ISSN2394-3777 (Print)
ISSN2394-3785 (Online)
Available online atwww.ijartet.com

ternational Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
ol. 5, Special Issue 10, March 2018

Revolution Of Digital Signatures

Lovejit Kaur
Assistant professor,Dept. of Commerce,
Swami Ganga GiriJanta girls college,Raikot (PB), 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 many traditional businesses and applications have been carrying out enormous amounts of electronic transactions , which have led to critical need of protecting the information from being maliciously altered , for ensuring the authenticity , and for supporting non repudiation . just as signatures facilitate validation and verification of the authenticity of paper documents. digital signature serve the purpose of validation and authentication of electronic documents. this technology is rather new and emerging and is expected to experience growth and widespread use in coming years. 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.

KEYWORDS: Non Repudiation, Encryption, Authentication, Hash Function, Key-Pair, Information Technology, Recognition.

I. INTRODUCTION

The authenticity of many legal, financial and other documents is determined by the presence or absence of an authorized handwritten signature. Various methods have been devised to solve this problem, but the use of digital signature is definitely the best solution amongst them. a digital signature is nothing but an attachment to any piece of electronic information ,which represents the content of the document and the identity of the originator of that document uniquely. Authentication, repudiation and verification of electronic data is important for any electronic transactions. 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.

II. OBJECTIVES OF THE STUDY:

1) to know exactly what is digital signature .
2) basic requirements and how it works.
3) Model of digital signature
4) Advantages
5) Disadvantages

III .LITERATURE REVIEW:

1. Pointchevala et al [2000] [1] provides some security arguments for digital signature as well as for blind signature. Here anyone can justify realistic parameters even if they are not optimal.
2. Gerić et al (2012) [2] provides information about

   XML sigantures. XML signatures are type of digital signatures generally helps in XML Transactions. It also defines a particular schema for the storage of XML data's result based on digital signature operations.
3. Nguyen et al (2011) [3] presented a paper on functionality Extension of the Digital Signature

   Standards. The protocol used here is based on Belarusian DS standards which are flexible and provide a possibility of natural extension of their functionality.
4. Zhang et al (2011) [4] makes an improvement on digital signature algorithm which is based on elliptic curve cryptography. In this paper he obtained a new digital signature scheme by improving the original digital signature based on elliptic curve cryptosystem.
5. Xuan et al (2009) [5] makes a research on the comparison of algorithms used by Digital signature in Mobile Web world. DSA, RSA and ECDSA are some algorithms which are generally used in comparison in this paper
6. Can et al (2009) [7] proposed a new conic curve digital signature scheme which uses two private keys and upgrade the difficulty of those key be stolen to make security of signature scheme higher and stronger.
8. value.
9. Campbell (2003) [11] provides a review on supporting digital signatures in mobile environments. According to the reviews Digital

   Signature Systems uses the end user's private key to generate a digital signature which has the characteristics of integrity and non-repudiation.
10. W. Romney et al (2006) [12] proposed a digital signature signing engine to protect the integrity of digital assets. Which helps in confronting technologically challenging issues in digital assets.

III .RESEARCH METHODOLOGY

the study is based on secondary sources of data / information Different books, journals, newspapers and relevant websites have been consulted in order to make the study an effective

1. WHAT IS DIGITAL SIGNATURE?

A digital signature is a mathematical scheme for demonstrating the authenticity of digital messages or documents. valid digital signature gives a recipient reason to believe that the message was created by a known sender(authentication) that the sender cannot deny having sent the message (non repudiation)and that the message was not altered in transit .(integrity)

2. BRIEF HISTORY OF DIGITAL SIGNATURE

For centuries, signatures have been the most conventional means of authentication. Roman law documented a combination of seals and signatures as the primary source for authenticating documents and legal contracts. The 1830s saw the first signs of electronic communications and legally recognized "electronic" signatures with the invention of the telegraph and Morse code. But it was the introduction of public key cryptography by Martin Hellman and Whitfield

Diffie in 1976 that established the first practical method of distributing cryptographic keys over an unprotected public network.

