Survey on Techniques Developed using Digital Signature: Public key Cryptography

Shivendra Singh
Student
Department of CSE
Amity University, Noida, India

Md. Sarfaraz Iqbal
Student
Department of CSE
Amity University, Noida, India

Arunima Jaiswal
Asst. Professor
Department of CSE
Amity University, Noida, India

ABSTRACT

The digital signature technique is essential for secure transactions over open networks. It is used in a variety of applications to ensure the integrity of data exchanged or stored and to prove to the recipient the originator's identity. Digital signature schemes are mostly used in cryptographic protocols to provide services like entity authentication, authenticated key transport and authenticated key agreement. This architecture is related with secure Hash Function and cryptographic algorithm In this paper we are going to make review about all those technique that are developed within last 5-10 years. And which are developed with the help of digital signature and based on public key cryptography. These techniques provides a better platform for security of data using cryptography.

General Terms

Safety, Key, Hiding, Symmetric, Signature, Stream, Block, Security, Algorithms.

Keywords

Digital Signature, Public key Cryptography, Block cipher, MD5, Security arguments, XML signatures, DSA, HEC, GPS, Geo-encryption.

1. INTRODUCTION

Now a days a lot of information go through the internet using different means. Some of the information are highly confidential and we cannot compromise with its security. So we use lot of different techniques and algorithms to make our data as secure as much as possible. And these techniques and algorithms are collectively called as Cryptography. There are lots of techniques comes under it. One of the important technique is Digital Signature which helps in assuring that the info provider and information provided both are genuine. This provide a better security level to the transfer of information over a network. Using this important technique of cryptography lots of other derived techniques are developed based on public key cryptography.

2. DIGITAL SIGNATURE

2.1 Overview

A digital signature is a mathematical technique that is generally used know whether a document or information is authenticated or not. In this technique a digital signature is generated as a valid reason for recipient to believe that this document or information is send only by the authorized sender. And it also assure that the message is not altered during the transfer over the network.

This technique generally deals in software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

2.2 Application

There Are Some Common Reasons For Applying A Digital Signature To Communications:

Authentication:-
Digital signature is used to identify the ownership information and content authentication using different cryptography algorithms

Integrity:-
Since only one digital signature can be created for each unique message for any sender therefore it can be effectively used to verify authenticity of sender and therefore the integrity of message**.**

Non-repudiation:-
Since the same signature is generated on the both side of transmission to authenticate the data, it is clear that the sender cannot deny that the information is send by him/her.

3. LITERATURE SURVEY

The last 1 or 1.5 decades have seen a lot of researches in field of digital signature in which lots of derived techniques are originated and applied in the security field.

Studies carried out in Literature Survey:-
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.

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.

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.

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.

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.

Jian-zhi et al (2009) [6] gives a design of Hyper Elliptic Curve Digital Signature in which they described DSA and HEC algorithms to combine them and to generate DSA-HEC digital signature system. Which provide a high security to check the uniqueness of data.

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.

Hai-peng et al (2009) [8] proposed an algorithm based on Hash Round Function and self-certified Public Key System worked on Digital signature. In this they contrived H-S DSA and analyze it according to time and security level.

Jarusombat et al (2006) [9] provides a digital signature techniques on mobile devices based on location. This techniques is works on those device that have low computational capability and low battery time period by using GPS technology and also by applying geo-encryption and mobility model in process of digital signature generation.

Harn (1994) [10] proposed three threshold digital signature schemes which is totally based on difficulty to solve the discrete log problems. In this the signature's group can be produced when the number of participating member is greater than or same as threshold value.

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.

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.

3.1 Summary of literature review

Table 1. Author wise addressed issues in their papers

Author Name	**Issue addressed**
Gordon W. Romney et al[12]	Digital signature signing engine to protect the integrity of digital assets.
L. Harn[10]	Group-oriented (t, n) threshold digital signature scheme and digital multi signature.
Xiang Can et al [7]	A New Conic Curve Digital Signature Scheme
Zuguang Xuan et al [5]	Comparison Research on Digital Signature Algorithms in Mobile Web Services.
Sandro Gerić et al [2]	XML Digital Signature and its Role in Information System Security.
Minh H. Nguyen et al [3]	On Functionality Extension of the Digital Signature Standards.
Qiuxia Zhang et al[4]	The Improvement of digital signature algorithm Based on elliptic curve cryptography.
Deng Jian-zhi, et al [6]	Design of Hyper Elliptic Curve Digital Signature.
Xiang Can et al [7]	A New Conic Curve Digital Signature Scheme.
Chen Hai-peng et al [8]	Digital Signature Algorithm Based on Hash Round Function and Self-certified Public Key System.
Santi Jarusombat et al [9]	Digital Signature on Mobile Devices based on Location.
Scott Campbell [11]	Supporting Digital Signatures in Mobile Environments.
Prakash Kuppuswamy et al [1]	A New Efficient Digital Signature Scheme Algorithm based on Block cipher.

