iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** III **Month of publication:** March 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 3 Issue III, March 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Digital Signature and Advanced Encryption Standard for Enhancing Data Security and Authentication in Cloud Computing

Nikhitha K. Nair[1], Navin K.S. [2], Soya Chandra C.S.[3]
Department of Computer Science and Engineering,
[1,3]*Sarabhai Institute of Science and Technology, Vellanad, Thiruvananthapuram-695543*
[2]*L.B.S. College of Engineering, Poojapura Thiruvananthapuram- 695012*

Abstract--- Cloud computing refers to distributed computing over the network. This means that the ability to execute an application or program over many computers at the same time. The data security issues are one of main concern while dealing with the cloud data. Different encryption techniques attempt to overcome these data security issues to a great extent. Advanced Encryption Standard (AES) is a commonly used symmetric key encryption algorithm used for encrypting the data to be stored in the cloud. Another problem which has a prominent role while dealing with cloud data is authentication. Digital signatures are used for verifying the authentication of the document send by the sender for sharing with the recipients.
Keywords: Cloud computing, Data Security, Authentication, AES and Digital Signature

I. INTRODUCTION

Cloud computing is an emerging and important epitome in which services can be assigned to various network connections, software or other services over the network. Cloud computing is basically a virtual pool of resources and these resources are provided to various users over the Internet. Some of prevalent problems associated with cloud computing include data privacy, data reliability, authentication, quality of service. Among these problems, data security and authentication are most critical and challenging. The domain covered under the cloud computing includes:

A. Software as a Service.
B. Platform as a Service.
C. Infrastructure as a Service.

In Software as a Service (SaaS), providers licenses to various software to customers according to their demand in pay-as-you-go model or at no charge. commercial software, software is managed from a central location and users are not required to handle various software upgrades and software patches.
Some of the characteristics of SaaS include providing web access to commercial software, software is managed from a central location and users are not required to handle various software upgrades and software patches.

