International Journal on Emerging Technologies (Special Issue on *RTIESTM-2016*) **7**(1): 76-79(2016)

ISSN No. (Print) : 0975-8364
ISSN No. (Online) : 2249-3255

A Novel Approach to Enhance the Security in Cloud Computing using AES Algorithm

***Nisha**[*] **and Nasseb Singh Dhillon**[**]*
**Student M. Tech., Department of Computer Science & Engineering*
A.I.E.T Faridkot, (PB), INDIA
***Assistant Professor, Department of Computer Science & Engineering*
A.I.E.T Faridkot, (PB), INDIA

(Corresponding author: Nisha)
(Received 04 October, 2015 Accepted 04 November, 2015)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: Cloud Computing has become one in every of the foremost talked regarding technologies in recent times and possesses a lot of attention from media yet as analysts attributable to the opportunities it's giving. Cloud Computing may be a term accustomed describe each a platform and kind of application. In this paper the attempt to secure data from unauthorized access. The Method of data security is AES algorithm for providing data security by encrypting the given data based on the AES. It is based on a design principle known as a substitution-permutation network, and is fast in both Software and Hardware. The algorithms used in AES are so simple that they can be easily implemented using heap processors and a minimum amount of memory and this data then can only be decrypted by authorized person by using his private key.

Index Terms*:* Cloud Computing, Cloud Security, Confidentiality, AES, File Encryption, Ciphers, Cloud, XOR Operation

I. INTRODUCTION

Information security is the hot topic of research in the field of computer science and technology, and the data encryption is one of the most important methods for information security. Cloud computing simply means Internet computing generally the internet is seen as collection of clouds; thus the word cloud computing can be defined as utilizing the internet to provide technology enabled services to the people and organizations. Storage space, networks, computer processing power, and specialized corporate and user applications. Cloud Computing may be a term accustomed describe each a platform and kind of application. Furthermore it also helps incorporates to improve there working ways increased scalability while providing services at distinct levels [4]. These levels are named as Software-as-a-services (Saas), Platform-as-a-Services (Paas), and Infrastructure-as-a-Service (Iaas) [12]. Software-as-a-service offers a complete application to the customer, as a service on demand. A single instance of the service runs on the cloud and multiple end users are serviced. Platform-as-a-service that enables developers to write applications those run on the cloud. Infrastructure-as-a-service provides basic storage and computing capacities as standardized services over the network [12]. The service providers are used to provide these services. This helps in delivering the storage and computing services using the internet. It makes ubiquitous data access possible to store data in cloud computing. Security is the most crucial aspect of cloud computing. Cloud security issues are steamed due to cloud services offering, core technology's implementation and arising from cloud characteristics. To make the cloud secure all the entities should be secure. In the system having multiple units the highest levels of the system security can be considered equal to the security of weakest entity.

As the next generation, Cloud Computing has versional architecture of IT Enterprise. In contrast to traditional solutions the IT services are under physical, logical and personnel controls. Current cloud service is grant access to web browser or host install application directly. Cloud storage space moves the users data to large data centres database, on which user does not have any management to manage data. The commercial achievement of Cloud Computing and up to date developments in Grid Computing has been create platform virtualization technology deal with high performance computing by both enterprises and individuals with high service-level requirements. Data security has grow to be predicament of cloud computing like file system, data security, host security.

Security is a secure mode practical Internet based on the cloud computing. These are security and trust issue forth, users data has been liberating to the Cloud and safety measures sphere of the data owner. The data is physically not available to the user the cloud shall provide a way for the user to check if the integrity of his data is maintain.

Our main works on this paper are:

-Our main objective is to enhance the security between the client and the cloud provider by enhancing the AES algorithm using file based encryption methodology.

-The security has a primary role in the services of Cloud computing because the data being transferred between the client and cloud provider is of utmost importance and thereby neither the client nor the cloud provider will sacrifice on the security of the cloud.

-The data is enclosed in the encrypted format using AES by the client itself before sending it to the cloud. The cloud provider will never come to know about the original data of the client.

-Moreover, the data sent to the cloud provider is encrypted using AES encryption algorithm.

-The key used in AES is retrieved from the file sent by the Cloud provider.

-These objectives are stated to ensure the privacy of the client's data when it is being transferred, processed or stored at the cloud provider.

II. RELATED WORK

As per Xueli Huang and Xiaojiang Du[1]: In cloud computing, we have problem like security of data, file system, host security. They have proposed a concept of "**Efficiently Secure Data Privacy on Hybrid Cloud**(AES)**"**protect confidentiality of data stored in cloud [1].The proposed algorithm also reduce the Computation and Storage overhead In the Private Cloud as well as Communication overhead between private and public Cloud.

