ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

ENHANCING NETWORK SECURITY IN CLOUD COMPUTING USING CIPHER CLOUD MECHANISM

B.Venkatesh[#1], V.Karthik*[2],M.Gowtham[#3],

Assistant Professor, UG Scholar,

Paavai Engineering College. Paavai Engineering College,

venkatboopathi@gmail.com v.karthik10021995@gmail.com

Abstract- **Network security is an essential thing which reduces the risk or security issues in the network. Cloud Computing is the emerging technology in this internet era. It is a client – server architecture which provides flexible infrastructure. Cloud is an online storage, able to handle large amount of data stored in various places. As it is an online technology, network security and data security becomes a big issue. Clients require their data to be safe and private from any tempering or unauthorized access. Various algorithms and protocols such as DSA, AES and RSA algorithms are implemented on virtual Cloud called Cipher Cloud to achieve authenticity and integrity. The prototype system reduces the network latency. The network latency is reduced by splitting up larger data file into n number of small packs and encrypts those data packs simultaneously. In this model the integrity of the data is tested by hash value. This paper proposes an architecture based model to reduce the work load of the Cloud Server and achieves data authenticity and integrity in cloud computing.**

Keywords– network security, Cipher Cloud, data authenticity, data integrity, data privacy.

I.INTRODUCTION

Cloud computing provides on demand access to the customers with shared resources. As it is an online technology, network security and data security becomes a big issue. It deals with the problem of accessing the data or important document and providing security to the information stored in the cloud. Cloud computing technology increases the availability of information at anytime, anywhere. While providing global access to the information the security issues such as unauthorized accessing or modification of information may occur.

Network security refers to any activities that are carried out to protect our network. Specifically, these activities ensure the usability, reliability and safety of our network and data [6]. Network security is accomplished through hardware and software. Network security consists of the policies adopted to prevent and monitor authorized access, misuse, modifications or denial of computer attacks and network accessible resources [6]. Network security involves the authorization of access to data in a network, which is controlled by the network administrator.

Cloud computing technology consists of various deployment models and these models are listed below:

A. ***Private Cloud***: A private cloud is a particular model of cloud computing that involves a distinct and secure cloud based environment in which only the specified client can operate [5].
B. ***Public Cloud***: A public cloud is a model, under which cloud services are provided in a virtualized environment, constructed using pooled shared physical resources, and accessible over a public network such as the internet [5].
C. ***Community Cloud***: A community cloud is a multi – tenant infrastructure that is shared among several organizations from a specific group with common computing concerns [7].

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

D. ***Hybrid Cloud***: A hybrid cloud is an integrated cloud service utilizing both private and public clouds to perform distinct functions within the same organizations [5].

In Cloud computing environment, there is a need to address some of the security concerns such as, authenticity, data integrity and privacy. The data integrity issues are addressed by using algorithms such as, Prove of Retrievability (PoR) and Dynamic Provable Data Possession (DPDP) [1].

This paper addresses the issues such as authenticity, data integrity verification and privacy preservation of data stored in a cloud server, and also increases the efficiency of the system. Here the efficiency of the system is increased by splitting the file in multiple segments and these segments are encrypted simultaneously.

II. EXISTING SYSTEM

There exists a system, which encrypts the data either stored locally or on the cloud. The Cloud server is entirely responsible for authentication, encryption and storage. The cloud service providers need to provide clients with secured access. Data integrity is the major issue needs to be noted and ensured. There are various methods are available to ensure the data integrity. Data integrity means, the data stored in the cloud needs to be unchanged or unmodified. One of the data integrity verification techniques is Prove of Retrievability (PoR) [1]. This protocol ensures that the data stored at any remote storage servers such as cloud remains unmodified. The drawback of this technique is that it does not protect the data from modification performed by transactions, which are carried out at the service provider's side.

Provable Data Possession (PDP) is another important protocol for ensuring possession of data files on online storage. But the technique fails to address the problem of integrity checking of dynamic data operations. To overcome this problem, a technique called Dynamic Provable Data Possession has been introduced [1]; it was an extension of PDP model. It was the first method to support dynamic data possession. On the other hand a new cloud architecture has been proposed to introduce integrity verification as a service. The disadvantage of this model is that it fails to achieve data privacy.

Encryption techniques are introduced to achieve data privacy and confidentiality [2], [8]. There are various encryption algorithms are used to encrypt the data file, which is stored on the cloud. The encryption process ensures the privacy preservation of data. While applying encryption algorithms on data files, the data file is encrypted (i.e) changed into some other format [2], [8]. After the encryption process is completed the encryption key and the encrypted data will be stored on the cloud. By using the encryption key the encrypted data file will be decrypted (i.e) converted into its original form [2], [8].

III. PROPOSED SYSTEM:

The proposed model is used to ensure authenticity, data integrity and privacy. The prototype system introduces a virtual cloud mechanism called cipher cloud for the authentication as well as encrypting the data file. In this proposed model, DSA algorithm is used for authentication purpose, AES and RSA algorithms are used for the encryption process. To achieve data integrity verification, double encryption process is carried out. Here the multilevel authentication is carried out to ensure the authenticity of the user [4]. While uploading/downloading a larger data files, the file will be splitting into multiple segments and these segments are encrypted using AES algorithm simultaneously. Finally, these encrypted data files will be moved to the cloud server. Then, the AES key will be encrypted using RSA algorithm. The encrypted form of AES key and private key generated by the RSA algorithm will be stored along with the corresponding data file.

