Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing

Mr. Prashant Rewagad[*1]
HOD, Dept of Computer Science & Engineering
G.H.Raisoni Institute of Engg and Management
Affiliated to North Maharashtra University
Jalgaon, India
prashant_rewagad@rediffmail.com

Ms.Yogita Pawar[*2]
M.E Student, Dept of Computer Science & Engineering
G.H.Raisoni Institute of Engg and Management
Affiliated to North Maharashtra University
Jalgaon, India
pawaryogita04@gmail.com

Abstract—**Cloud computing is the apt technology for the decade. It allows user to store large amount of data in cloud storage and use as and when required, from any part of the world, via any terminal equipment. Since cloud computing is rest on internet, security issues like privacy, data security, confidentiality, and authentication is encountered. In order to get rid of the same, a variety of encryption algorithms and mechanisms are used. Many researchers choose the best they found and use it in different combination to provide security to the data in cloud. On the similar terms, we have chosen to make use of a combination of authentication technique and key exchange algorithm blended with an encryption algorithm. This combination is referred to as "Three way mechanism" because it ensures all the three protection scheme of authentication, data security and verification, at the same time. In this paper, we have proposed to make use of digital signature and Diffie Hellman key exchange blended with (AES) Advanced Encryption Standard encryption algorithm to protect confidentiality of data stored in cloud. Even if the key in transmission is hacked, the facility of Diffie Hellman key exchange render it useless, since key in transit is of no use without user's private key, which is confined only to the legitimate user. This proposed architecture of three way mechanism makes it tough for hackers to crack the security system, thereby protecting data stored in cloud.**

Keywords- Cloud Computing, AES Algorithm, Data Cofidentiality

I. INTRODUCTION

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[5]. Cloud computing is new utility of the century, which many enterprises wants to incorporates in order to improve their way of working. It implies sharing of computing resources to handle applications. Cloud computing offers reduced capital expenditure, operational risks, complexity and maintenance, and increased scalability while providing services at different abstraction levels, namely Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS)[6]. It is used in consumer-oriented applications such as financial portfolios delivering personalized information, or power immersive computer games. It is a pay as peruse kind of service, hence has become very popular in very less time.

Since cloud computing is a utility available on net, so various issues like user privacy, data theft and leakage, eaves dropping, unauthenticated access and various hackers' attacks are raised. These unsolved security issues of authentication, privacy, data protection and data verification are main hindrance for widespread adoption of cloud computing. Hence to get a overwhelmed acceptance to cloud computing in finance, market and industry as well, we have proposed a secure architecture for it. Under the above mentioned title, I am incorporating three security control mechanisms viz authentication, Encryption and data verification technique in to a single stand alone system. Hence it is a three ways protection scheme wherein digital signature provides authentication, encryption algorithm provides session encryption key and is used to encrypt user data file as well, which is to be saved in cloud and lastly trusted computing to verify integrity of user data.

II. PROBLEM STATEMENT

With cloud computing, organizations can use services and data is stored at any physical location outside their own control. This facility raised the various security questions like privacy, confidentiality, integrity etc and demanded a trusted computing environment wherein data confidentiality can be maintained. To induce trust in the computing, there is need of a system which performs authentication, verification and encrypted data transfer, hence maintaining data confidentiality.

TABLE 1: Types of Attacks [8]

Name of Attack	Description
Tampering	An attacker may alter information either stored in local files, database or is sent over public network.
Eavesdropping Information Disclosure	This type of attack occurs when attacker gains access in the data path and gains access to monitor and read the messages.
Repudiation	Sender tries to repudiate, or refute the validity of a statement or contract which is sent by him/her.

