International Journal For Technological Research In Engineering
Volume 1, Issue 10, June-2014 *ISSN (Online): 2347 - 4718*

DATA SECURITY IN CLOUD COMPUTING USING DIGITAL SIGNATURE

Dhaval Patel[1] (ME scholar), M.B.Chaudhari[2] (HOD)
Computer Science and Engineering Department
Government Engineering College, Gandhinagar, Gujarat, India.

Abstract: The cloud is a next generation platform that provides dynamic resource pools, virtualization, and high availability. Cloud computing is a way to increase the capacity or add capabilities dynamically without investing in new infrastructure or licensing new software. Since cloud computing is rest on internet, various security issues like privacy, data integrity, confidentiality, authentication and trust encounter. Different encryption algorithms are applied for reducing the security risk in cloud network. On the similar terms in my system we use combination of authentication techniques and key exchange algorithms blended with the encryption algorithms. This combination is referring as the "three step mechanism" because it ensures data authentication, data integrity and data confidentiality. In this paper I choose digital signature and Daffier Hellman key exchange blended with AES algorithms to protect confidentiality on cloud.

Index Terms: Cloud computing, AES algorithms, data confidentiality

I. INTRODUCTION

Cloud computing is a large-amount of distributed computing paradigm driven at economics scale, in which a pool of abstracted, virtualized, dynamically-scalable, highly available and configurable and reconfigurable computing resources can be rapidly provisioned and released with minimal effort in the data centers. According to NIST "cloud computing is a model for enabling 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"[3][10]. Cloud computing is internet based computing environment where software, infrastructure, platform, devices and other resources and hosting to computers are provided as services on a pay-per-as-you-use basis to consumer.

II. CLOUD COMPUTING SERVICE MODEL

In the cloud computing, the available service models are:

- Infrastructure as a Service (IaaS): This model allows user to rent processing, storage, network and other resources. The user can deploy and run the guest OS and application.[2] The user does not manage of control the underlying cloud infrastructure but has control over only OS, storage and deployed application and possibly selected networking components. Examples include Amazon Elastic Computer Cloud (EC2), Microsoft Windows Azure.
- Platform as a Service (PaaS): Provides the consumer with the capability to deploy onto the cloud infrastructure, consumer created or acquired applications, produced using programming languages and tools supported by the provider [2]. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations. Examples include Google's Apps Engine, Microsoft- Windows Live. Open shift, etc.
- Software as a Service (SaaS): Provide the user with the capability to use the provider's applications running on a cloud infrastructure. The applications are accessible from various consumer devices, through a thin client interface, such as a web browser. [2] The consumer does not manage or control the underlying cloud infrastructure various resources. Examples include Salesforce.com, VoIP from Skype and Vonage, Google's Gmail and Apps, instant messaging from Yahoo and AOL.

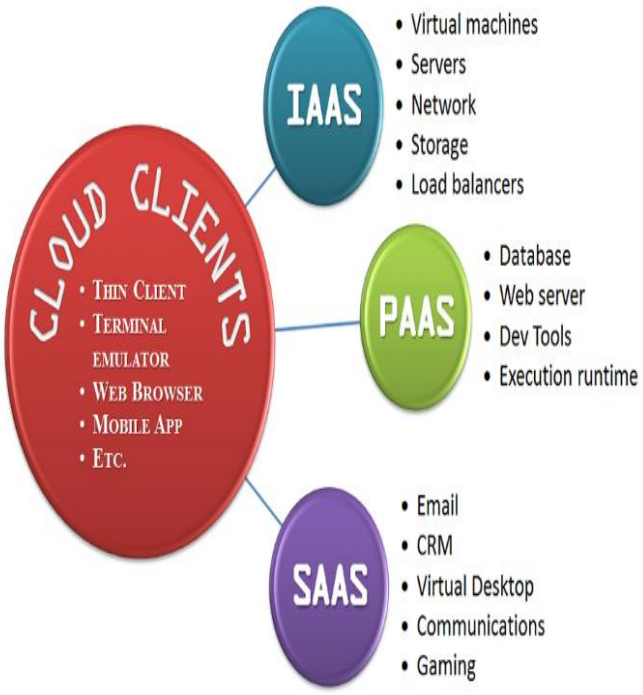

Fig. 1: Service Model of Cloud computing

III. DEPLOYMENT MODEL OF CLOUD COMPUTING

Four deployment models have been identified for cloud computing architecture solution:

