GLOBAL JOURNAL OF ADVANCED RESEARCH
(Scholarly Peer Review Publishing System)

SECURITY ISSUES AND ALGORITHMS IN CLOUD COMPUTING

K. Vijayakumar
Research Scholar,
Research Department of Computer Science,
NGM College, Pollachi, Tamilnadu,
India

ABSTRACT

Cloud security is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing. Encryption is a well known technology for protecting sensitive data. Use of the combination of Public and Private key encryption to hide the sensitive data of users, and cipher text retrieval. This paper presents an overview of security issues and also analyzes the feasibility of applying encryption algorithm for data security and privacy in cloud Storage. It also tried to cover the various algorithms used by researchers to solve the open security problems.

Keywords: Cloud Computing, Security, Privacy, Encryption Algorithms.

1. INTRODUCTION

Many organizations today are feeling pressure to reduce IT costs and optimize IT operations. Cloud computing is rapidly emerging as a viable means to create dynamic, rapidly provisioned resources for operating platforms, applications, development environments, storage and backup capabilities, and many more IT functions. A staggering number of security considerations exist that information security professionals need to consider when evaluating the risks of cloud computing.

The first fundamental issue is the loss of hands-on control of system, application, and data security. Many of the existing best practice security controls that infosec professionals have come to rely on are not available in cloud environments, stripped down in many ways, or not able to be controlled by security teams. Security professionals must become heavily involved in the development of contract language and Service Level Agreements (SLAs) when doing business with Cloud Service Providers (CSPs). Compliance and auditing concerns are compounded. Control verification and audit reporting within CSP environments may be less in-depth and frequent as audit and security teams require.

2. CLOUD COMPUTING FRAMEWORK

Service Models: These three are the most widely used service models of cloud computing.

i) Software as a service (SaaS).

It is also referred as software available on demand, it is based on multi-tenant architecture. Software like word processor, CRM (Customer Relation Management), etc. or application services like schedule, calendar, etc. are executed in the

GLOBAL JOURNAL OF ADVANCED RESEARCH
(Scholarly Peer Review Publishing System)

"cloud" using the interconnectivity of the internet to do manipulation on data. Custom services are combined with 3rd party commercial services via Service oriented architecture to create new applications. It is a software delivery for business applications like accounting, content delivery, Human resource management (HRM), Enterprise resource planning (ERP) etc on demand on pay-as-you go model [1].

ii) Platform as a Service (PaaS).

This layer of cloud provides computing platform and solution stack as service**.** Platform-as-a-Service provides the user with the freedom of application design, application development, testing, deployment and hosting as well as application services such as team collaboration, web service integration and database integration, security, scalability, storage, persistence, state management, application versioning, without thinking about the underlying hardware and software layers by providing facilities required for completion of project through web application and services via Internet.

iii) Infrastructure as a Service (IaaS).

Infrastructure as a service delivers a platform virtualization environment as a service. Instead of purchasing servers, software, data center space or network equipment, clients can buy these resources as outsourced service. In other words the client uses the third party infrastructure services to support its operations including hardware, storage, servers and networking components.

3. CLOUD SECURITY AND PRIVACY

It is generally recommended that information security controls be selected and implemented according and in proportion to the risks, typically by assessing the threats, vulnerabilities and impacts. While cloud security concerns can be grouped into any number of dimensions (e.g. Gartner named seven [2] while the Cloud Security Alliance identified fourteen areas of concern[3]).

Cloud computing security architecture is depicted in Figure 1. Cloud provider is concerned with cloud orchestration and cloud service management. Cloud auditor assesses the data in the cloud environment. Cloud broker has different services such as intermediation, aggregation and arbitrage. So Cloud Consumer, Cloud Provider, and Cloud Broker acts as a major role in cloud security.

