blowfish	64	32-448	14 or less	Fastest and less memory consumption	Less ssecure
Twofish	128	128, 192 or 256	16	More secure than blowfish	Cracked by some attacks

B. Asymmetric Techniques

It is also known as public-key cryptography. Asymmetric encryption algorithm uses two keys instead of one. One is a private key only known to the recipient of the message and the other is a public key known to everyone and can be freely distributed. Either key can be used to encrypt and decrypt the message. However if only key A is used to encrypt the message then only key B can be used to decrypt it. Conversely, if key B is used to encrypt the message then only key A can be used to decrypt it.

Asymmetric algorithms are slower than symmetric algorithms. But it has better key distribution than symmetric algorithm. It has better scalability and also provides authenticity and non-repudiation.

Table 2. Comparison among Asymmetric Techniques

Techniques	Features	Drawbacks
RSA	Increased security and also used for authentication purposes	Due to factorization of large no., computational overhead increases
ECC	• More efficient as it uses small key sizes • More difficult to challenge • Reduce transmission requirements	Less secure as compared to symmetric algorithms.

IV. CONCLUSION

As the security is a very important aspect of cloud computing, the cloud provider must develop sufficient controls to provide greater level of security than the organization would have if the cloud were not used. In this, we have discussed various security issues. As Data security is one of the major issue, we have also discussed what the various solutions to ensure data security are. In this paper, we discussed some of the cryptographic techniques. Form our observations, we conclude that Blowfish consumes less memory for encryption but AES technique is more secure than all other techniques in symmetric encryption technology. In case of Asymmetric techniques, ECC is the best algorithm. It provides highest strength with small key sizes, resulting in faster computations. These algorithms can be used in combination to achieve high security with faster computation, low power and memory consumption

V. REFERENCES

[1] Yogesh Kumar, Rajiv Munjal, 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, October 2011.

[2] Pratap Chandra Mandal, “Evaluation of performance of the symmetric key algorithms: DES, TDES, AES and Blowfish”, Journal of Global Research in Computer Science, Vol. 3, No. 8, August 2012.

[3] Yang Tang, Patrick P.C. Lee, John C.S. Lui, and Radia Perlman, “Secure overlay cloud storage with access control and assured deletion”, IEEE transactions on dependable and secure computing, Vol. 9, no. 6, Nov/Dec 2012”.

[4] Sajjad Hashemi, “Data storage security challenges in cloud computing”, International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 2, No. 4, August 2013

[5] Ms. Disha H. Parekh, Dr. R. Sridaran, "An Analysis of Security Challenges in Cloud Computing", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 4, No.1, 2013.

[6] Vanya Diwan, Shubhra Malhotra, Rachna Jain, "Cloud security solutions: Comparison among various cryptographic algorithms", International Journal of Advanced Research in Computer Science and Software Engineering , Vol. 4, Issue 4, April 2014.

[7] MD Asif Mushtaque Harsh Dhiman, Shahnawaz Hussain Shivangi Maheshwari, "Evaluation of DES, TDES, AES, Bowfish and Twofish encryption algorithm: based on space complexity", International Journal of Engineering Research & Technology (IJERT), Vol. 3, Issue 4, April 2014.

[8] A. P Shaikh, V. kaul, "Enhanced security algorithm using hybrid encryption and ECC", IOSR Journal of Computer Engineering (IOSR-JCE), Vol. 6, Issue 3, Ver. IV (May-Jun. 2014), PP 80-85.

[9] Mitali, Vijay Kumar and Arvind Sharma, "A survey on various cryptography techniques", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS),Vol. 3, Issue 4, August 2014.

[10] Nikhil Gajra, Shamsuddin S. Khan, Pradnya Rane, "Private cloud security: secured authentication by using enhanced algorithm", International Conference on Advances in Communication and Computing Technologies, August 2014.

[11] Saurin Khedia, Nishant Khatri, "A review on hybrid techniques of security in cloud computing", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 11, November 2014.

[12] Pulkit Chaudhary, "Security concerns and privacy issues in cloud computing", International Journal of Current Engineering and Technology, Vol. 4, No. 6, December 2014.