ISSN: 2379-3686 International Journal of Science Research and Technology
Volume 2 Issue 1, p p 21-24, 25th March 2016

STUDY OF VARIOUS CLOUD COMPUTING SECURITY ALGORITHMS

Pooja P Vasani,
Department of Computer Engineering,
Atmiya Institute of Technology and Science, Rajkot, Gujarat, India

Nishant S Sanghani
Department of Computer Engineering,
Shri Labhubhai trivedi Institute of Engineering and Technology, Rajkot, Gujarat, India

Cloud computing is a latest new computing paradigm where applications, data and IT services are provided over the Internet. Cloud computing serves different types of the resources in virtualized form which can be utilized dynamically. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centers. Organizations use the Cloud in a variety of different service models (SaaS, PaaS, and IaaS) and deployment models (Private, Public, Hybrid, and Community). There are a number of security issues/concerns associated with cloud computing but these issues fall into two broad categories: security issues faced by cloud providers (organizations providing software-, platform-, or infrastructure-as-a-service via the cloud) and security issues faced by their customers (companies or organizations who host applications or store data on the cloud). The responsibility goes both ways, however: the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the user must take measures to fortify their application and use strong passwords and authentication measures are taken.

Index Terms—**Cloud Computing, Security, SaaS, PaaS, IaaS, DES, RSA, BlowFish, Diffie-Hellman.**

I. INTRODUCTION

The cloud computing is a large group of interconnected computers and cloud symbol represents a group of systems or complicated networks. Cloud computing is one way of communication among the various system in the network with the help of internet. Cloud computing is a computing paradigm, where a large pool of systems are connected in private or public networks, to provide dynamically scalable infrastructure for application, data and file storage. With the advent of this technology, the cost of computation, application hosting, content storage and delivery is reduced significantly. Cloud computing is a marketing term for technologies that provide computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services.[1]

Cloud Services

Cloud computing can be thought as different layers or models which provide different services.
Cloud contains three types of services as follows.

1. Infrastructure-as-a-Service (IaaS)- This type of cloud computing distributes a full computer infrastructure via the Internet. Most popular IaaS provider like Amazon Web Services offers virtual server instances with unique IP addresses and block of storage on demand. Here customers usually use the service provider's application program interface to start, stop, access, modify and configure their virtual servers and storage as is needed. In the enterprise, cloud computing allocates services to a company to pay for only as much facility as is required, and bring more flexible tools online as soon as required. [8]

2. Platform-as-a-Service(PaaS)- This type of cloud computing offers a product development tool or environment that users can access and utilize online, even in collaboration with others and hosted on the provider's infrastructure. In PaaS, developers create applications on the service provider's platform over the Internet. PaaS service providers may use Application Program Interfaces (APIs), gateway software or website portals installed on the customer's premises. [8]

3. Software-as-a-Service (SaaS) -This type of cloud computing model offers users the hardware infrastructure, the software product and interrelates with the users through a front-end gateway or portal. Here a provider authorizes an application to clients either as a service on demand in a "pay-as-you-go" model or at no charge by a subscription. [8]

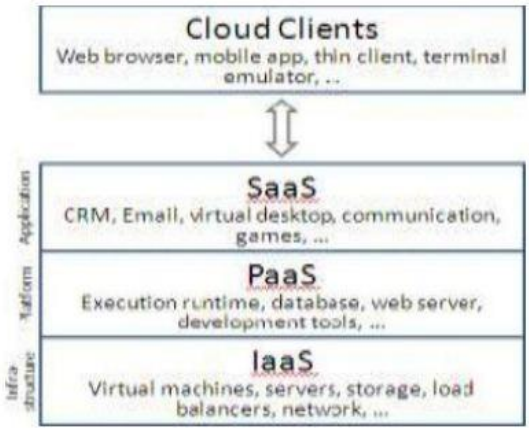

Figure 1. Cloud Services [8]

Types of Cloud

Cloud Computing technology and services can be implemented in different ways according to their purpose and characteristics. These different types of deployment of Cloud are categorized in four ways as follows [4].

