International Journal of Research in Advent Technology, Vol.6, No.12, December 2018
E-ISSN: 2321-9637
Available online at www.ijrat.org

Cloud Security Systems: A Comparison Study on DSA and AES Algorithms

Biju Ottathengil Thankappan
Manager-Operation Support
CPA Global
30200 Telegraph Road, Bingham Farms
Michigan-48025, USA

Abstract-In Present days, Cloud Computing is a cluster of sources and resources offered by internet or network. This technology is completely internet dependent wherein data is stored and maintained through a data storage center of a cloud provider. Its applications are spread in both academic and industrial domains. Cloud Computing minimizes organization's expenditure in resource management and user's maintenance of hardware and software. In turn organization's financial investment and time towards management of infrastructure reduces which also improves organizations performance.
This paper provides a comparison and review between emerging AES and DSA Algorithms for tackling cloud computing security issues and threats.

1. INTRODUCTION

NIST (National Institute of Standards and Technology) defines cloud computing as follows: "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [1].

Cloud Security systems has a robust architecture along with strong security implementation at every layer in a stack also additionally geared up by legal compliances and government protection. In a cloud based security, maintaining the cost of facilities and hardware is not required. There is no need to manage and maintain storage devices/physical severs. A software – based security tool is enforced which monitors and protects the information flow in and out of the cloud resource.

Some of the examples of cloud computing services are [2]: Windows Azure: by Microsoft that permits companies to develop and run services from their cloud. Google Docs: A free provision by Google that permits to open Microsoft Office documents as well as share them with other users through Internet. Amazon EC2 and Amazon Web Services (AWS): Amazon.com provides various cloud computing services. OwnCloud – free ware software that allows running of a cloud file storage service. The concept of cloud and its security measures are complex. It needs to be secured at every layer in a stack. The layers are; Infrastructure, Platform, Application and Data.

Every system administrator will have root access privileges and thereby can install or execute any sort of software which may lead to cold boot attacks or tampering of hardware. In Infrastructure Layer concept, no single individual will be given the right to all privileges. Employing stringent security devices, Surveillance mechanisms and restricted access protects hardware's physical integrity.
The concept of platform layer is to consider and maintain security aspects such as confidentiality, authentication, integrity of the data and its availability.

This paper provides a comparative study of DSA algorithm and AES algorithm in mobile cloud computing. Attacks such as linear cryptanalysis or differential have also been proved on the algorithms making it efficient and worthwhile for further study and advancement in researchers. The statistical analysis and performance of the algorithms contribute capability and assurance of cloud security encryption and decryption. Software performance of the same is efficient and facilitates parallelism and makes efficient use of available processor resources. Our study also aids students of graduate, post graduate levels in development of further advancement of AES and DSA algorithms for cloud security.

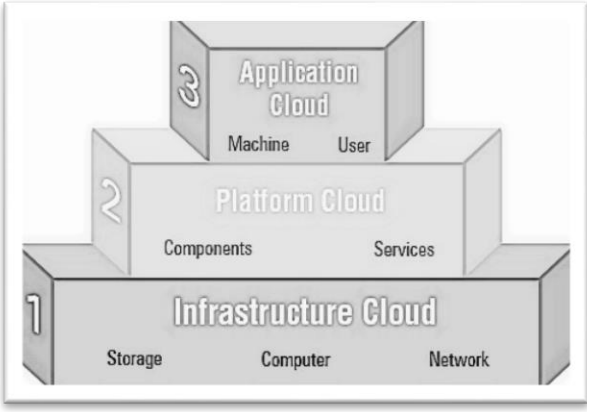

Figure 1: Layers of Cloud Security [3]

2. PERFORMANCE PROTOCOL OF CLOUD BASED SECURITY

Server Security
A traditional network has no norms for ensuring complete protection of servers. Through cloud based security traffic is fed to a cloud instead of being directly fed to a server. A cloud inspects the traffic and allows access to only legitimate users.

Data Inspection and Filtering
A traditional network consists of applications in it, which filters data prior it reaches a server. The Applications filter the traffic once it reaches a network. Applications in turn are also costly and difficult to maintain. Through cloud based security, traffic is directed to the security cloud initially wherein it will be filtered before reaching an application system.

Private Cloud
Cloud based security offers a private cloud which differentiates client application's unwanted traffic access. It ensures protection from shared resource problems.

Management of Data and Security Encryption
Cloud based security manages identity of the data and limits access from unrecognized applications which could decipher the encrypted files.

Compliance Rules
Cloud based security has a rules protocol to be obeyed which ensures safety of the database.

Table 1 below depicts comparison of a traditional network with a cloud based security system.