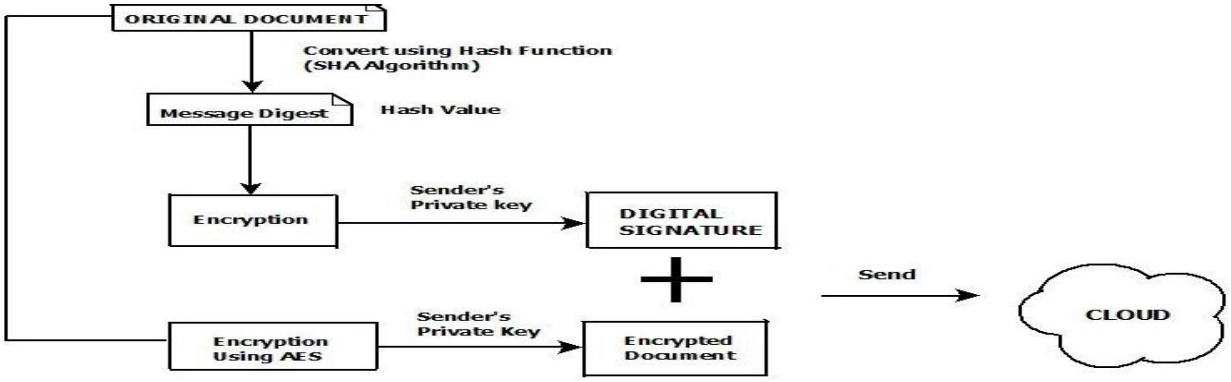


Fig.1. Working model

©IJRASET 2015: All Rights are Reserved

In Platform as a Service (PaaS), provides the computing platform that helps in creating web applications easily and quickly without the requirement of buying and maintaining the software and the infrastructure underneath. Some of the characteristics of PaaS include providing the facility to use web based user interface creation tools to create, modify, test and deploy various user interface scenarios, providing integration with various web services and databases through internet and multiple concurrent users can use the same developed applications. In Infrastructure as a Service (IaaS), provides a way for delivering cloud computing infrastructure servers, networks, storage and operating systems as an on-demand service. Some of the characteristics of IaaS include resources are being distributed as a service, generally includes multiple users on a single piece of hardware and it allows dynamic scaling. The main challenging problem while dealing with cloud computing is data security issues. The field of cloud computing is worthwhile only if data owners can store their data in a secured way. Encryption is the prominent solution to handle data security issues when dealing with the cloud data. Different encryption algorithms that are being used in these days included Data Encryption Standard (DES), Exclusive-OR (XOR), Advanced Encryption Standard (AES), RSA and Homomorphic encryption schemes. To enhance security on data stored in the cloud, different encryption schemes can be used at a time. Dual encryption enhances data security than single encryption since expert users are difficult to hack the original data. Authentication is another important requirement while sharing information among users. Signatures help to ensure that a particular message or data belongs to the respective sender. Digital signatures play a central role in verification of the sender of a document's identity. The signature for a particular document is created with the help of the private key of the sender. Using the public key of the sender, then only receiver can get the original document sent by the sender.

II. SECURITY ISSUES IN CLOUD COMPUTING

Some of security issues while dealing with cloud computing includes:

A. Confidentiality of data

In cloud computing, privacy of data has real influence particularly in administering of cloud service providers control over various users information stored in various appropriate databases.

B. Identification and Authentication

Authorization is a vital security requirement in cloud computing to ensure whether referential integrity is maintained or not. So client profile, username and password must be checked for authentication.

C. Non-repudiation

The sender who signed the document cannot repudiate the signature at a later time. Also the receiver of the digitally signed document can prove to the third party that the document was signed by the sender who it is claimed to be signed by.

III. PROBLEM FORMULATION

The problem is that when the data owners who upload documents in the cloud for storage, there can hackers who can hack the original documents and tamper those documents. The most prominent solution to this problem is use of encryption techniques to enhance data security. One of the most commonly used encryption techniques is Advanced Encryption Standard (AES) which is a symmetric key encryption scheme. Symmetric encryption techniques uses same key for both encryption and decryption purpose. Another problem in cloud data is authentication of documents send by the sender to the receiver. Digital signatures play a vital role in providing authentication and non-repudiation .The Non-repudiation means that the sender who signed the document cannot repudiate the signature at a later time. Also the receiver of the digitally signed document can prove to the third party that the document was signed by the sender who it is claimed to be signed by.

IV. ENCRYPTION TECHNIQUE FOR ENHANCING DATA SECURITY.

The most commonly used encryption standard is Advanced Encryption Standard. It is a Symmetric key encryption scheme. That is, same key is used by the sender to encrypt the document and by the receiver to decrypt the encrypted document to obtain the original document. AES encryption scheme is a block cipher algorithm which operates on 128- bit data blocks which supporting three different cipher key lengths of 128, 192 and 256 bits. These three flavors of AEs algorithm are also referred as AES-128, AES-192 and AES-256 for 128,192 and 256-bit cipher keys respectively. During the encryption process, each round is composed of a set of four basic operations. The decryption process applies the inverse of these operations in the reverse order. The basic operations include: adding round key, mixing the columns, shift the rows and substitution of bytes. In AES

©IJRASET 2015: All Rights are Reserved

encryption, same key (private key) is used for encrypting and decrypting the document. So only if the receiver knows the private key of the sender, then only he/she can decrypt the encrypted message send by the sender. This enhances security on data stored by the sender to the cloud.

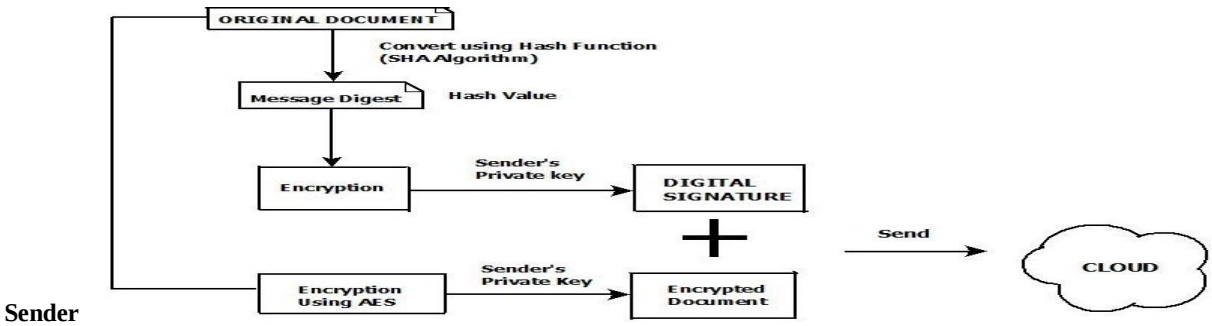
V. DIGITAL SIGNATURES FOR AUTHENTICATION

