

Improve Security of Cloud Storage using Digital Signature

Vishal R. Pancholi
Research Scholar
Pacific University Udaipur,
Rajasthan

Dr. Bhadresh P. Patel
I/C Principal
Matrushri L.J Gandhi (Bakorvala) BCA College
Modasa, Gujarat

Abstract

Cloud computing is the pertinent technology for the decade. The cloud computing is Internet based computer, shared software information and resource to world. These cloud environment resources are shared to all servers, and separate users. The cloud computing chains distributed services multi-domain Infrastructure, and multi-users. It certifies user to store large amount of data in cloud storage and use as and when essential, from wherever in the world, via any terminal equipment. Since cloud computing is rest on internet, security issues like privacy, data security, confidentiality, and authentication is faced. In order to get free from the alike, a variation of encryption algorithms and mechanisms are used. On the similar terms, this paper is carrying out the implementation of Digital Signature.

Keywords: Digital Signature, Security, Cloud Computing, Cryptography, Authentication

I. INTRODUCTION

The cloud computing is Internet based computer, shared software information and resource to world. These cloud environment resources are shared to all servers, and separate users. The cloud computing supports distributed services multi-domain Infrastructure, and multi-users [1]. Digital signatures are used to device electronic signatures, a broader word that refers to any electronic data that conveys the intent of a signature.

Properly implemented, a digital signature provides the receiver reason to trust the message was sent by the claimed sender. Digital seals and signatures are alike to handwritten signatures and stamped seals. Digital signatures are corresponding to traditional handwritten signatures in many respects, but correctly implemented digital signatures are more challenging to copy than the handwritten form.

Digital signature patterns, in the sense used at this time, are cryptographically based, and must be implemented properly to be operative. Digital signatures can also provide non-repudiation, meaning that the signer cannot successfully privilege they did not sign a message, while also claiming their private key rests secret; further, some non-repudiation systems offer a time stamp for the digital signature, so that even if the private key is exposed, the signature is legal. Digitally signed messages may be anything representable as a bitstring: examples include electronic mail, contracts, or a message sent via certain cryptographic protocol.

The digital signature creation and verification process achieves the subsequent legal requirements:

A. Signer Authentication

A person's digital signature cannot be forged except his private key is stolen. This means that if a digital signature can be confirmed by A's public key, then it must have been created by A's private key. The digital signature verification process thus validates the identity of the signer.

B. Message Authentication

A digital signature is constructed upon the hash value (or message digest) of the actual message. Thus a digital signature is unique for each message and automatically authenticates the message.

C. Affirmative Act

The process of digital signature creation involves the signer to use his private key (usually by entering a password). This obvious act alerts the signer that he is initiating a transaction that may have legal consequences.

II. LITERATURE REVIEW

According to [1], a new user security for cloud computing platform includes RSA and encryption algorithm is implemented. The user login execution period is not a part of higher, (i.e.) implementation of each algorithm is perform different servers, and download, upload a files to take overall system is stop difficult.

In [2], it is to propose a kind of digital signature based on public key. By this way, both digital signature and defending illegal interpolation and replication of digital products are effectively realized.

In [3], it is presented that, the digital signature has become a significant tool in international commerce. Additional businesses will likely use digital signatures in an increasing percentage of their commercial transactions As a digital signature provides the legal elements of a traditional handwritten signature and enhanced security, integrity, and authenticity, additional businesses will likely use digital signatures in an increasing percentage of their commercial transactions.

According to [5], it attempted reviews of all researches occurred on Digital Signature in past 1 or 1.5 decades and also recognizes the advantages and disadvantages of Digital Signature based on Public key cryptography. A digital signature is a technique of cryptography which authenticates the particular info and also provides integrity to the information that to be transmitted over a network. This paper revise about all those techniques which are developed or derived from the Digital Signature technique and are based on public key cryptography. And also shows the evolution of digital signature in last 15 years.

III. HOW DIGITAL SIGNATURE CERTIFICATE WORKS?

A Digital Signature Certificate explicitly associates the identity of an individual/device with a pair of electronic keys - public and private keys - and this association is endorsed by the Certifying Authorities.

The certificate contains information about a user's identity (for example, their name, pin code, country, email address, the date the certificate was issued and the name of the Certifying Authority that issued it).

These keys complement each other in that one does not function in the absence of the other. They are used by browsers and servers to encrypt and decrypt information regarding the identity of the certificate user during information exchange processes.

The private key is stored on the user's computer hard disk or on an external device such as a token. The user retains control of the private key; it can only be used with the issued password. The public key is disseminated with the encrypted information.

The authentication process fails if either one of these keys in not available or do not match. This means that the encrypted data cannot be decrypted and therefore, is inaccessible to unauthorized parties. [7]

IV. DIGITAL SIGNATURE TECHNOLOGY

Digital Signature is a method to encrypt a message (such as documents, contracts, notifications) which will be transferred, adopting data-exchanging protocol and data-encrypting algorithm [2].