In This paper Rewagad and Pawar [2]: In cloud computing, we have problem like security of data, file system, host security. They have proposed a concept of digital signature with Diffie-Hellman algorithm and Advanced Encryption Standard encryption algorithm (AES) to protect confidentiality of data stored in cloud [2].This proposed architecture of three way mechanism makes it tough for hackers to crack the security system, thereby protecting data stored in cloud.

Amanpreet Kaur, *et.al,* (March 2013): [3] In this paper there is a analysis of feasibility of attacks on cloud i.e "Extrusion" to detect and prevent attacks caused by unauthorized users. In this paper author discuss about the cloud computing.. [3]In this paper, author discuss about the various scheduling problems. One of the challenging scheduling problems in Cloud data centers is to take the allocation and migration of reconfigurable virtual machines into consideration as well as the integrated features of hosting physical machines.

As per Hime lDev, Sen. Buet, [4] "An Approach to Protect the Privacy Of Cloud Data From Data Mining Based Attacks" architecture is based on Distributed architecture to Eliminate the privacy risk On cloud data is proposed in this paper. The Proposed Distributed Architecture distributing user data among multiple cloud providers to make the data mining a difficult job to the attackers, minimizing the risk with information leakage by any provider and ensure the greater availability of data and optimizes the cost

.Cong Wang, Qian Wang and Kui Ren [5]: According to author users no longer have physical possession of the possibly larger size of outsourced data makes the data integrity protection in cloud computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities [10]. Thus, enabling public audit ability for cloud data storage security introduces an effective third party auditor (TPA). The third-party auditors audit the cloud data storage without demanding the local copy of data and introduce no additional on-line burden to the cloud user.

A. AES

The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. It is based on the Rijndael cipher developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, who submitted a proposal to NIST during the AES selection process.AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. The key size, which can be 128, 192, or 256 bits, depends on the number of rounds.

10 rounds of repetition for 128-bit keys.

12 rounds of repetition for 192-bit keys.

14 rounds of repetition for 256-bit keys.

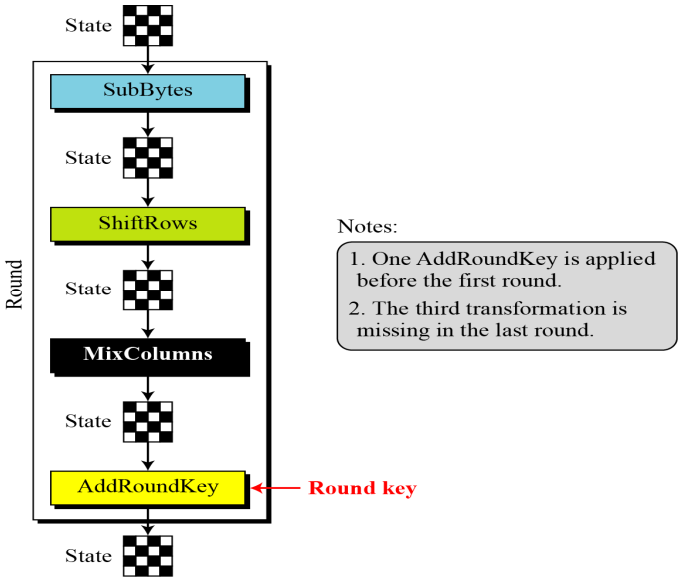

Fig. 1. Structure of each round at the encryption side.

III. PROPOSED WORK

-Client will enter the data that has to be sent to the Cloud Provider. We are going to use file based encryption through Enhanced AES algorithm in cloud computing.

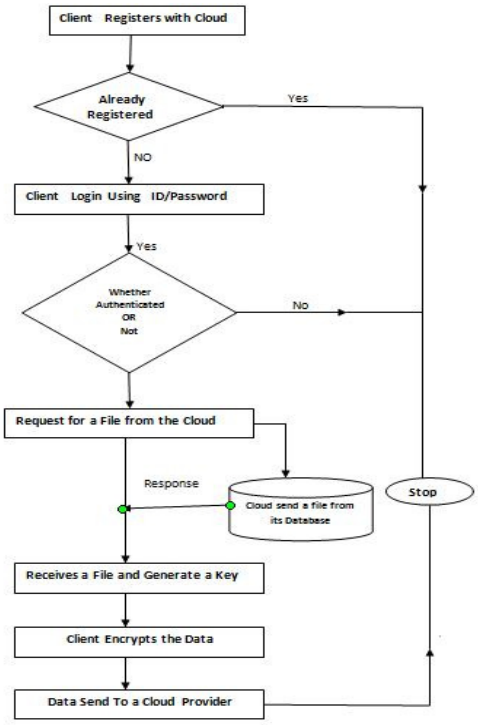

Fig. 2 Flowchart of Proposed Work.