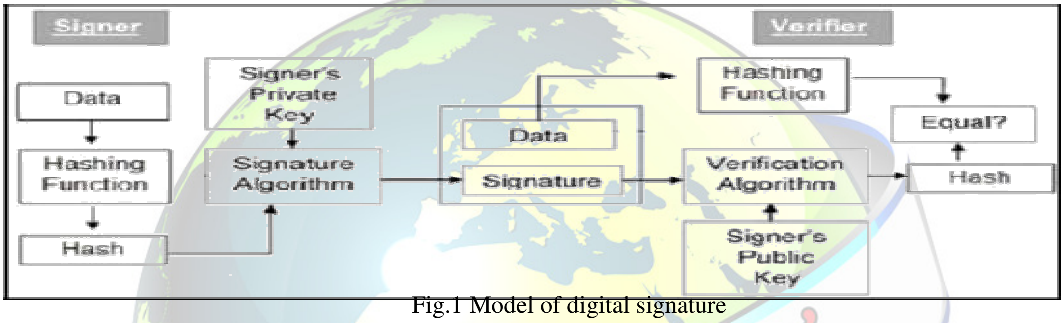


Fig.1 Model of digital signature

The following point explain the entire process in detail

2.1 Each person adopting this scheme has a public-private key pair

2.2 Generally, the key pairs used for encryption/decryption and signing/verifying are different. the private key used for signing is referred to as the signature key and the public key as the verification key.

2.3 Signer feeds data to the hash function and generates hash of data

2.4 Hash value and signature key are then feed to the signature algorithm produces the digital signature on given hash. signature appended to the data and then both are sent to the verifier

2.5 Verifier feed the digital signature and the verification key into the verification algorithm. The verification algorithm gives some value as a output

2.6 Verifier also runs same hash function on received data to generate hash value.

2.7 For verification this hash value and output of verification algorithm are compared based on the comparison result, verifier decide whether the digital signature is valid.

2.8 Since digital signature is created by private key of signer and on one as can have this key, the signer cannot repudiate signing the data in future

3. FORMS OF DIGITAL SIGNATURE.

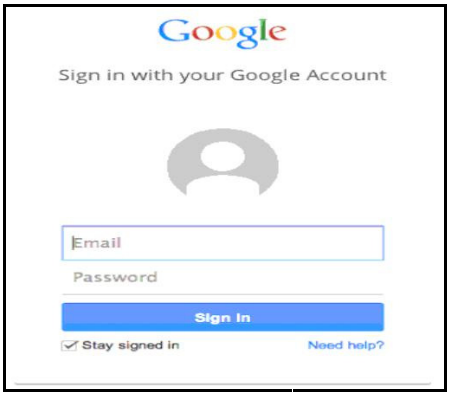
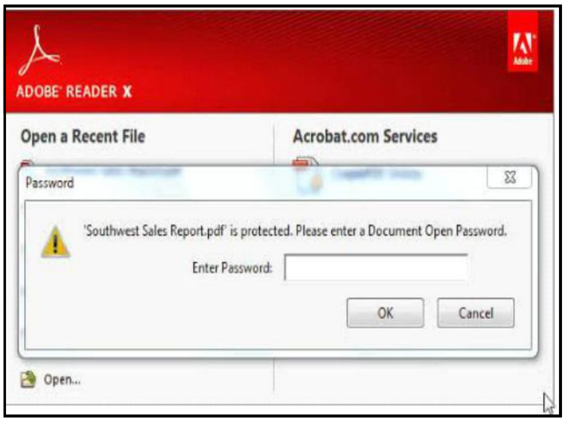


figure 2. signing in for google id



'Southwest Sales Report.pdf' is protected. Please enter a Document Open Password.