978-0-7695-4958-3/13 $26.00 © 2013 IEEE
DOI 10.1109/CSNT.2013.97

Elevation of Privileges	An attacker may access unauthorized to information and resources
Man-in-the-Middle Attack	This type of attack occurs when an attacks infiltrates the communication channel in order to monitor the communication and modify the messages for malicious purposes
Replay Attack	A replay attack is defined as when an attacker or originator sends a valid data with intention to use it maliciously or fraudulently.
Identity Spoofing	Identity spoofing occurs when an attacker impersonates the users as the originator of the message in order to gain access on a network.
Differential Analysis Threat	When new versions are released, a differential analysis of the new and old version would indicate where differences in the code exist
Viruses and Worms	Viruses and worms are very common and well known attacks. These are piece of code that decrease the performance of hardware and application even these malicious codes corrupts files on local file system

III. Related Works

As per Uma Somani, Kanika Lakhani and Manish Mundra [1]: In Cloud computing, we have problem like security of data, files system, backups, network traffic, host security .They have proposed a concept of digital signature with RSA algorithm, to encrypt the data while transferring it over the network. This technique solves the dual problem of authentication and security. The strength of their work is the framework proposed to address security and privacy issue.

Volker Fusenig and Ayush Sharma [2]: states a new approach called cloud networking which adds networking functionalities to cloud computing and enables dynamic and flexible placement of virtual resources crossing provider borders. This allows various kinds of optimization, e.g., reducing latency or network load. This paper presents a security architecture that enables a user of cloud networking to define security requirements and enforce them in the cloud networking infrastructure.

As per Deyan Chen and Hong Zhao [3] from the consumers' perspective, cloud computing security concerns are specially data security and privacy protection issues which remain the primary inhibitor for adoption of cloud computing services. They provided a concise but all-round analysis on data security and privacy protection issues associated with cloud computing across all stages of data life cycle. Then they proposed to protect data using various scheme and policies like airavat etc. This system can prevent privacy leakage without authorization in Map-Reduce computing process. The weakness is that it just a theory which depends on other scheme and policies for its implementation.

As per Eman M.Mohamed and Hatem S. Abdelkader [8] Cloud computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique feature, however, raises many new security challenges. Every cloud provider solves this problem by encrypting the data by using encryption algorithms. Thus their paper investigates the basic problem of cloud computing data security. They presented the data security model of cloud computing based on the study of the cloud architecture. They implemented software to enhance work in a data security model for cloud computing. Finally they applied this software in the Amazon EC2 Micro instance for evaluation process.

G. Jai Arul Jose, C. Sajeev, and Dr. C. Suyambulingom [9]: proposed to generate RSA Public keys and Private Keys for public and private access to overcome the problem of data security. Certificate Binary file is used inside control node configuration file to make sure cloud data flow securely. The control node sends data through Secure Socket Layer after certificate activation. Finally AES algorithm is used for encryption .This unique combination makes this solution best to prevent different types of attacks. The strength of their work is strong data security against various attacks. If a user is attempt to login falsely for many times, the system automatically slowing the service and temporarily stop the account service for the particular user.

IV. Proposed System

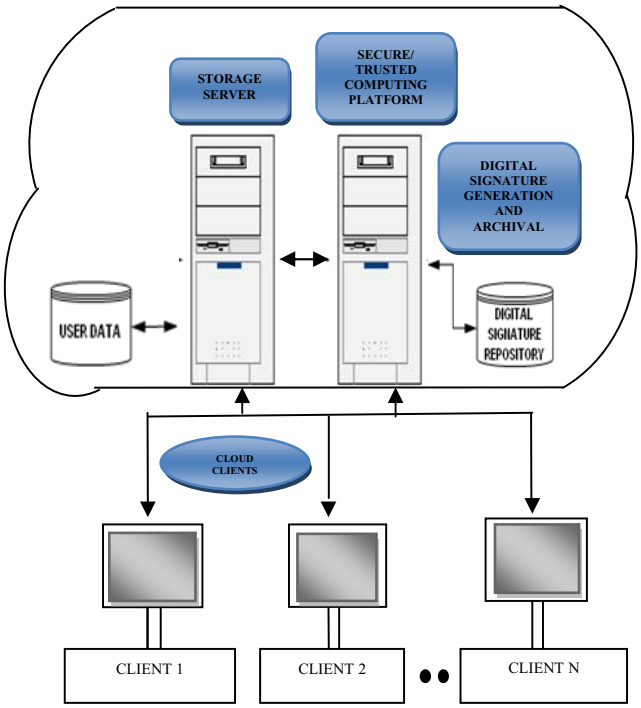

Figure 1. Proposed Architecture

In our proposed architecture, we are using three ways protection scheme. Firstly Diffie Hellman algorithm is used to generate keys for key exchange step. Then digital signature is used for authentication, thereafter AES encryption algorithm is used to encrypt or decrypt user's data file. All this is implemented to provide trusted

computing environment in order to avoid data modification at the server end. For the same reason two separate servers are maintained, one for encryption process known as (trusted) computing platform and another known as storage server for storing user data file.