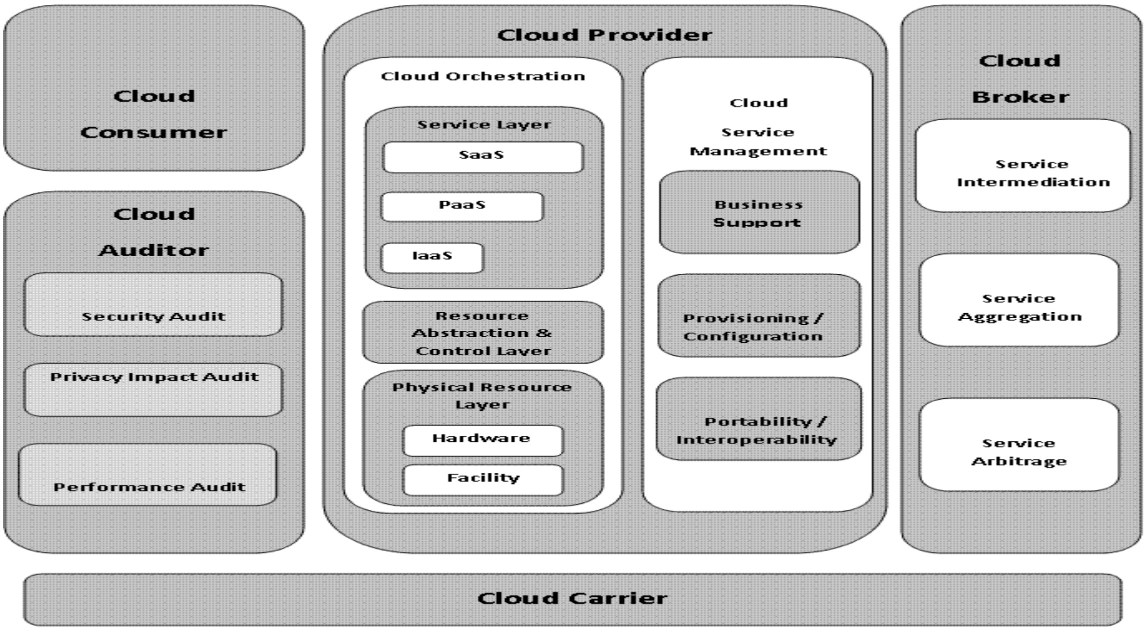

Fig. 1 - Cloud Computing Security

Various information security concerns relating to the IT and other professionals associated with cloud services are typically handled through pre-, para- and post-employment activities such as security screening potential recruits, security awareness and training programs, proactive security monitoring and supervision, disciplinary procedures and contractual obligations embedded in employment contracts, service level agreements, codes of conduct, policies etc.

Availability

Cloud providers help ensure that customers can rely on access to their data and applications; at least in part (failures at any point - not just within the cloud service providers' domains - may disrupt the communications chains between users and applications).

Application Security

Cloud providers ensure that applications available as a service via the cloud (SaaS) are secure by specifying, designing, implementing, testing and maintaining appropriate application security measures in the production environment. Note that - as with any commercial software - the controls they implement may not necessarily fully mitigate all the risks they have identified, and that they may not necessarily have identified all the risks that are of concern to customers. Consequently, customers may also need to assure themselves that cloud applications are adequately secured for their specific purposes, including their compliance obligations.

Privacy

Providers ensure that all critical data (credit card numbers, for example) are masked or encrypted (even better) and that only authorized users have access to data in its entirety. Moreover, digital identities and credentials must be protected as should any data that the provider collects or produces about customer activity in the cloud.

Legal Issues

Finally, providers and customers must consider legal issues, such as Contracts and E-Discovery, and the related laws, which may vary by country [2].

4. CLOUD SECURITY CONTROLS

Cloud security architecture is effective only if the correct defensive implementations are in place. Efficient cloud security architecture should recognize the issues that will arise with security management[7]. The security management addresses these issues with security controls.

These controls are put in place to safeguard any weaknesses in the system and reduce the effect of an attack. While there are many types of controls behind a cloud security architecture, they can usually be found in one of the following categories:[2]

Deterrent Controls

These controls are intended to reduce attacks on a cloud system. Much like a warning sign on a fence or a property, deterrent controls typically reduce the threat level by informing potential attackers that there will be adverse consequences for them if they proceed. [Some consider them a subset of preventive controls.]

Preventive Controls

Preventive controls strengthen the system against incidents, generally by reducing if not actually eliminating vulnerabilities. Strong authentication of cloud users, for instance, makes it less likely that unauthorized users can access cloud systems, and more likely that cloud users are positively identified.

Detective Controls

Detective controls are intended to detect and react appropriately to any incidents that occur. In the event of an attack, a detective control will signal the preventative or corrective controls to address the issue[5]. System and network security monitoring, including intrusion detection and prevention arrangements, are typically employed to detect attacks on cloud systems and the supporting communications infrastructure.

Corrective Controls

Corrective controls reduce the consequences of an incident, normally by limiting the damage. They come into effect during or after an incident. Restoring system backups in order to rebuild a compromised system is an example of a corrective control.

5. SECURITY ALGORITHMS

i) RSA- is an algorithm for public-key cryptography, involves a public key and a private key[9]. 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. User data include encryption prior to storage, user authentication procedures prior to storage or retrieval, and building secure channels for data transmission [10].

