IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

ENCRYPT DATA USING DIGITAL SIGNATURE WITH DIFFIE HELLMAN AND AES FOR DATA SECURITY

Asmita*, Abdul Quadir Md

* School of Computer Science VIT University, Chennai, India

Assistant Professor, School of Computer Science VIT University, Chennai, India

ABSTRACT

Data is stored online in cloud computing. Cloud computing is a model for requirement to access a shared pool of configuration computing resource. In cloud computing all stored data is managed online by remote servers. In cloud the entire service is done online by third person so there is a possibility of data hacked, many security problems like data lost, data stolen or data changed are there in cloud computing. This paper proposed Diffie Hellman with AES key encryption and Digital Signature. It is known three protection scheme i.e. authentication, data encryption and data verification at the same time. So that we can know about the verification of the data. We encrypt data before send so that if man in middle attack on data in between it is not understandable by attacker.

KEYWORDS: Cloud Computing, Diffie Hellman, Digital Signature, AES Algorithm, Data Authentication

INTRODUCTION

In cloud computing many servers connected through internet that allows online data storage and data access. Cloud is classified into three classes public, private, hybrid. work a day we use cloud computing services but people usually did not know about this for example online data storage, g-mail, drop drive etc. The conception of cloud computing is mystery till now.

Cloud computing is the result of progress and advocacy of existing technologies. The goal of cloud computing is to allow users to take benifit from all of these technologies, without the need of deep familiarity about each one of them. Cloud computing increase scalability and reduce cost. Cloud computing is classified into three types i.e. SaaS(software as a service), PaaS(platform as a service), IaaS(infrastructure as a service).

SaaS is a software delivery methodology that provides multiple accesses to software and its functions remotely as a Web-based service. SaaS is a scalable architecture. IaaS is the delivery of technology infrastructure as an on demand scalable service. Iaas can be coupled with Managed Services for OS and application support. PaaS provides all of the facilities required to guide the complete lifecycle of building and delivering web application and services entirely from the internet.

Since all process in cloud computing development online, therefore many security arguments like data privacy, data stolen, data leakage and unauthorized access present in cloud computing. These unsolved security problem of privacy, data protection, data verification are main problem for widespread adoption of cloud computing. In this paper I am using three security control mechanism i.e. authentication, data verification and data verification. All these technique used in well organized manner in a single system. So it is called three way mechanisms. In which digital signature provides verification i.e. we can find out that data was sent by sender or hacker, encryption algorithm maintain session encryption key and it is used to encrypt the sender data so that if hacker attack in between he cannot understand the data and in last trusted computing to verify integrity of user data.

Overview of algorithms:

a. Diffie Hellman.
b. AES algorithm.
c. Digital signature.

In Diffie Hellman sender and receiver agree upon a key for data that would be exchanged between them.

1. Sender and receiver select two prime no.
    2. Sender picks a random no a and sends g
    3. Receiver picks a random no b and sends gb to sender.
    4. Sender computes (gb)a.
    5. Receiver computes (ga)b.

In AES algorithm is a symmetric block cipher. This means that it uses the same key for both encryption and decryption the AES standard states that the algorithm can only accept a block size of 128 bits and a choice of three keys - 128, 192, 256 bits.

In digital signature we can check the authentication and integrity of a document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message and that the message was not altered in between.

PROBLEM STATEMENT

All data is stored on clouds online. On cloud all service handled by mediator. There are many security question in cloud computing like privacy. There are many types of attacks like

1. Tempering: In this attacker change the data or make it public.
2. Elevation of privileges: In this type of attack attacker access data through unauthorized access. Sender and receiver don’t know anything about this.
3. Man in middle attack: In this type of attack attacker keeps his eyes on the communication channel and modify the data for malicious purpose.
4. 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.

EXISTING METHODOLOGY

As per Yogita Pawar[1]: First 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.

As per Dhaval Patel[2]: First they use Diffie Hellman algorithm for key exchange and then AES encryption algorithms. Digital signature is responsible for the authentication and they use SHA as a hashing algorithms for the computing the signature and AES as encryption algorithms.