When a user wants to upload a file to the cloud server, first key are exchanged using Diffie Hellman key exchange at the time of login, then the client is authenticated using digital signature. Finally user's data file is encrypted using AES and only then it is uploaded to another (cloud) Storage server. Now when client is in need of same file, it is to be downloaded from cloud server. For that purpose, when user login, first encryption keys are exchanged, file to be downloaded is selected, authentication takes place using digital signature then, AES is used to decrypt the saved file and client can access the file.

A. Execution Steps:

1. Sign up
2. Login from TCP
   - 2.1 Key Exchange – Diffie Hellman
   - 2.2 Digital Signature –SHA-I
3. Uploading / Downloading Data Encryption- AES
4. Data is stored / retrieved from Storage server
5. Logout.

B. Hardware specification:

The system running the application should have following minimum requirements:

1. Pentium Core.
2. RAM Size 128mb.
3. Processor 1.2GHz.

C. Software specification:

The system running the application must have the following:

1. Supporting OS: Windows XP, VISTA, LINUX: Red Hat, Ubuntu, Fedora.
2. Java Development Kit - jdk1.6.0_02.
3. Java Runtime Environment - jre1.6.0_06.
4. Web Browser like Google chrome with Java Plug-in installed.
5. Wireless connectivity driver.

D. Technology Specific Tools used

In this work we use following technology tools:

1. Java Development Kit - jdk1.6.0_02.
2. Java Runtime Environment - jre1.6.0_06.
3. Java.awt package for layout of the applet.
4. Java.net package for connection settings and message passing.
5. Netbeans
6. Java Web Start.
7. SOAP.
8. Glassfish Server.
9. Socket Options interface of methods to get/set socket options.

REFERENCES

[1] Uma Somani, Kanika Lakhani, Manish Mundra "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing" 2010 IEEE 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).

[2] Volker Fusenig and Ayush Sharma "Security Architecture for Cloud Networking" 2012 IEEE International Conference on Computing, Networking and Communications, Cloud Computing and Networking Symposium.

[3] Deyan Chen and Hong Zhao "Data Security and Privacy Protection Issues in Cloud Computing" 2012 IEEE International Conference on Computer Science and Electronics Engineering.

[4] Zhang Xin , Lai Song-qing and Liu Nai-wen "Research on Cloud Computing Data Security Model Based on Multi-dimension" 2012 IEEE International symposium on information Technology in medicine and education.

[5] Farhan Bashir Shaikh and Sajjad Haider "Security Threats in Cloud Computing" 2011 IEEE 6th international conference on Internet Technology and secured transactions, 11-14 December 2011, Abu Dhabi United States of Arab Emirates.

[6] Balachandra Reddy Kandukuri, Ramacrishna PaturiV, Atanu Rakshi, "Cloud Security Issues" 2009 IEEE International Conference on Services Computing.

[7] Ayesha Malik and Muhammad Mohsin Nazir "Security Framework for Cloud Computing Environment: A Review" in Journal of Emerging Trends in Computing and Information Sciences VOL. 3, NO. 3, March 2012.

[8] Sherif el-etriby , Eman m.Mohamed and Hatem s. Abdelkader published "Modern Encryption Techniques for Cloud Computing Randomness and Performance Testing " in the third international conference on communications and information technology ICCIT 2012.

[9] G. Jai Arul Jose, C. Sajeev, Dr. C. Suyambulingom "Implementation of Data Security in Cloud Computing" International Journal of P2P Network Trends and Technology- Volume1 Issue1- 2011 .

[10] Mohamed Al Morsy, John Grundy and Ingo Müller "An Analysis of The Cloud Computing Security Problem" Proceedings of APSEC 2010 Cloud Workshop, Sydney, Australia,30thNov2010.