Digital signatures are mainly used for detecting unauthorized modifications to data. The digital signatures are generated with the help of a private key. The private key is known only to the sender. The digital signature is verified by the receiver by making use of the public key. Private key which is known only to the sender and never shared can be used for the process of signature generation and the public keys which are known to everyone can be used in the process of signature verification. Digital signatures also play an important role in proving to the third party that document was signed by the original sender. This is known to be as non-repudiation because the sender of the document who signed the document cannot repudiate the signature later. There are three algorithms that are suitable for generating digital signatures under Digital Signature Standard (DSS) which include DSA (Digital Signature Algorithm), RSA algorithm and Elliptical Curve Digital Signature Algorithm. Also a hash function is used under this standard for signature generation. This hash function which is to obtained is a condensed version of the data, which is called message digest. This message digest is then put into the Digital Signature Algorithm to generate a digitally signed message. The same hash function is used in the signature verification process. The hash function which is used in the Digital Signature Standard is specified in the Secure Hash Standard (SHS), which are specifications for the Secure Hash Algorithm (SHA). When the input message which if of length less than $2^{64,}$ then SHA produces an output of 160-bit (message digest).

VI. METHODOLOGY

When the data owner (sender) wants to store the original documents in the cloud for sharing with the data users (recipients), the data owner first create a digital signature for the document. For creating a digital signature, he/she computes a hash value for the original document using Secure Hash Algorithm (SHA). This hash value which is obtained is a condensed version of the data, which is called message digest. This message digest is then encrypted using the sender's private key. Thus, digital signature for the document is generated. Then the original document is encrypted using the same private key of the sender using AES encryption scheme. The data owner (sender) sends the encrypted document along with the digital signature to the cloud for storage. The data user (recipient) requests to the cloud for the corresponding document send by the sender. Then the data user receives the encrypted document along with the digital signature. The recipient separates the encrypted document from the digital signature. Then the recipient decrypts the encrypted document using the sender's private key and obtains the original document. The AES encryption scheme is used for the encryption and decryption of document. After digital signature generation, then is the process of digital signature verification. For that the digital signature is then decrypted using the public key. After decryption, the recipient obtains the hash value generated using SHA algorithm. Then the recipient takes the decrypted original document and computes a new hash value for it using the same SHA algorithm. The recipient verifies the hash values. If both the hash values matches, then it means that the document belongs to the claimed /original sender. On the other hand, if both the hash values do not match, then it means the original document may have been tampered. Thus digital signatures can be used for providing authentication and non-repudiation.