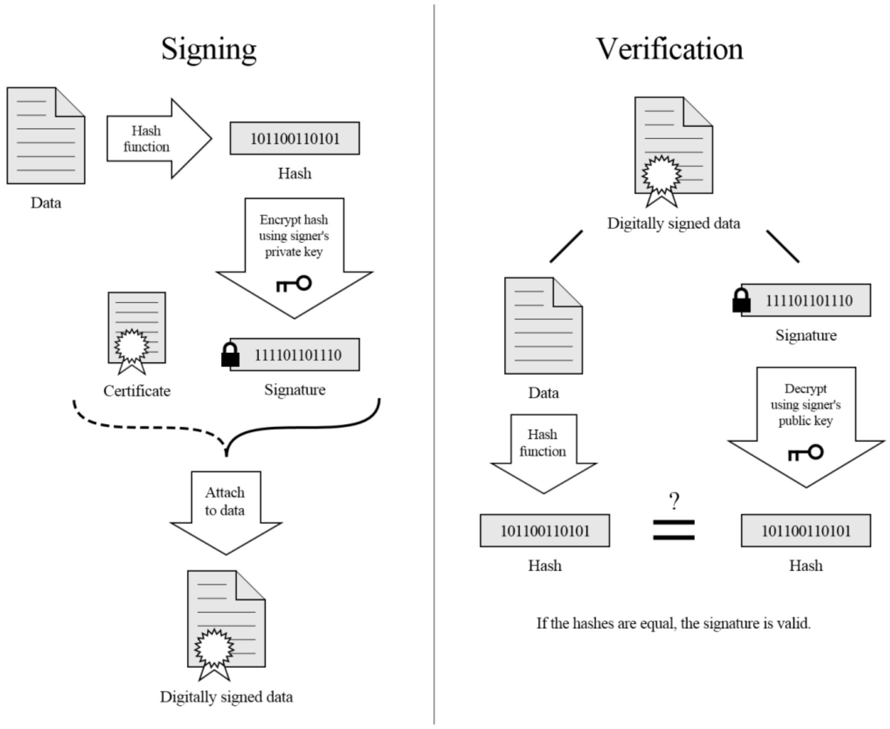

Fig 1: Digital Signature mechanism

4. ADVANTAGES & DISADVANTAGES

Like all the rest the digital signature technique also has its share of advantages and disadvantages.

4.1 Advantages

Following are the advantages of symmetric key cryptography

4.1.1 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.

4.1.2 Costs: Transmission over a network is cheaper than postal services. And if it is done by Digital Signature, it is much cheaper than others.

4.1.3 Security: By using digital signatures and electronic documents alter the risks of documents being decoded, read, removed, or altered while in transmission.

4.1.4 Non-Repudiation: Passing an electronic document digitally identifies you as the signatory and that cannot be later denied.

4.1.5 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.

4.1.6 Time-Stamp: With the help of time-stamping your digital signatures you will get the correct time when the documents is signed.

4.1.7 Authenticity: Both paper stamp and digital stamp have same value of authenticity.

4.2 Disadvantages

Following are the disadvantages of digital signature:-

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

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

4.2.3 Software: Sender and receiver both have to buy authorized software too, to make transmission smoother and easier.

4.2.4 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.

4.2.5 Compatibility: There are many compatibility issues are also found during the use of digital signature in different-different platform.

4.2.6 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.

4.2.7 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.

5. CONCLUSION

This paper attempts to reviews 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 authenticate the particular info and also provide 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.

6. ACKNOWLEDGMENTS

We would like to thank Arunima Jaiswal from Amity School of Engineering and Technology for the useful discussions we had with her at the beginning of the paper and for the constant guidance she has provided us with throughout the completion.

7. REFERENCES

[1] A New Efficient Digital Signature Scheme Algorithm based on Block cipher by Prakash Kuppuswamy, Peer Mohammad Appa,Dr. Saeed Q Y Al-Khalidi, IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661, ISBN: 2278-8727Volume 7, Issue 1 (Nov. - Dec. 2012), PP 47-52

[2] XML Digital Signature and its Role in Information System Security by Sandro Gerić, Tomislav Vidačić, MIPRO 2012, May 21-25,2012, Opatija, Croatia.

[3] On Functionality Extension of the Digital Signature Standards by Minh H. Nguyen, Duy N. HOi, Dung H. Luu, Alexander A. Moldovyan, and Nikolay A. Moldovyan, 2011 International Conference on Advanced Technologies for Communications (ATC 2011).

[4] The Improvement of digital signature algorithm Based on elliptic curve cryptography by Qiuxia Zhang , Zhan Li , Chao Song, 978-1-4577-0536-6/11/$26.00 ©2011 IEEE

[5] Comparison Research on Digital Signature Algorithms in Mobile Web Services by Zuguang Xuan, Zhenjun Du, Rong Chen, partially supported by National Natural Science Foundation of China (No. 60775028), Dalian Science & Technology Program (No. 2007A14GX042) and Dalian Maritime University Youth Foundation (DLMU-ZL-200803), 978-1-4244-4639-1/09/$25.00 ©2009 IEEE

[6] Design of Hyper Elliptic Curve Digital Signature by Deng Jian-zhi, Cheng Xiao-hui, Gui Qiong, 2009 International Conference on Information Technology and Computer Science.

[7] A New Conic Curve Digital Signature Scheme by Xiang Can, You Lin, 2009 Fifth International Conference on Information Assurance and Security.

[8] Digital Signature Algorithm Based on Hash Round Function and Self-certified Public Key System by Chen Hai-peng, Shen Xuan-jing, Wei Wei, 2009 First International Workshop on Education Technology and Computer Science.

[9] Digital Signature on Mobile Devices based on Location by Santi Jarusombat and Surin Kittitornkun, 0-7803-9740-X/06/$20.00 © 2006 IEEE.

[10] Group-oriented (t, n) threshold digital signature scheme and digital multi signature by L. Harn, IEE Proc.-Comput. Digit. Tech., Vol. 141, No. 5, September 1994.

[11] Supporting Digital Signatures in Mobile Environments by Scott Campbell, Twelfth IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE'03) 1080-1383/03 $17.00 © 2003 IEEE.

[12] Digital signature signing engine to protect the integrity of digital assets by Gordon W. Romney, 1-4244-0406-1/06/$20.00 ©2006 IEEE.