1. Private Cloud:

In this Cloud, Infrastructure is deployed and operated by an Organization where all the resources can be owned, maintained and controlled by it only. It can be managed internally or by Third-party. It is also hosted internally or externally. [4]

2. Community Cloud:

In this Cloud, Infrastructure of Cloud is deployed and operated by several organizations in sharing that supports a specific community with common approaches. [4]

3. Public Cloud:

In this Cloud, Infrastructure of Cloud is available to the general public or large group of different kinds of organization. Client can access services without any control and at specific rent. Client's services and data can be co-located with other users. [4]

4. Hybrid Cloud:

In this Cloud, Infrastructure of Cloud can be combination of Private, Community and Public Cloud Infrastructure. This combination of two or more clouds is with unique characteristics, entities and benefits to the users. Multiple kinds of Cloud are connected in such a way that programs and data can be transferred from one system to another deployment Cloud system. [4]

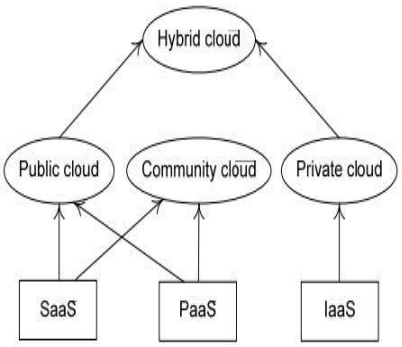

Figure 2. Types of Cloud [4]

II. Security Challenges

The following are some of the notable challenges associated with cloud computing, and although some of these may cause a slowdown when delivering more services in the cloud, most also can provide opportunities, if resolved with due care and attention in the planning stages.[2]

• Security and Privacy — perhaps two of the more "hot button" issues surrounding cloud computing relate to storing and securing data, and monitoring the use of the cloud by the service providers. These issues are generally attributed to slowing the deployment of cloud services. These challenges can be addressed, for example, by storing the information internal to the organization, but allowing it to be used in the cloud. For this to occur, though, the security mechanisms between organization and the cloud need to be robust and a Hybrid cloud could support such a deployment. [2]

• Lack of Standards — Clouds have documented interfaces; however, no standards are associated with these, and thus it is unlikely that most clouds will be interoperable. The Open Grid Forum is developing an Open Cloud Computing Interface to resolve this issue and the Open Cloud Consortium is working on cloud computing standards and practices. The findings of these groups will need to mature, but it is not known whether they will address the needs of the people deploying the services and the specific interfaces these services need. However, keeping up to date on the latest standards as they evolve will allow them to be leveraged, if applicable. [2]

• Continuously Evolving — User requirements are continuously evolving, as are the requirements for interfaces, networking, and storage. This means that a "cloud," especially a public one, does not remain static and is also continuously evolving. [2]

III. Security Concerns

1. Data? The main thing that is where the data is because the data is in cloud so the cloud provider should agree to provide security to the data of our customers. [3]

2. Access? And second thing that who has access to the data that is at cloud. If anyone using the cloud needs to look at who is managing their data and what types of controls are applied. [3]

3. Training to Employees? Train the employees because the employees need to know how to access the data maintaining security. [3]

4. Data Classification? Because there is data of different user so the question is ―Is Data Classified. [3]

5 service level agreement (SLA)? The SLA serves as a contracted level of guaranteed service between the cloud provider and the customer that specifies what level of services will be provided. [3]

6. What happens if there is a security breach? If a security incident occurs, what support will you receive from the cloud provider? While many providers promote their services as being unhackable, cloud based services are an attractive target to hackers. [3]

IV. KEY SECURITY ISSUES IN CLOUD COMPUTING

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. The business application includes Software as a Service (SaaS), Utility Computing, Web Services, Platform as a Service (PaaS), and Managed Service Providers (MSP), Service Commerce and Internet

Integration.[10] There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management. Therefore, security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that interconnects the systems in a cloud has to be secure and mapping the virtual machines to the physical machines has to be carried out securely.[10] Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. The given below are the various security concerns in a cloud computing environment. [10]

- Data Transmission
- Virtual Machine Security
- Network Security
- Data Security
- Data Privacy
- Data Integrity
- Data Location
- Data Availability
- Data Segregation
- Security Policy and Compliance
- Patch management

V. Cloud Security Algorithms

In Cloud Storage any organization's or individual's data is stored in and accessible from multiple distributed and connected resources that comprise a cloud. To provide secure communication over distributed and connected resources, encryption algorithm plays a vital role. It is the fundamental tool for protecting the data. Encryption algorithm converts the data into scrambled form by using "the key" and only user have the key to decrypt the data. In Symmetric key encryption, only one key is used to encrypt and decrypt the data. Another technique is known as asymmetric key encryption where two keys- private and public keys are used. Public key is used for encryption and private key is used for decryption [5].