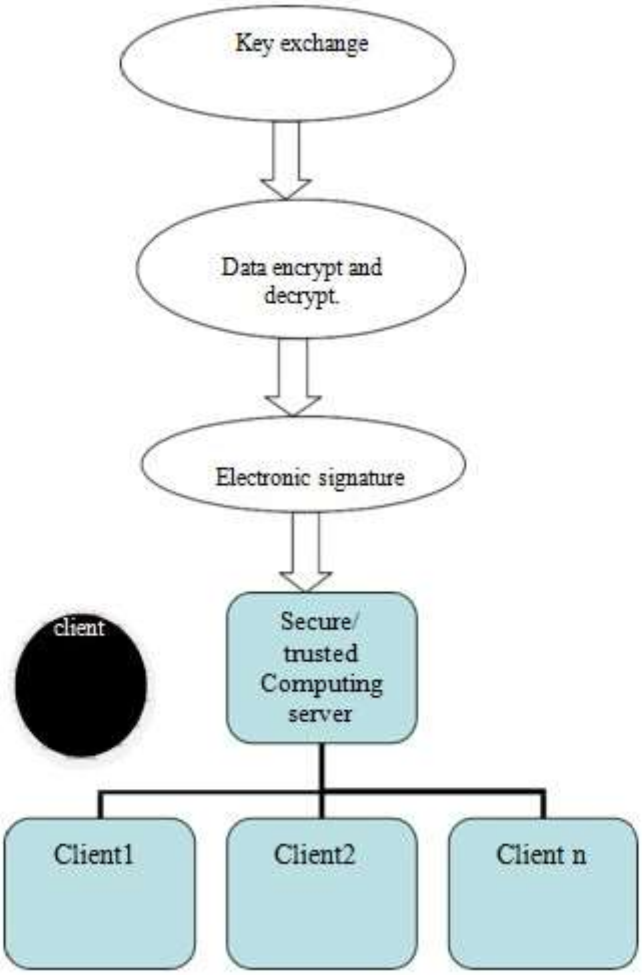
As per Deyan Chen[3]: Cloud computing security concerns are specially data security and privacy protection issues which remain the primary inhibitor for adoption of cloud computing services. They provided a concise but all-round analysis on data security and privacy protection issues associated with cloud computing across all stages of data life cycle. Then they proposed to protect data using various scheme and policies. This system can prevent privacy leakage without authorization in Map-Reduce computing process.

As per Volker Fusenig and Ayush Sharma[4]: This paper proposed a security architecture that enables a user of cloud networking to define security specification and enforce them in the cloud networking framework.

As per Parsi Kalpana and Sudha Singaraju[5]: User data is encrypted first and then it is stored in the Cloud. When essential, user places a request for the data for the Cloud provider, Cloud provider authenticates the user and delivers the data.

PROPOSED SYSTEM

In this proposed paper first i used the diffie hellman for key exchange then we encrypt and decrypt the data using AES encryption algo after that I used the digital signature for authentication. If the two user wants to connect with each other then they have to exchange the key first by using diffie hellman then they have to encrypt the data by using AES encryption algo then they use digital signature for verification. By this hacker can not hack the data and if hacker hacked the data he can not figure out it because it is in encrypted form. Then we store the data on clouds. If attacker approach the data first the system will investigate about the key if attacker use the wrong key it will not open. By using digital signature we can easily examine that the data was sent by the sender or not.



REFERENCES

[1] Ms Yogita Pawar "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing" 2013 International Conference on Communication Systems and Network Technologies.

[2] Dhaval Patel "DATA SECURITY IN CLOUD COMPUTING USING DIGITAL SIGNATURE" International journal for technological Research in Engineering.

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

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

[5] Parsi Kalpana and Sudha Singaraju " Data Security in Cloud Computing using RSA Algorithm" International Journal of Research in Computer and Communication technology.