This proposed system consists of three modules for performing the above mentioned operations and the modules are listed below:

Application module: This module provides user interface for the system. By using this module the user can upload or download the data files.

Cipher Cloud: It is the virtual mechanism responsible for the following activities:

- To perform DSA based authentication
- To split up the data file into multiple segments
- To perform AES encryption on segments of the data file simultaneously.
- To encrypt the AES key using RSA algorithm

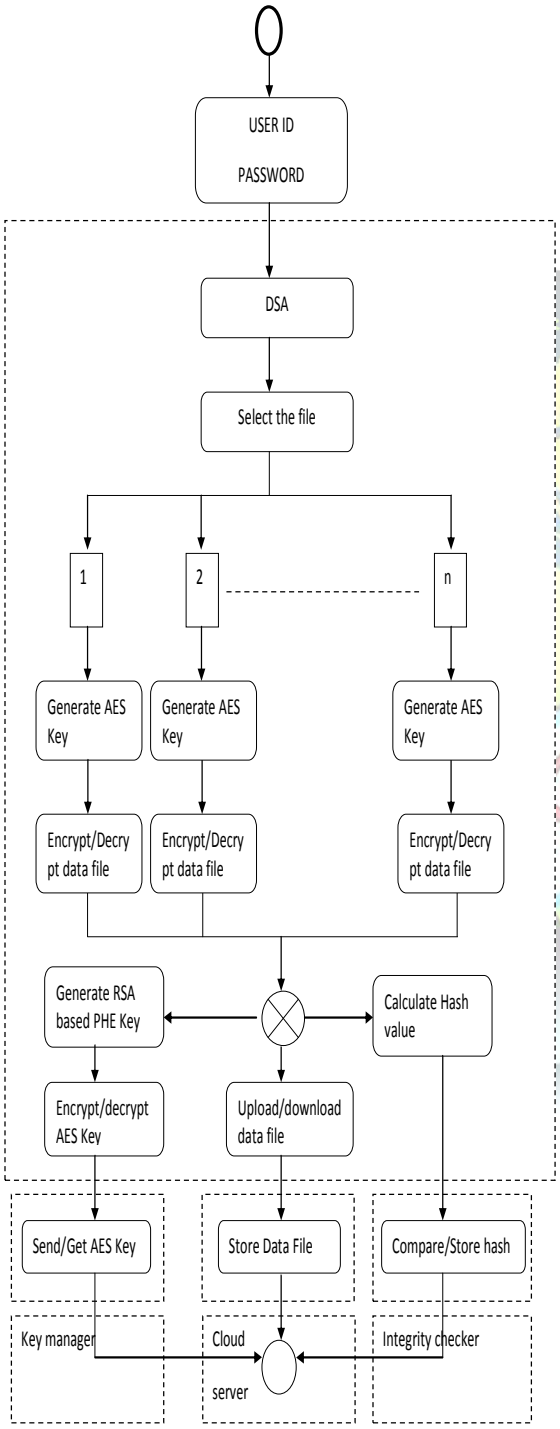
Cloud workspace:

It is the server side module which is used to store the encrypted data file and key values.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

The cloud workspace provides storage for the uploading/downloading data files.

IV. ARCHITECTURE DESIGN:



Figno.1.System's architecture

The figno.1 shows the system architecture and design of the proposed model. The proposed architecture of the system provides the detailed design and workflow of the prototype model.

Implementation of the system:

The user is validated using the unique user id and password. Then, the user's digital signature has been verified using DSA algorithm. After, validating the user he/she can upload/download the data file. Once the user upload the data file, it will be split into multiple segments having equal size, then these data segments are encrypted simultaneously using AES-128 bit algorithm. After completing the encryption process the encrypted files are merged into a single file and stored in cloud server.

RSA based partial homomorphic encryption technique is used to generate RSA key for the particular AES encryption key [1]. Finally, these encrypted key has been stored in the cloud server. While retrieving the data from cloud, the integrity of the data can be verified using hash value comparison [1]. To verify the integrity of the data, the meta data will also be used [2].

V. CONCLUSION AND FUTURE WORKS

Cloud computing is the emerging technology in recent trends and it has some security issues while providing global access to the data. This paper presented a prototype system which maintains data integrity and privacy simultaneously and also increases the efficiency of the system.

In this system RSA algorithm is used to encrypt the AES key for an easy implementation. The security of the system may enrich by using some advanced techniques instead of RSA algorithm. By using advanced encryption techniques the efficiency of the system can be improved.

VI. RERENCES

[1] Mohammed Faez Al-Jaberi and AnazidaZainal,"Data Integrity and Privacy Model in Cloud Computing", International Symposium on Biometrics and Security Technologies,2014

[2] ChandrashekharS.Pawar,PankajR.patil,Sujitkumar V.Chaudhari, "Providing Security and Integrity for Data Stored in Cloud Storage",2014

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

[3] Manpreet kaur, Rajbir Singh, " Implementing encryption Algorithms to Enhance Data Security of Cloud Computing ", International Journal of Computer Applications, Vol 70 – No 18, May 2013

[4] GarimaSaini, Naveen Sharma, "Triple Security of Data in Cloud Computing " on 2014.

[5] http://www.interoute.com/cloud-article/what-private-cloud

[6] https://en.wikipedia.org/wiki/Network_security

[7] http://searchcloudstorage.techtarget.com/definition/community-cloud

[8] http://aesencryption.net/