1. Data Encryption Standard (DES) Algorithm

The Data Encryption Standard (DES) is a symmetric-key block cipher published as FIPS-46 in the Federal Register in January 1977 by the National Institute of Standards and Technology (NIST). At the encryption site, DES takes a 64-bit plain text and creates a 64-bit cipher text, at the decryption site, it takes a 64-bit cipher text and creates a 64-bit plain text, and same 56 bit cipher key is used for both encryption and decryption. The encryption process is made of two permutations (P-boxes), which we call initial and final permutation, and sixteen Feistel rounds. Each round uses a different 48-bit round key generated from the cipher key according to a predefined algorithm. DES performs an initial permutation on the entire 64 bit block of data. It is then split into two, 32 bit sub-blocks, L0 and R0 which are then passed into what is known as Feistel rounds. Each of the rounds is identical and the effects of increasing their number are twofold - the algorithms security is increased and its temporal efficiency decreased. At the end of the 16th round, the 32 bit L15 and R15 output quantities are swapped to create what is known as the pre-output. This [R15, L15] concatenation is permuted using a function which is the exact inverse of the initial permutation. The output of this final permutation is the 64 bit cipher text. [5]

2. RSA Algorithm

RSA Algorithm named after its inventers (Rivest, Shamir, and Adelman) is best suited for data traveling to/from Web and Cloud based environments. In working with Cloud Computing, the end user data is first encrypted and then stored on the Cloud. When the data is required, the end user simply needs to place a request to the Cloud Service provider for accessing the data. For this the Cloud service provider first authenticates the user to be the authentic owner and then delivers the data to the requester using RSA Asymmetric Algorithm. This algorithm has support from .NET Security Framework as well. [6] The RSA algorithm named after Ron Rivest, Adi Shamir, and Leonard Adleman. It is based on a property of positive integers. RSA uses modular exponential for encryption and decryption. RSA is an algorithm for public-key Cryptography, involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key RSA uses two exponents, e and d, where e is public and d is private. Let the plaintext is M and C is cipher text, then at encryption [5]

$C = M^e \bmod n$

And at decryption side

$M = C^d \bmod n$.

3. Diffie-Hellman Key Exchange (D-H):

This is a method for exchanging cryptographic keys by first establishing a shared secret key to use for the inter communication and not for encryption or decryption. This key exchange process ensures the two parties that have no prior knowledge of each other to jointly establish a shared secret key over unsecure internet. Transformations of keys are interchanged and both end up with the same session key that looks like a secret key. Then each can then calculate a third session key that cannot easily be derived by an attacker who knows both exchanged values. This key encrypts the subsequent communications using a symmetric key cipher but is vulnerable to the Man-in-the Middle (MITM) attack. This key exchange is not used for exchanging real large data unlike RSA. [6]

4. Blowfish Algorithm

Blowfish Algorithm is a symmetric key algorithm which was developed in 1993 by Bruce Schneier. Its working is almost similar to DES but in DES key size is small and can be decrypted easily but in Blowfish algorithm the size of key is large and it can vary from 32 to 448 bits. Blowfish also consists of 16 rounds like DES. Blowfish algorithm can encrypt data having size multiple of eight and if the size of the message is not multiple of eight than bits are padded. In Blowfish algorithm also 64 bits of plain text is divided into two parts of size 32 bits. One part taken as the left part of

message and other is right part of message. The left part is XOR with the elements of P-array which creates some value, then that value is passed through transformation function F. The value originated from the transformation function is again XOR with the other half of the message i.e. with right bits, then F function is called which replace the left half of the message and P replaces the right side message. [7]

5. MULTI PRIME RSA ALGORITHM

Multi-prime RSA is an isolated version of RSA cryptosystem. In Multi-prime the modulus consists of more than two prime numbers and the decryption will be speed-up by using Chinese remainder theorem. [9]

Multi-prime RSA is composed of three phases

i) Key Generation
ii) Encryption
iii) Decryption

For any integer, r>= 2, r-prime RSA consists of the following three algorithms.