- Private cloud: The cloud infrastructure is operated for a private organization. It may be managed by the organization or a third party, and may exist on premise or off premise.[4][9]
- Community cloud: The cloud infrastructure is shared by several organizations and supports a specific community that has communal concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party, and may exist on premise or off premise.[4]
- Public cloud: A public or external cloud is a general-purpose cloud computing environment managed by a cloud provider.[8] The cloud provider could be external provider, such as Amazon EC2, Google Apps, Salesforce, etc. that leases third-party cloud resource to the consumer. However, a cloud could be public even when third party cloud resources are not used; the most important aspect of a public cloud is its content.
- Hybrid cloud: The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology, that enables data and application portability. [4]

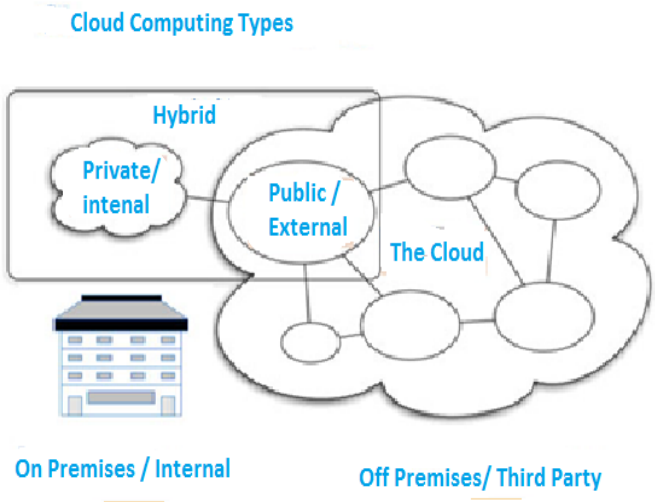

Fig. 2: Deployment model of cloud computing

IV. PROBLEM STATEMENT

In cloud computing, organizations can use services and data is stored at any physical location outside their own control. This facility creates the various security issues 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.

Name of Attacks	Description
Tampering	An attacker may alter information either stored in local files, database or is sent over public network.
Repudiation	Sender tries to repudiate, or refute the validity of a statement or contract which is sent by him/her.
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.
Identity snoofing	Identity spoofing occurs when an attacker impersonates the users as the originator of the message in order to gain access on a network.

TABLE 1: Types of attacks

V. RELATED WORK

As per Uma Somani, Kanika Lakhani and Manish Mundra [1]: In cloud computing we have problem like security of data, file system, backup, host security. They have proposed a concept of digital signature with RSA algorithms to encrypt the data while transferring it over network. This technique solves the dual problem of authentication and confidentiality. As per Shobha Rajak, Ashok Verma [5]: In this paper, data security in cloud by the digital signature with the help of CFX_MF algorithms is given. In this digital signature is used for the authentication and non-repudiation of message, both the identity of sender and the integrity of the message content. In this integrity check over the cloud computing performed by TPA which examine the data from user and extract the request of unauthorized user. K. Govinda, Dr.E.Sathiyamoorthy [6]: identity based secure data transfer in cloud using GDS (Group Digital Signature) is introduced. In this schema the group manager communicate with the cloud provider using the secret key generated using the Diffie Hillman key exchange algorithms. Now the group manager receives the member (user in the group) public key. For member who sends the data to the cloud server it can sign the message with the assigned (d, n) private key. Now the message is received by the group manager authenticate the member and then collect the required detail and attach the secret group id and sign and send to the cloud provider. Cloud provider authenticates the message and allows the encrypted message to store in private cloud. Deyan Chen and Hong Zhao [7]: from the consumers perspective cloud computing security concerns are specifically data security and privacy protection issues which remain the primary inhibitor for the 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 the all the stages of data life cycle. The weakness is that it is theory which depends on other schema and polices for its implementation.