Table 1: Comparison of traditional network with cloud based security system

Traditional Network	Cloud Based Security System
Decreased Efficiency	Efficiently utilizes Resources
time to market is high	time to market is reduced
Higher investment costs	Costs are usage-based
Scaling is Slow	Quickly scalable
Upfront costs are higher	Upfront investment costs are less
In – house data centers	Third – party data centers

3. CHALLENGES IN CLOUD COMPUTING ANALYSIS

Research and Analysis is yet at an early stage in cloud computing. Numerous problems have not been completely analyzed and addressed. Simultaneously new challenges also arise in industries. Below mentioned are some of the concerns.

MULTITENANCY

Multi-tenancy happens during numerous users using the same cloud for information and data sharing or runs on a single server. It occurs when multiple consumers share the same application, running on a same operating system, on the same hardware, with the same data-storage system and both the attacker and the sufferer are sharing the common server. Specifically in application-layer multi-tenancy, resources are shared at every infrastructure layer and also have valid performance and security concerns. For example, multiple service requests accessing resources at a same time increases wait time and not necessarily CPU time [4].

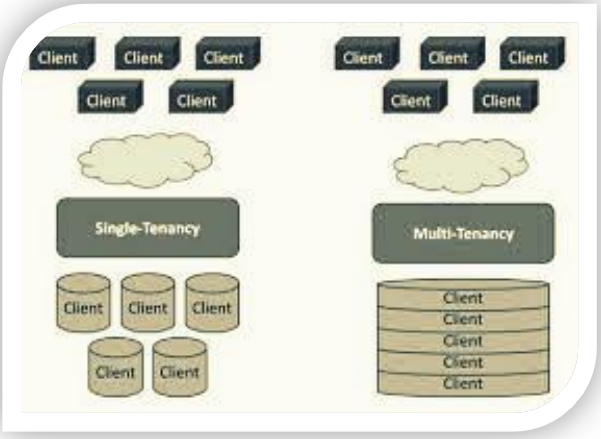

Figure 2: Depicts difference between single tenancy and multi tenancy [5]

ACCESS CONTROLS

Most important management is identity management and authentication in cloud computing. Strength of passwords, its change frequency, password recovery methods are

important elements of access determining how secure is the data in internal systems.

DATA ENCRYPTION

Security of data ranges from simple (easy management, low cost, less secure) to highly secure (complexity, high cost, access limitations). Based on the options available the user must under his/her requirement and decide based on desired security level.

DIGITAL FORENSICS

Examinations cannot be conducted in cases wherein a cloud storage device cannot be physically accessed. Process models are developed to formalize collection of the same [6]. Another approach is to employ a tool which processes in the cloud [7].

INTEROPERABILITY

It's the ability of multiple systems working together for information exchange. Most of the cloud networks would be configured as closed systems and thereby does not interact mutually. This lack of interaction makes it tough for users to include their IT systems on the cloud.

4. AES ALGORITHM AND DSA ALGORITHM

DSA Algorithm

In Digital Signature Algorithm [8], initially user data is encrypted and shared in cloud. In the event of user's data requirement, he/she must place a request for the same to the cloud provider after which the provider authenticates user and delivers data. In DSA, cloud service provider performs encryption and cloud user/end customer performs decryption. For improved and efficient cloud security multiple keys are used. DSA consists of two keys i.e., private key and public key. Keys are generated randomly and they are used at a single time by multiple users.

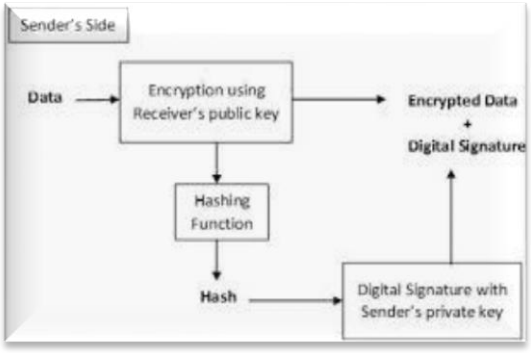

Figure 3: Illustrates working mechanism of DSA Algorithm [9]

AES Algorithm

In Advanced Encryption Standard [10] Algorithm data encryption is performed prior to cloud launch. This algorithm provides protection of data and encryption keys. It also assures the credentials to be under user's control and it will also be not tampered in the process of transit or storage. Physical key management server will be installed in the end customer's premises for key storage.

This algorithm has also good key agility and quick key setup time. A block cipher by design AES has a block length of 128 bits. For 128 bit key length encryption, ten rounds of processing is performed. Every round consists of four steps; SubBytes, ShiftRows, MixColumns and AddRoundKey.

5. LIMITATIONS

Customization options are limited in Cloud Computing, but on the other hand it offers lower costs and focuses on competence. Due to cloud computing's dependency on internet; a person cannot access his/her applications, data or server from a cloud during a slowdown or service outage. Confidentiality and Privacy are concerns in few applications. For example, workers (sworn translators) under NDA's stipulation might overcome issues regarding delicate data which is not encrypted [11]. Customer service is also an issue of concern by users. As per sources of Cloud Security Alliance, topmost threats in the cloud are Hardware Failure, Insecure Interfaces and API's, Data Loss & Leakage—which accounted for 10%, 29% and 25% of all cloud security outages respectively. Altogether, they form vulnerabilities in a shared technology. Many of the cloud computing vendors have put on efforts in technical support improvement in the past few years, but a good service also comes at a price.

