International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 6 | ISSN : 2456-3307

Digital Signature

Pooja[1], Mrs. Mamta Yadav[2]
[1]M.Tech Scholar CSE, M.D.U Rohtak,YCET Narnaul, Mahendergarh, Haryana, India
[2]Assistant Professor, CSE, M.D.U Rohtak,YCET Narnaul, Mahendergarh, Haryana, India

ABSTRACT

The Information Technology Act 2000 (IT Act) dictates digital signatures as a means of authentication and security of electronic documents. Digital signature is an electronic token that creates binding between an entity and a data record. They serve the purpose of validation and authentication of electronic documents .Validation refers to the process of certifying the contents of the document, while authentication refers to the process of certifying the sender of the document. It can be said that a digital signature is an electronic version of a handwritten signature. The signing process is implemented with the help of public key cryptography; the signatory uses her private key to create a digital signature for a document. It is used to ensure that the original content of the message or document that has been sent is unchanged. Its varied nature has provided easy, faster, accurate and convenient mechanism for creating, storing, transmission and retrieval of data without involving traditional paper based formalities. This has increased the use of digital technology in day to day life which has led the world to go online that in turn has increased techno-dependency. Increasingly the business dealings, communication, official data and commercial transactions are being carried out in cyberspace. There has been transformation of world from paper based to digital based work. In the last few years, there has been a rapidly growing demand for a working digital signature framework for both public and public sector. The study revolves around the maximum information on digital signature, the future of Information Technology.

I. INTRODUCTION

Authentication, repudiation and verification of electronic data is important for any electronic transactions. Therefore, unless these objectives have not been achieved, the authentication and secure electronic transaction will merely remain virtual. In order to achieve the authentication and security of electronic data the mechanism of digital signature is used. Digital signature can be described as a method of authenticating data i.e. to verify that the received document is indeed from the claimed sender and its content has not been altered in any way since the person has created it. Just as the stamps, seal or signature play role in traditional system to create the authentication of paper document, the digital signature plays the role of authenticating the electronic record. It creates the authenticity of any electronic record which subscriber of digital signature wants to be authenticated the electronic record by affixing his digital signature. The signature is an unforgeable piece of data attesting that a named person wrote or otherwise agreed to the document to which the signature is attached. It performs Signer Authentication, Message authentication and Verification. Digital Signature is created with the help of cryptographic method. The basic objectives of affixing of 'Digital Signature' are – Create authenticity of the originator Digital signature allow the recipient of a message or document to verify the sender. A digital signature is specific for a particular user and thus, a valid digital signature is used to affirm that a message originated from a specific user. So that at any moment after the creation of any digital material, the authenticity of the originator can be verified. It is also essential that at any latter moment, the originator will not capable to deny the creation of document by him. A digitally signed message or document cannot be altered without invalidating the signature. This is true whether the message is encrypted or not. A valid digital signature upon receipt of a message or document confirms that the message or document was not altered in transit. Any recipient will not be in a state to modify, change, alter, or tamper with the document created by originator. The mechanism should also ensure to the originator that no one else than him will be capable to modify, change, alter or tamper with the document Non-repudiation Since a digital signature is the equivalent to a handwritten signature, its use is taken to be a sign of acknowledgement of a message or document. Thus, if someone has digitally signed a document, he or she cannot deny such a document. So, the entire mechanism will ensure that the document and identify mechanism will not play foul and nobody will be in position at any latter moment to deny the responsibility and liability arising out of the document. For originator, that he will not be in position to repudiate what he had created, for recipient, he will not be in position by any means to modify the content created by originator.

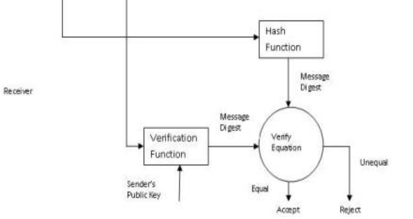
II. DIGITAL SIGNATURE VERIFICATION

Digital signature technology permits the recipient of given signed message to verify its real origin and its integrity. The digital signature verification process is purposed to determine if a given message has been signed by the private key that corresponds to a given public key. The digital signature verification process cannot determine whether the given message has been signed by a given person. If we need to examine whether a person has signed a given message, we are required to obtain his real public key in some manner. This is possible either by getting the public key in a secure way (on a floppy disk or CD) or by means of a digital certificate. Without using a secure way to obtain the real public key of given person, it is impossible to check whether the given message is really signed by this person. Digital verification process

Step 1: Calculate the current hash value- A hash-value of the signed message is calculated. For this, the same hashing algorithm is used as was used during the signing process. The resultant hash-value is called the current hashvalue because it is calculated from the current state of the message.