VI. PROPOSED SYSTEM AND RESULT

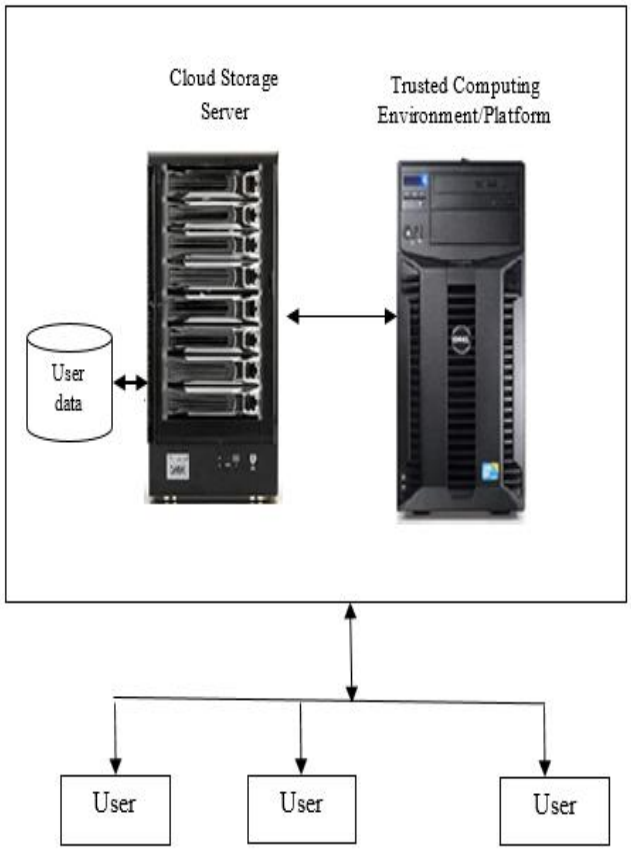

Fig. 3: Proposed model

In our system we use trusted computing platform for performing the operation like user authentication, data verification. In our system we use three way protection scheme in which first we use Diffie Hell-man algorithms for key exchange algorithms for the AES encryption algorithms. Digital signature is responsible for the authentication and we use SHA as a hashing algorithms for the computing the signature and AES as encryption algorithms.

File Uploading Process (Encryption operation):

1. Client can generate the message digest using the SHA hashing algorithms and sign it using the private key (d, n) of RSA algorithms.
2. Now the data is encrypted using the AES encryption algorithms with secret key.
3. The computing server now verify the signature and stored the file to the storage server.

File Downloading Process (Decryption operation):

1. Computing server retrieve the file from storage server according to the client request.
2. Now perform the decryption operation and extract the signature
3. Now compute the signature and verify it. If it is successfully verified then data is stored at the client side otherwise modification is detected and data is stored at the client side.