6. CONCLUSION AND FUTURE WORK

Foremost issues in cloud computing model are resource sharing, data security, and features of security such as virtualization and network. The complexity in cloud computing makes it a critical issue in pursuing end-to-end security. There is a need for new security techniques to be developed and older security techniques to be drastically modified to work in the cloud architecture environment. Cloud Computing has expansive anticipation, but the threats of end-to-end security lodged are directly proportional to its superior offered advantages.

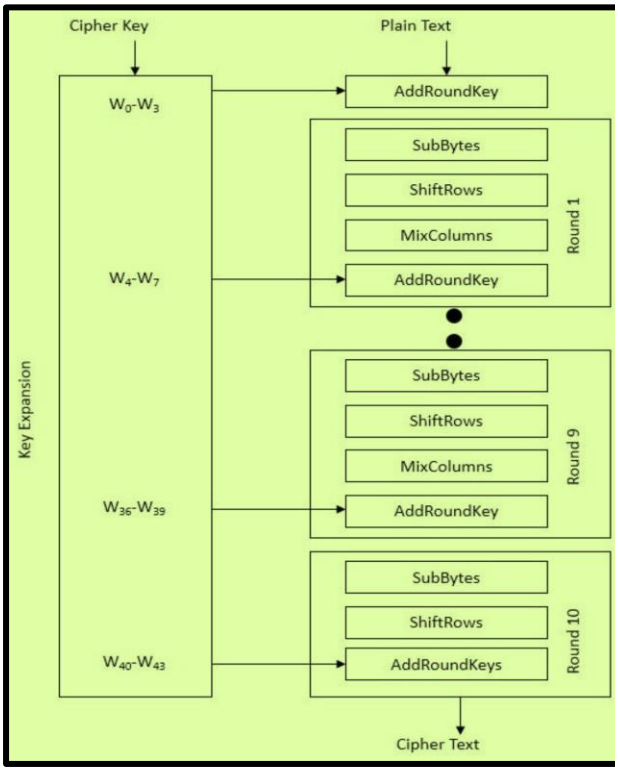

Figure 4: Depicts working mechanism of AES Algorithm [10]

AES algorithm practically up scales in the fact that the cipher and its inverse use different components which eradicates probability of semi-weak or weak keys. AES algorithm's memory consumption is less and its execution time is in milliseconds with unique packet size for both encryption and decryption advantageous over DSA and other Algorithms. DSA assures authenticity, confidentiality and data integrity compared to electronic transactions. As the research and development is yet at an emerging stage, our work would provide a generic understanding and comparison of research comparisons in single and multi - cloud domains of cloud computing and make way for upcoming research.

REFERENCES

[1]. Patricia Yancey Martin and Barry A. Turner. Grounded theory and organizational research. The Journal of Applied Behavioral Science, 22(2):141-157, April 1986.
[2]. www.computerhope.com/jargon/c/cloudcom.htm
[3]. www.tatvasoft.com/blog/cloud-computing-models/
[4]. S. Subashini, V. Kavitha, "A survey on security issues in service delivery models of cloud computing"; Journal of Network and Computer Applications, Vol. 34(1), pp 1–11, Academic Press Ltd., UK, 2011, ISSN: 1084-8045.
[5]. Dr.Chinthagunta Mukundha, Mandadi Kavya, O.Sahithi Reddy R.Tejaswini "A Comprehensive Study on Multi-Tenancy Techniques in Cloud Computing Models" International Journal of Engineering Research and Development e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com Volume 13, Issue 9 (September 2017), PP.59-64
[6]. R., Adams, "The emergence of cloud storage and the need for a new digital forensic process model". *researchrepository.murdoch.edu.au*. Retrieved 2018-03-18.
[7]. *Richard, Adams,; Graham, Mann,; Valerie, Hobbs, (2017).* "ISEEK, a tool for high speed, concurrent, distributed forensic data acquisition". *Research Online.* doi:10.4225/75/5a838d3b1d27f.
[8]. Swati Chaudhaary, Arvind Negi, Prashant Chaudhary "Secure Data Communication in Cloud Computing using Proposed DSA" International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 8, August 2015
[9]. K.Sivaraman "A comparision study of RSA and DSA algorithm in mobile cloud computing" International Journal of Pure and Applied Mathematics Volume 116 No. 8 2017, 247-253 ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
[10]. Abha Sachdev, Mohit Bhansali "Enhancing Cloud Computing Security using AES Algorithm" International Journal of Computer Applications (0975 – 8887) Volume 67– No.9, April 2013
[11]. Karra, Maria. "Cloud solutions for translation, yes or no?". IAPTI.org. Retrieved 23 February 2017.