Fig. 3 file encryption in case of bank statements or reports

4. APPLICATIONS OF DIGITAL SIGNATURE

1. Electronic mall
2. Data storage
3. Electronic fund transfer

4. Software distribution

5. DVANTAGES

Following are the advantages of symmetric key cryptography

- Speed: By using DS business have not to wait for paper documents to be sent by any postal services. Contracts are written, completed, and signed by all concerned parties in a short period of time.
- Costs: Transmission over a network is cheaper than postal services. And if it is done by Digital Signature, it is much cheaper than others.
- Security: By using digital signatures and electronic documents alter the risks of documents being decoded, read, removed, or altered while in transmission.
- Non-Repudiation: Passing an electronic document digitally identifies you as the signatory and that cannot be later denied.
- Imposter prevention: Not a single person else can oven your digital signature or submit an electronic document incorrectly appealing it was sign up by you.
- Time-Stamp: With the help of time stamping your digital signatures you will get the correct time when the documents is signed.
- Authenticity: Both paper stamp and digital stamp have same value of authenticity

6. DISADVANTAGES

Following are the disadvantages of digital signature:-

- Expiry: Digital signatures are also like just other electronic media and we all know that each of them have a limited time. Therefore, it shows that DS is also come with its expiry.

□ Certificates: Both sender and receiver must have to buy authorized certificates for the effective use of digital signature.

- Software: Sender and receiver both have to buy authorized software too, to make transmission smoother and easier.
- Law: In some states and countries, commandments regarding computer-generated and technology-based issues are weak or even non-existent. Exchange in such jurisdictions becomes very risky for those who use digitally signed electronic documents.
- Compatibility: Issues are also found many compatibility during the use of digital signature in different-different platform.
- *The* generation process and verification process of digital signature needs substantial quantity of time. So, for regular exchange of communications the speed of communication will decrease.
- If a user changes his private key after every fixed break of period, then the record of all these changes must be reserved. If an argument arises over a previously sent message then the old key pair needs to be referred. Thus loading of all the preceding keys is another overhead.
- Necessity-Digital signatures are a great security feature, but that does not mean they are a necessary one. If you own a law firm that deals in confidential materials, you might want to invest in a digital signature application for your clients. However, if you own a small family business that deals primarily in cash, you probably do not need it.
- Technological Compatibility **-** refers to standards and the ability of one digital signature system to "talk" to another. It is difficult to develop standards across a wideuser base.
- Security Concerns - These efforts are perpetually hampered by lost or borrowed

sswords, theft and tampering, and vulnerable storage and backup facilities.

- Legal Issues **-** There is clear consensus that digital signature should be legally acceptable. However, many questions remain unanswered in the legal arena.

IV. CONCLUSION

Many conventional and modern businesses and applications have recently been carrying out enormous amounts of electronic transactions, which have led to a critical need for protecting the information from being maliciously altered, for ensuring the authenticity, and for supporting non repudiation .Just as signatures facilitate validation and verification of the authenticity of paper documents, digital signatures serve the purpose of validation and authentication of electronic documents. It is an essential aspect for creating secure environment for electronic transactions. Digital signature has not only proved an essential techno-legal requirement, but it has made the e-commerce meaningful.

REFERENCES

1.http://www.developer.com/java/ent/article.php/3092771/How-Digital-Signatures-Work-Digitally-Signing-Messages.htm
Ecommerce - Legal Issuesauthored by RohasNagpal.
e-book:http://www.ebooktoyou.net/ebook/digital-signaturedownload-pdf.php
2.StallingsW., *Cryptography and Network Security*, 3rd ed. EnglewoodCliffs, NJ: Prentice-Hall, 2002.
3.FeghhiJ. and P. Williams, *Digital Certificates: Applied Internet Security* 1sted. Reading, MA: Addison-Wesley(1999).
4. Denning, D.E. Cryptography and Data Security. Reading, MA: Addison-Wesley(1982).
5 .Stallings, W. Cryptography and Network Security: Principles and Practice, 4th ed. Englewood Cliffs, NJ: Prentice Hall(2006).
6.Practical Security Aspects of Digital Signature Systems: Florian Nentwich, EnginKirda, and Christopher Kruegel

Secure Systems Lab, Technical University Vienna(JUNE-2006).

Author Name: Lovejit Kaur

Designation: Assistant Professor

Department: Commerce

Educational Qualification: B.com (honours) ,M.COM,UGC NET Qualified

Research publications: 1 in international journal