VII. DESIGN FRAMEWORK



©IJRASET 2015: All Rights are Reserved

Fig. 2. Working of the System at sender side

Recipient

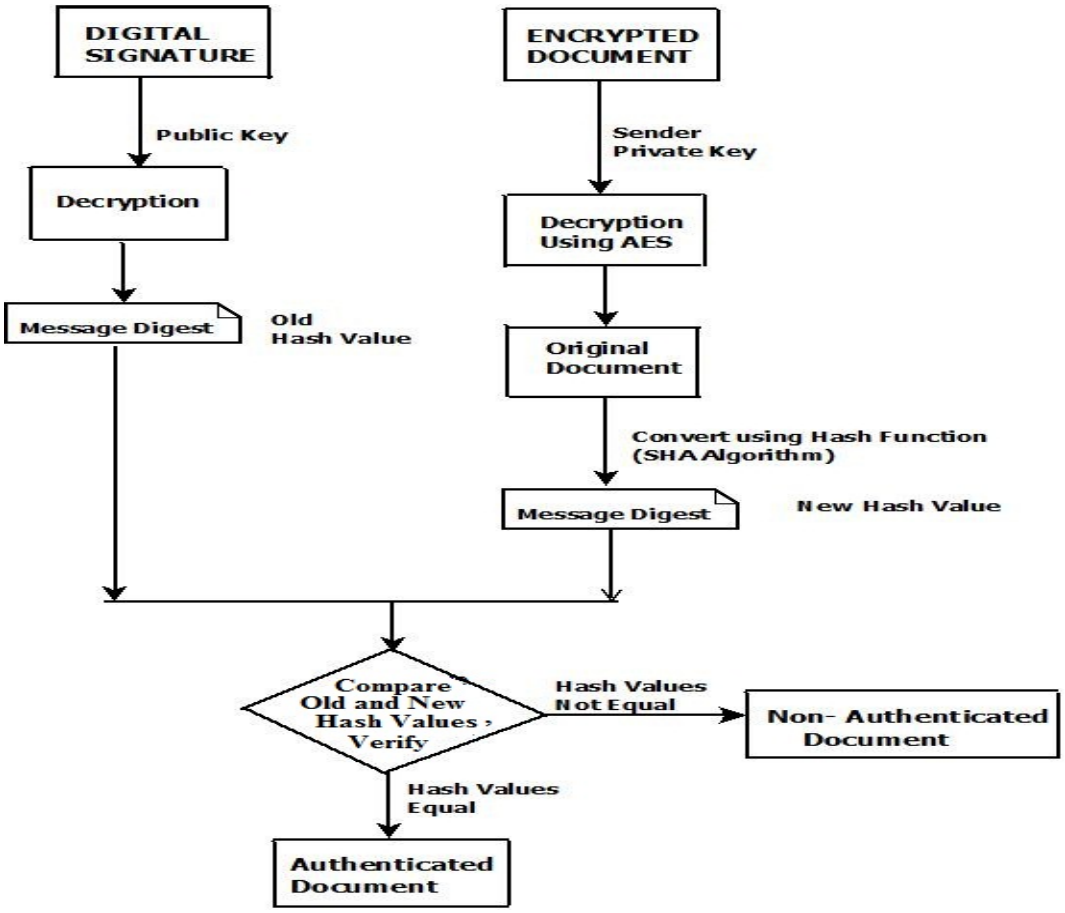


Fig. 3. Working of the system at Recipient side

VIII. CONCLUSION

Cloud computing is an apt technology which allow users to store their data in cloud storage and use them when required.
The cloud rest on the internet so various security and privacy issues can arise. Cloud computing mainly deals with the problem of data security and data authentication. Advanced Encryption Standard (AES) is being used for encrypting the data for ensuring data security. The mechanism which is being used for ensuring authentication is digital signatures. Digital Signature algorithm deals with digital signature creation and verification process. For both digital signature generation and signature verification process, same hash function is used.