-In the first step we will make a virtual cloud for saving the files and this virtual cloud is made with the help of development tool i.e. Cloud Sim. Inside the cloud Data Centre, we are having the Storage as a service (SAAS) for storing the files received from the client.

-The cloud server has number of files like a1.txt, a1.mp3, a1. mdf, a1.jpg.Client will make a request to the cloud server for sending the file. This file will be used by the client for encrypting the data before sending it to the cloud

-The cloud server will send any file to the client. These files are stored inside the SAAS component of the cloud provider. Client will read the file's data and will randomly generate the row number and column number depending upon the length of the file.

-If anyone tries to hack the data while transferring from client to the gateway, he/she will get only encoded data and If anyone tries to perform the mining on the files stored at the cloud provider, no results will be retrieved

CONCLUSION

This study collectively describes cloud computing security challenges in general and describes the mitigation practices that have been proposed to handle the identified challenges. We have successfully implemented the above proposed system and has reached to a solution that by using the file encryption method along with AES, we can achieve the better security in cloud computing. However, most important future work identifies here is that there are concrete standards for cloud computing security still missing.

There are some open cloud manifesto standards and few efforts made by the cloud security alliance to standardize the process in the cloud. The cloud vendors and users do not encourage the usage of these standards as they are restrictive. In addition to this the cloud computing with such great offering such as storage, infrastructure and application designing capabilities on the go to the IT industry still fail to have proper standards for interoperability with other cloud service providers. This failure to provide concrete security standards, common underlying framework for data migration and global standards for cloud interoperability, make the leading technology the cloud computing" still a vulnerable option for aspiring users.

REFERENCES

[1]. Mr. Prashant Rewagad, Ms. Yogita Pawar, "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing," 978-0-7695-4958-3/13 © 2013 IEEE *International Conference on Communication Systems and Network Technologies.*

[2]. Mazhar Ali, Kashif Bilal, Samee U. Khan, "Division and Replication of Data in Cloud for Optimal Performance and Security," DOI 10.1109/TCC.2015.24004060, *IEEE Transaction on Cloud Computing*.

[3]. Hamid Banirostam, Alireza Hedayati, "A Trust Based Approach for Increasing Security in Cloud Computing Infrastructure," 2013 UKSim *15th International Conference on Computing Modelling and Simulation, 978-0-7695-4994-1/13 © 2013 IEEE.*

[4]. Shuai Han, Jianchuan Xing, " Ensuring Data Storage Security Through a Novel Third Party Auditor Scheme in Cloud Computing." CCIS2011 978-1-61284-204-2/11/$26.00 © 2011 IEEE.

[5]. Tejinder Sharma, Vijay Kumar Banga, " Efficient and Enhanced Algorithm in Cloud Computing," ISSN: 2231-2307, *International Journal of Soft Computing and Engineering (IJSCE)* 2013.

[6]. Balasaraswathi V.R, Manikandan. S, "Enchanced Security for Multi-Cloud Strorage using Cryptographic Data Splitting with Dynamic Approach," ISBN No.978-1-4799-3914-5/14 ©2014 *IEEE International Conference on Advanced Communication Control and Computing Technologies.*

[7]. Jen-Sheng Wang, Che-Hung Liu, Grace TR Lin, " How to Manage Information Security in Cloud Computing," 978-1-4577-0653-0/11/$26.00 © 2011 IEEE.

[8]. Teemu Kanstren, Sami Lehtonen, Reijo Savola, "Architecture for High Confidence Cloud Security Monitoring," DOI 10.1109/IC2E.2015.21 *IEEE International Conference on Cloud Engineering*.

[9]. Eman M. Mohamed, Hatem S. Abdelkader, Sherif El-Etriby, " Data Security Model for Cloud Computing" 2013 the twelfth international conference on networks. ISBN: 978-1-61208-245-5.

[10]. Ramgovind S, Eloff MM, Smith E, "The Management of Security in Cloud Computing," 978-1-4244-5495-2/10/$26.00 ©2010 IEEE.

[11]. Cong Wang, Qian Wang and Kui Ren, "Privacy Preserving Public Auditing for Data Storage Security in Cloud Computing," IEEE INFOCOM 2010.

[12]. Pardeep Bhosale, Priyanka Deshmukh, Girish Dimbar, Ashwini Deshpande, " Enhancing Data Security in Cloud Computing Using 3D Framework and Digital Signature with Encryption," *International Journal of Engineering Research and Technology* 2012 ISSN: 2278-0181.