Limitations

- ❖ Using small primes.
- ❖ Using primes that are very close.
- ❖ Message is an observable **e**th power.
- ❖ Two people using the same N, receiving the same message.
- ❖ Sending the same message to e or more people with the same e (Hastad’s attack).

ii) MD5- (Message-Digest algorithm 5), a widely used cryptographic hash function with a 128-bit hash value, processes a variable-length message into a fixed-length output of 128 bits. The input message is broken up into chunks of 512-bit blocks. the message is padded so that its length is divisible by 512.

In this sender use the public key of the receiver to encrypt the message and receiver use its private key to decrypt the message.

iii) AES- In cryptography, the Advanced Encryption Standard (AES) is a symmetric-key encryption standard. Each of these ciphers has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively[6]. AES algorithm ensures that the hash code is encrypted in a highly secure manner. AES has a fixed block size of 128 bits and uses a key size of 128 in this paper. Its algorithm is as follows:

1. Key Expansion
2. Initial Round
3. Add Round Key
4. Rounds
5. Sub Bytes - a non-linear substitution step where each byte is replaced with another according to a lookup table.
6. Shift Rows - a transposition step where each row of the state is shifted cyclically a certain number of steps.
7. Mix Columns - a mixing operation which operates on the columns of the state, combining the four bytes in each column
8. Add Round Key - each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule.
9. Final Round (no Mix Columns)
10. Sub Bytes
11. Shift Rows

GLOBAL JOURNAL OF ADVANCED RESEARCH
(Scholarly Peer Review Publishing System)

12. Add Round Key

6. OPEN ISSUES IN CLOUD SECURITY

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[5]. 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 ensure that the provider has taken the proper security measures to protect their information, and the user must take measures to use strong passwords and authentication measures.

The extensive use of virtualization in implementing cloud infrastructure brings unique security concerns for customers or tenants of a public cloud service[7]. Virtualization alters the relationship between the OS and underlying hardware - be it computing, storage or even networking. This introduces an additional layer - virtualization - that itself must be properly configured, managed and secured[8]. Specific concerns include the potential to compromise the virtualization software, or "hypervisor". While these concerns are largely theoretical, they do exist[3]. For example, a breach in the administrator workstation with the management software of the virtualization software can cause the whole datacenter to go down or be reconfigured to an attacker's liking.

7. CONCLUSION

The strength of cloud computing is the ability to manage risks in particular to security issues. Security algorithms mentioned for advanced encryption and decryption can be implemented in future to enhance security over the network. In the future, we will extend our research by providing algorithm implementations to justify our concepts of security for cloud computing.

8. REFERENCES

[1] http://en.wikipedia.org/wiki/Cloud_computing.

[2] "Gartner: Seven cloud-computing security risks". InfoWorld. 2008-07-02. Retrieved 2010-01-25.

[3] "Security Guidance for Critical Areas of Focus in Cloud Computing". Cloud Security Alliance. 2011. Retrieved 2011-05-04.

[4] Krutz, Ronald L., and Russell Dean Vines. "Cloud Computing Security Architecture." Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Indianapolis, IN: Wiley, 2010. 179-80. Print.

[5] Winkler, Vic (2011). *Securing the Cloud: Cloud Computer Security Techniques and Tactics*. Waltham, MA USA: Elsevier. p. 59. ISBN 978-1-59749-592-9.

[6] M. Sudha, Dr. Bandaru Rama Krishna Rao, M. Monica ―A Comprehensive Approach to Ensure Secure Data Communication in Cloud Environment, in International Journal of Computer Applications (0975 – 8887) Volume 12– No.8, December 2010.

[7] "Swamp Computing a.k.a. Cloud Computing". Web Security Journal. 2009-12-28. Retrieved 2010-01-25.

[8] Hickey, Kathleen. "Dark Cloud: Study finds security risks in virtualization". Government Security News. Retrieved 12 February 2012.

[9] Andrea Pellegrini, Valeria Bertacco, "Fault-Based attack of RSA Authentication".

[10] N. Saravanan, A. Mahendiran, N. Venkata Subramanian and N. Sairam, "An Implementation of RSA Algorithm in Google Cloud using Cloud SQL", Research Journal of Applied Sciences, Engineering and Technology, 2012, ISSN: 2040-7467.

Authors Biography

Mr. K. Vijayakumar received his MCA degree from Bharathiar University in 1999 and completed his M.Phil. degree in Computer Science from Bharathiar University in 2005. He is currently pursuing his Ph.D. at the Research Department of Computer Science, NGM College, Pollachi, under Bharathiar University, Coimbatore. His research interests include Computer Simulation and Networks Security. He has 14 years of teaching experience. He is presently working as an Assistant Professor and Head, Department of Information Technology, NGM College, Pollachi.