REFERENCES

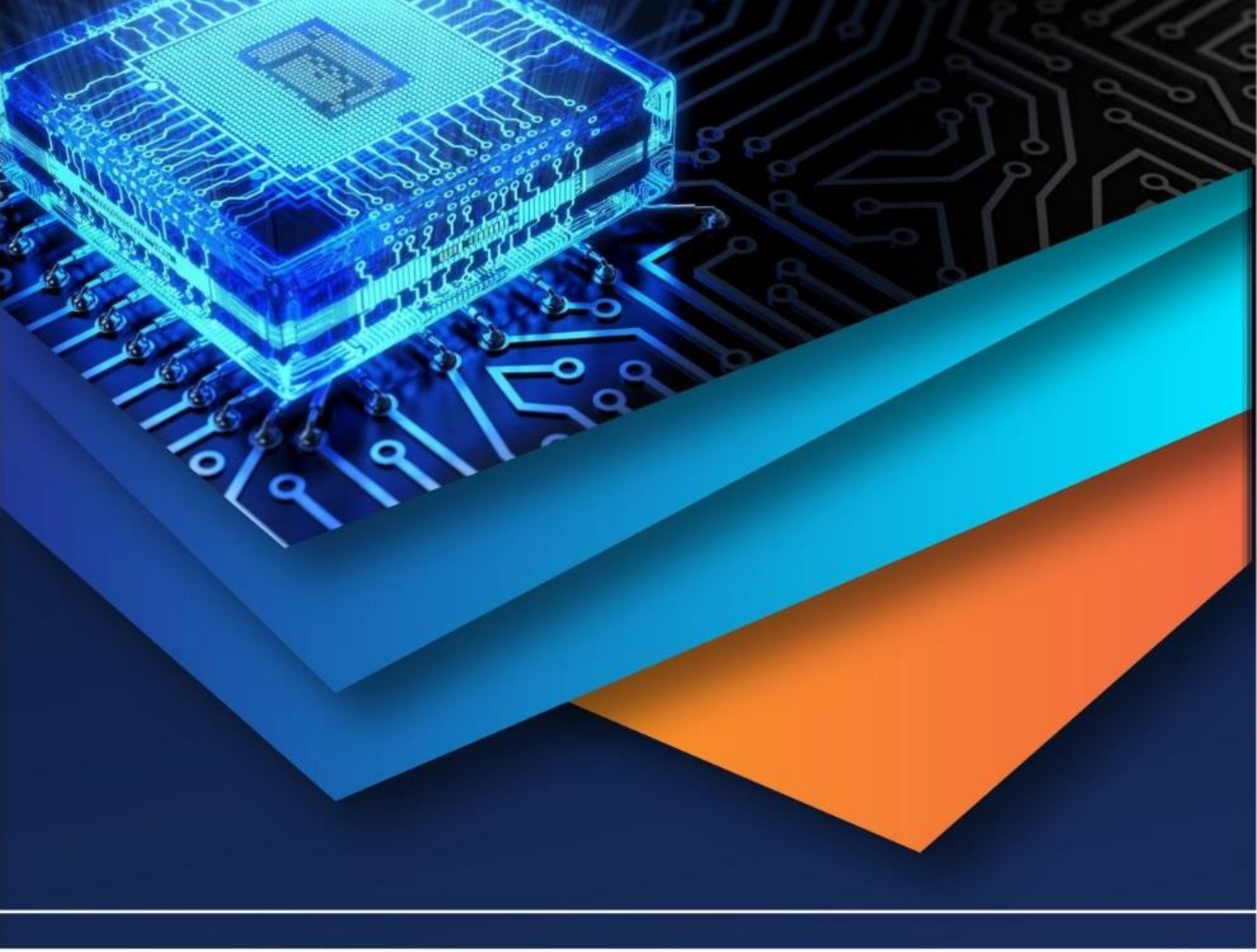
[1] Balachandra Reddy Kandukuri, Rama Krishna Paturi and Dr. AtanuRakshit, “Cloud security issues” In ServicesComputing, 2009. IEEE International Conference on, page 517520, 2009.
[2] S. Kamara and K. Lauter,“Cryptographic cloud storage,” in *RLCPS, January 2010, LNCS.Springer, Heidelberg.*
[3] Kresimir Popovic and Zeljko Hocenski “Cloud computing security issues and challenges”,MIPRO 2010, May 24-28, 2010, Opatija, Croatia.
[4] T. Sivasakthi1 and Dr. N Prabakaran “Applying Digital Signature with Encryption Algorithm of User Authentication for Data Security in Cloud Computing”, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 2, February 2014.
[5] Devan Chen and Hong Zhao “Data security and Privacy Protection Issues in Cloud Computing ” IEEE 2012
[6] S. Pearson, “Taking Account of Privacy when Designing Cloud Computing Services”, CLOUD_09,May 23, 2009, Vancouver, Canad.
[7] Dhaval Patel and ,M.B.Chaudhari, “Data Security In Cloud Computing Using Digital signature”International Journal For Technological Research In Engineering Volume 1, Issue 10, June-2014

©IJRASET 2015: All Rights are Reserved

[8] Shobha Rajak, Ashok Verma "Secure Data Storage in the Cloud using Digital Signature Mechanism" IJARCET June 2012 .
[9] Cong Wang, Qian Wang and Kui Ren. ―Ensuring Data Storage Security in Cloud computing‖ 978-1-4244-3876- 1/2009 IEEE.
[10]. Dr. Chander Kant and Yogesh Sharma, "Enhanced Security Architecture for Cloud Data Security" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013, pp. 571-575.

.

©IJRASET 2015: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)