Key Generation:

Let N be the product of r, randomly chosen distinct primes p1…..pr.

Compute Euler's Totient function of N: $\varphi(N) = \Pi i=1^{r} (p_i-1)$.

Choose an integer e, $1 < e < \varphi(N)$, such that $\gcd(e,\varphi(N)) = 1$. The pair (N; e) is the public key.

Compute the integer $d \in Z_N$ such that $ed \equiv 1 \bmod \varphi(N)$, here d is the private key.

Encryption:

For any message $M \in Z_N$, the cipher text is computed as $C \equiv m^e \bmod N$

Decryption:

Decryption is done using the Chinese remainder theorem.

Let $di \equiv d \bmod (p_i-1)$. To decrypt the cipher text C, one can first computes $M_i \equiv \acute{} C^d_i \bmod p_i$ for each i, $1 <= i <= \cdot r$, then combines the M_i's using the CRT to obtain $M \equiv C^d \bmod N$. [9]

VI. CONCLUSION

With Cloud computing emerging as a new in thing in technology industry, public and private enterprise and corporate organizations are either using the Cloud services or in process of moving there but face security, privacy and data theft issues. This makes Cloud security a must to break the acceptance hindrance of the cloud environment. Use of security algorithms and ensuring these are implemented for cloud and needs to be properly utilized in order to ensure end user security.

VII. REFERNCES

1. MS. Pooja P Vasani, MR. Nishant S Sanghani "Literature Review: Various Priority Based Task Scheduling Algorithms In Cloud Computing" Journal of Information, Knowledge and Research in Computer Engineering, Vol– 02, Issue 2, November 12 to October 13, pp 298-302
2. Randeep Kaur ,Supriya Kinger "Analysis of Security Algorithms in Cloud Computing" International Journal of Application or Innovation in Engineering & Management (IJAIEM), Vol 3, Issue 3, March 2014, pp 171-176
3. K.S.Suresh, Prof K.V.Prasad "Security Issues and Security Algorithms in Cloud Computing" International Journal of Advanced Research in Computer Science & Software Engineering, Vol 2, Issue 10, October 2012, pp 110-114
4. MR Nishant S Sanghani, MR. R J Khimani, Asst. Prof. K K Sutaria, MS. Pooja P Vasani "Pre-Emptable Shortest Job Next Scheduling In Private Cloud Computing" Journal of Information, Knowledge and Research in Computer Engineering, Vol 2, Issue 2, November 12 to October 13, pp 385-388
5. Shakeeba S. Khan, Prof.R.R. Tuteja "Security in Cloud Computing using Cryptographic Algorithms" International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 1, January 2015, pp 148-154
6. Akashdeep Bhardwaj, Dr. GVB Subrahmanyam, Dr. Vinay Avasthi, Dr. Hanumat Sastry "Security Algorithms for Cloud Computing Environment"
7. Er. Ashima Pansotra and Er. Simar Preet Singh "Cloud Security Algorithms" International Journal of Security and Its Applications Vol.9, No.10 (2015), pp.353-360
8. MS. Pooja P Vasani, MR. Nishant S Sanghani "Resource Utilization & Execution Time Enhancement by Priority Based Pre-emptable Shortest Job Next Scheduling In Private Cloud Computing " International Journal of Engineering Research & Technology (IJERT), Vol. 2, Issue 9, September – 2013, pp 1649-1654
9. Suganya .N, N.Boopal M.E , Naveena .M "Implementing Multiprime RSA Algorithm to Enhance the Data Security in Cloud Computing" International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Issue 1, January 2015, pp 18953-18957
10. Rabi Prasad Padhy, Manas Ranjan Patra, Suresh Chandra Satapathy "Cloud Computing: Security Issues and Research Challenges" IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), Vol. 1, Issue. 2, December 2011, pp 136-146