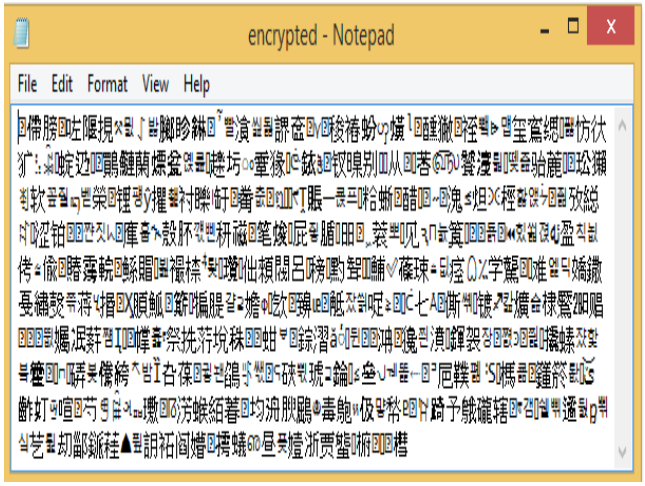

Fig. 4: Encrypted Data

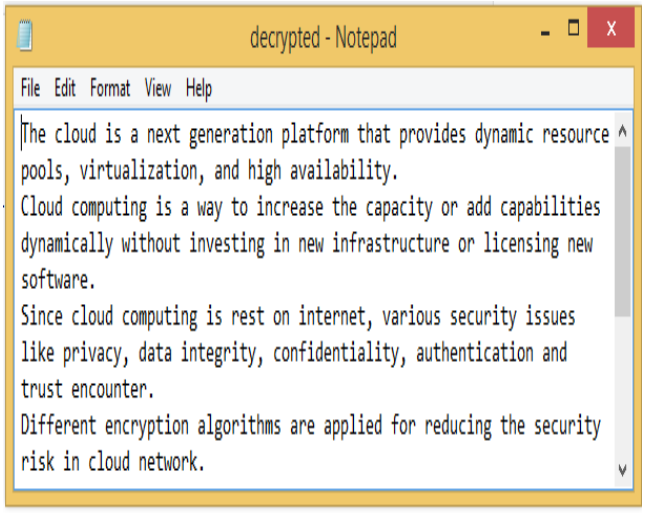

Fig. 5: Decrypted Data

In the below figure we show the performance of our system with the different data encryption algorithms with respect to encryption time.

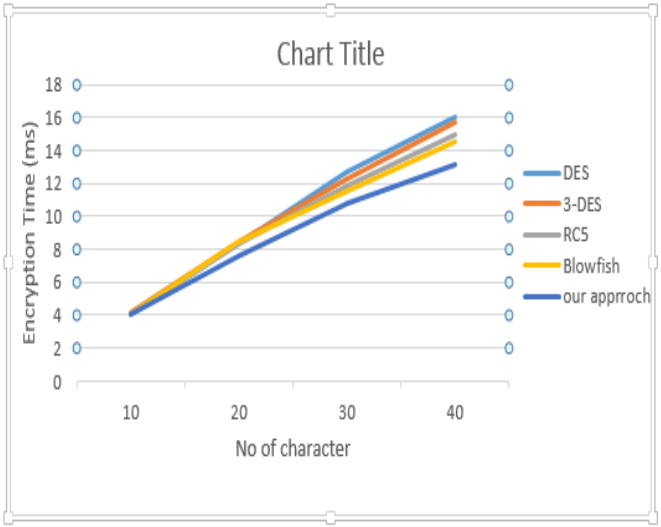

Fig. 6: Comparison of encryption time

VII. CONCLUSION

Cloud computing is the apt technology for the last decade. It allow user to store their data in cloud storage and use when required. So cloud is rest on internet, various security issues like privacy, confidentiality, authentication and integrity is encountered. I will review many authentication and encryption algorithms for data security in cloud network. We proposed and implement the digital signature for authentication and AES as encryption algorithms for data security in cloud computing. So this system more secures than the existing system which uses symmetric encryption algorithms RC4, Blowfish, 3DES, DES etc. In future we can optimize efficiency of system by reducing size of key for encryption and check the performance with the proposed algorithms.

REFERENCES

[1] Uma Somani, Kanika Lakhani and Manish Mundra "Implementing Digital Signature with RSA Encryption Algorithms to Enhance the Data Security of Cloud in Cloud computing" IEEE 2010
[2] Dimitrios Zissis, Dimitrios Lekkas "Addressing cloud computing security issues" 2010 Future Generation Computer Systems (Science Direct)
[3] http://en.wikipedia.org/wiki/Cloud_computing
[4] S. Subashini, V. Kavita "A survey on security issues in service delivery model of cloud computing" 2010 Journal of Network and Computer Applications (Science Direct)
[5] Shobha Rajak, Ashok Verma "Secure Data Storage in the Cloud using Digital Signature Mechanism" IJARCET June 2012
[6] K. Govinda, Dr. E. Sathiyamoorthy "Identity Anonymization and Secure Data Storage using Group Signature in Private Cloud" Science Direct 2012
[7] Devan Chen and Hong Zhao "Data security and Privacy Protection Issues in Cloud Computing " IEEE 2012
[8] C. Onwubiko "Security issues in Cloud computing" Principles, Systems and Applications, Computer Communications and Networks – (Springer)
[9] Defining Cloud Deployment Models, http://bizcloudnetwork. Com/defining-cloud-deployment -models/
[10] Security Guidance for Critical Areas of Focus in Cloud Computing V2.1 Prepared by Cloud Security Alliance December 2009