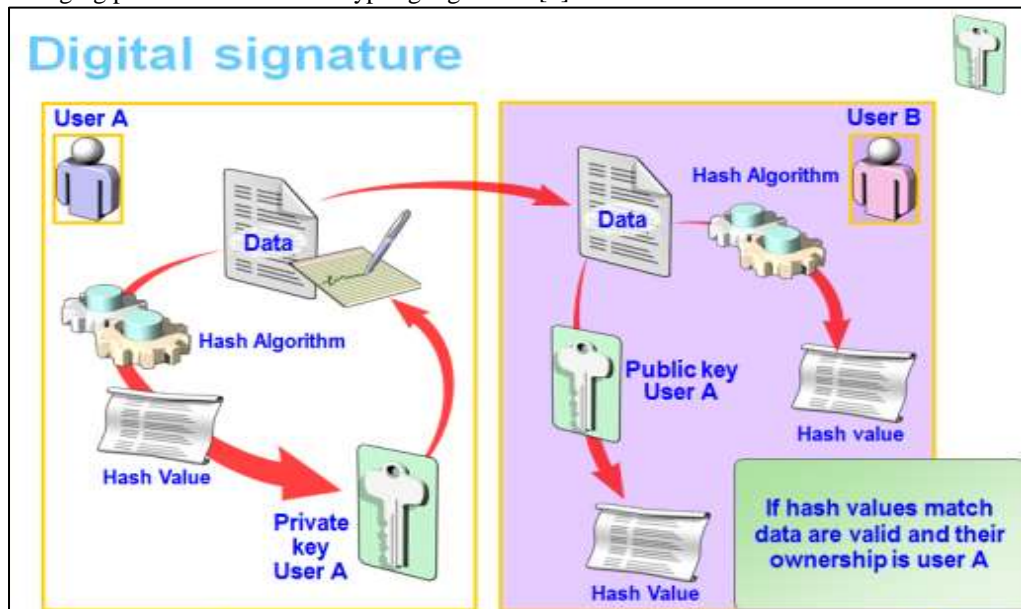


Fig. 1: Working of digital signature

Formally, a digital signature scheme is a triple of probabilistic polynomial time algorithms, (G, S, V), satisfying:

- G (key-generator) generates a public key, pk, and a corresponding private key, sk, on input 1n, where n is the security parameter.
- S (signing) returns a tag, t, on the inputs: the private key, sk, and a string, x.
- V (verifying) outputs accepted or rejected on the inputs: the public key, pk, a string, x, and a tag, t.

For correctness, S and V must satisfy

$$\Pr[(pk, sk) \leftarrow G(1n), V(pk, x, S(sk, x)) = \text{accepted}] = 1$$

A digital signature scheme is secure if for every non-uniform probabilistic polynomial time adversary, A

$$\Pr[(pk, sk) \leftarrow G(1n), (x, t) \leftarrow AS(sk, \cdot)(pk, 1n), x \notin Q, V(pk, x, t) = \text{accepted}] < \text{negl}(n),$$

Where $AS(sk, \cdot)$ denotes that A has access to the oracle, $S(sk, \cdot)$, and Q denotes the set of the queries on S made by A, which knows the public key, pk, and the security parameter, n. Note that we require any adversary cannot directly query the string, x, on S.

In cryptography, a random oracle is an oracle (a theoretical black box) that responds to every unique query with a (truly) random response chosen uniformly from its output domain.

D. Properties

Properties of Digital Signature can be described as follows for which it has been chosen in Internet Security:-

- The signature must be an authentic one that means the recipient should recognize that the signer signed the document.
- The signature to be used for a specific transaction and it cannot be used in another document.
- It must not be irreversible, i.e. the electronic document should not be changed once it is signed by somebody.
- Signature should be non-repudiated, which means after the signer signs a document then the signer cannot claim that he has not signed.

E. Applications of Digital Signature

- Digital signatures are being increasingly used in secure e-mail and credit card transactions over the Internet.
- Digital signature certificates can be employed in wireless networks.
- Digital signature certificates in e-tendering systems are allowed.

V. CONCLUSION

The significance of high assurance is required for any kind of transmission of data in cloud computing. There are so many techniques available to protect the data over the cloud. This paper offered an algorithm of generating digital signature. The security of the system is comparatively enhanced using this approach. The result will be more effectual when someone applies Digital Signature to protect the data.

REFERENCES

- [1] T. Sivasakthi 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
- [2] Hongjie Zhu, Daxing Li "Research on Digital Signature in Electronic Commerce", Proceedings of the International Multi Conference of Engineers and Computer Scientists 2008 Vol I IMECS 2008, 19-21 March, 2008, Hong Kong
- [3] Payel Saha "A comprehensive study on digital signature for internet security" ACCENTS Transactions on Information Security, Vol 1(1) ISSN (Online): 2455-7196
- [4] Mr. Hemant Kumar, Dr. Ajit Singh "An Efficient Implementation of Digital Signature Algorithm with SRNN Public Key Cryptography" , IJRREST: International Journal of Research Review in Engineering Science and Technology (ISSN 2278- 6643) | Volume-1 Issue-1, June 2012
- [5] Shivendra Singh, Md. Sarfaraz Iqbal, Arunima Jaiswal "Survey on Techniques Developed using Digital Signature: Public key Cryptography", International Journal of Computer Applications (0975 – 8887) Volume 117 – No. 16, May 2015
- [6] Prakash Kuppuswamy, Peer Mohammad Appa, Dr. Saeed Q Y Al-Khalidi, "A New Efficient Digital Signature Scheme Algorithm based on Block cipher", IOSR Journal of Computer Engineering (IOSRJCE)
- [7] <http://www.e-mudhra.com/faq.html>
- [8] Mr. Navanath P. Jashav, Mrs. L. Laxmi "Public Auditing: Security in Cloud Storage" IJIRST–International Journal for Innovative Research in Science & Technology| Vol. 1, Issue 2, July 2014