Step 2: Calculate the original Hash-Value- The digital signature is decrypted with the help of same encryption algorithm that was used during the signing process. The decryption is done by the public key that corresponds to the private key that was used during the signing of the message. As a result, we obtain the original hash-value (the original message digests).

Step 3: Compare the current and the Original HashValues- We compare the current hash-value obtained (from first step) with the original hash-value obtained (from second step), If the two values are same, the verification is successful and proves that the message has been signed with the private key that corresponds to the public key used in the verification process. If the two values are different, this means that the digital signature is invalid and the verification is unsuccessful.



Authentication is a security service that addresses the concept of authentic communication between entities. This security service provides proof of origin authenticationbetween the sender and the responder. This is achieved through the use of credentials like the user name and password or in PKI environment public key certificates are used. Integrity addresses the concept of trustworthiness of IT assets especially the data, message, or a stream of data. In this section we defined types of Digital Signature Schemes and procedures of their implementation. For beginning we must refer that in this paper we only introduced and compared these schemes and only we referenced to implementation algorithms.

III. IMPLEMENTATION

Digital signatures are very important tools toimplement secure and correct signs. Today, traditional physical signature is out-dated. Communications between partners of a company is significant issue that must be secure. Digital signature provides suitable background for sending secure messages using different schemes. Depending on different usages we must choose correct and appropriate option for signing our messages such as proxy-schemes. In this paper, we review and compare some of these implementation methods to optimize signing procedure. As we mentioned above, usually digital signature schemes are categorized in 4 aspects

1. Schemes with Increased Efficiency
2. Schemes with Increased Security
3. Schemes with Anonymity Services
4. Schemes with Enhanced Signing and Verification

In this section we defined types of Digital Signature Schemes and procedures of their implementation. For beginning we must refer that in this paper we only introduced and compared these schemes and only we referenced to implementation algorithms.

It is categorized in Schemes with Increased Security. Its security level is very high because maintains validity of the key, after key is comprised [1]. As we referred its high level security is caused to large of usages. Idea behind Forward Secure Scheme is T (total time of verifying public key). Splits time T into equal periods that any periods have special different Secret Key. Public key is remained constant while next Secret Key is generated according to previous Secret Key and Key Update Algorithm. In special way, generates two random & prime numbers P1 & P2 and uses them to generate and verify steps of signature generation and verification.

Definition 3: Update Algorithm It's a simple algorithm to calculate signatures in periods of time.

1. If j=T then return to generation protocol
2. Regenerates ej+1, ... , eT and starting with constant P
3. Computes SJ+1 That j is the current time; S is the generated Signature his period.

Verification shows how much sings of these schemes are verified correctly and gives us the validity and invalidity of signatures in practice. When a message is signed and is sent to desired location, receiver verify message with his or him public-key. If decryption procedure is done correctly, verification is acceptable. If not, identity of signer is denied. Procedure of verification must certify signer's identity. In some cases, May a valid signature is recognized as invalid and an invalid signature is recognized as valid. This is a bad feature for verification that its result always is not true.

Efficiency parameter defines which scheme is more effective and optimal for its applications. This is an approximation parameter that based on several conditions such as programmer's skill to implement mentioned algorithms, security of network and system designs, percentages of verification signatures, relations between choosing appropriate scheme and its applications and so on. As referred above, efficiency is calculated approximately and it’s not enough for judgement among these schemes. This only provides an overview to select appropriate schemes according to our applications

DIGITAL SIGNATURE USES:

- ✓ With the use of digital signature we can eliminate the possibility of committing fraud because the digital signature cannot be altered. Moreover the forging signature is impossible.
- ✓ By having a digital signature we are proving the document to be valid. We are assuring the recipient that the document is free from forgery or false information.
- ✓ No fever of data loss.
- ✓ Just need a little knowledge to operate the system.
- ✓ Doesn’t require any extra hardware device.
- ✓ Addition, Clipping, Construction and updating of the attendance record and face.
- ✓ Comparing the image with the faces that are there in our database.
- ✓ If the digital signature is changed and decrypted with the public key, then the obtained original value will not be the original hash-value of the original message instead some other value.
- ✓ If the message was changed after its signing, the current hash-value obtained from this changed message will be different from the original hash-value because the two different messages correspond to different hash-values.
- ✓ If the public key does not match up to the private key used for signing, the original hash-value obtained by decrypting the signature with an incorrect key will not be incorrect.
- ✓ Using a digital signature satisfies some type of legal requirement for the document in question. A digital signature takes care of any formal legal aspect of executing the document.
- ✓ Includes an automatic date and time stamp, which is critical in business transactions.
- ✓ Increases the speed and accuracy of transactions.
- ✓ Digital signatures are a computerized form of signatur that verifies that a package was sent by a certain individual or business, or that the right person actually signed a document. These signatures are secure and legal, and they can greatly improve your security

IV. REFERENCES

[1]. F.E.S.,Dunbar, 2002. Digital Signature SchemeVariation, presented in University of Waterloo.

[2]. A., Menezes, P., Van., Oorschot, and S. Vanstone,CRC Press, 1996. Handbook of Applied Cryptography.

[3]. Z.,Liu, Y.,Hu, X.,Zhang, H.,Ma, 2010. Provably securemulti-proxy signature scheme with revocation in the standardmodel. Elsevier journal of computer Communications.

[4]. J.,Zhang, C.,Liu, Y.,Yang, 2009. An efficient secureproxy verifiably encrypted signature scheme. Elsevier Journalof Networks and Computer Applications.

[5]. F.,Li & M.,Khurram Khan, 2010. A biometric identitybasedsigncryption scheme. Elsevier Future Generation Computer Systems.

[6]. L.,Buttyán, L.,Dóra, F.,Martinelli, M.,Petrocchi,2010. Fast certificate-based authentication scheme in multioperatormaintained wireless mesh networks. ElsevierComputer CommunicationsTransform", in Proc. 7th IEEE International Symposium on Signal Processing and InformationTechnology (ISSPIT'07), December 2007, Egypt.

[7]. R.A. Santosa and P. Bao, "Audio-to-image wavelet transform based audio steganography," Proc. of47th Int. Symposium ELMAR, June 2005, pp. 209- 212.

[8]. Xuping Huang, Ryota Kawashima, Norihisa Segawa, Yoshihiko Abe. "The Real-Time Steganography Based on Audio-to-Audio Data Bit Stream",Technical report of IEICE, ISEC, vol.106 pp.15-22, September 2006.

[9]. Aoki, Naofumi. "A Band Widening Technique for VoIP Speech Using Steganography Technology", Report of IEICE, SP,106(333), pp.31-36, 2006.

[10]. Xuping Huang, Ryota Kawashima, Norihisa Segawa, Yoshihiko Abe International Conference on Intelligent "Information Hiding and Multimedia Signal Processing" © 2008 IEEE.

[11]. A. Delforouz, Mohammad Pooyan, "Adaptive Digital Audio Steganography Based on Integer wavelet transform ", IEEE Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2007, 26-28 Nov 2007, pp 283-286.

[12]. R. A. Santosa, P. Bao," Audio-to-Image Wavelet Transform based Audio Steganography", 47th International Symposium ELMAR-2005 , 08-10 June 2005, Zadar, Croatia, pp 209-212.

[13]. S. Shirali-Shahreza, M. T. Manzuri-Shalmani, "Adaptive Wavelet Domain Audio Steganography with High Capacity and Low Error Rate", IEEE International Conference on Information and Emerging Technologies, 2007, 06-07 July 2007 pp 1-5.

[14]. Yincheng Qi, Jianwen Fu, and Jinsha Yuan, "Wavelet domain audio steganalysis based on statistical moments of histogram", Journal of System Simulation, Vol 20, No. 7, pp. 1912-1914, April 2008.

[15]. Yin-cheng qi, liang ye, chong liu "Wavelet domain audio steganalysis for multiplicative embedding model" Proceedings of the 2009 International Conference on Wavelet Analysis and Pattern Recognition, Baoding, 12-15 July 2009.

[16]. V. Vapnik, "Statistical Learning Theory", John Wiley, 2008.