International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-9, Issue-3, May 2021
https://doi.org/10.21276/ijircst.2021.9.3.7
Article ID IRP1149, Pages 43-47
www.ijircst.org

A Comprehensive Study on Digital Signature

J. Chandrashekhara[1], Anu V B[2], Prabhavathi H[3], Ramya B R[4]

[1,2,3,4] Lecturers, Department of Studies and Research in Computer Science, Davangere University, Davanagere, India

Correspondence should be addressed to J. Chandrashekhara**;** chandrashekharjk92@gmail.com

Copyright © 2021 J. Chandrashekhara et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

ABSTRACT- For secure and smart transactions over open networks, the Digital Signature Concept is necessary. It is having forms of programs with a view to make certain the integrity of information exchanged or saved and to show the identity of the originator to the recipient. Digital Signature techniques are usually used in cryptographic protocols to provide services like entity authentication, authenticated key delivery and authenticated key agreement. With using cellular devices as a client of internet, the risk of unauthorized and unauthenticated get admission to of crucial files (e.g. contracts, receipts, and so forth.) is growing every day. Although Digital Signature is supposed to be the solution for the unauthorized get right of entry to, its implementation isn't always good enough till now. The symmetric records transfer mechanism is used for the transfer of essential documents, but there's a want of a greater ready mechanism for safe transfer and verification of the documents. This Research paper presents a comprehensive study of Digital Signature and its benefits.

KEYWORDS- Authentication, Cryptography, Digital Signature, Verification

I. INTRODUCTION

Digital signature or digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or report. A valid digital signature offers a recipient cause to agree with that the message became created by using a recognized sender, and that it turned into now not altered in transit. Digital signatures are normally used for software distribution, financial transactions, and in other instances wherein it's far critical to come across forgery or tampering. In our ordinary lifestyles Internet have become integral parts. Security is an important term in this regard. If serious attack occurs, communication, trade, transaction and other important functions will be affected. Public key cryptography is a shape of cryptography, which usually allows customers to talk securely without having prior access to a shared secret key. This is completed by way of the usage of a pair of cryptographic keys unique as public key and personal key. A public key is essentially like an e mail deal with, and a private key, just like the e mail deal with password. The public key is sent to the receiver, at the same time as the non-public key is not disclosed to absolutely everyone [1]. They are related mathematically. What has been encrypted with the first key can only be decrypted with the second - and vice versa [4]. Hence, if a desires to ship a comfortable e mail to B, A ought to encrypt it with B's public key, so that when B receives the encrypted e-mail, he can decrypt it the usage of his own private key. When we say, A encrypts the report, what A in reality does is runs this file thru a hash function software. The hash characteristic software program produces a hard and fast duration of alphabets, numbers and logos for any report. This is known as the hash result. [5] [6]. The hash result is never the equal for two different documents. Any small alteration inside the file will generate a wholly extraordinary hash result. The hash function software will always produce the same hash result of a particular message. Thus, if there may be any doubt about the message being intercepted, all one should do is to examine the hash functions at each ends. Authentication of the digital record will be effected by the use of uneven crypto gadget (that's nothing but the public key cryptography system explained above) and hash function, which envelope and rework the preliminary digital record into any other digital document. A Digital Signature Certificate basically includes the public key of the person who holds it, alongside different details inclusive of contact details, and the most crucial component, this is the digital signature of the Certifying Authority [2][7]. The major reason of one of these certificates is to reveal that a trustable authority appointed and controlled by way of the Government, has attested the statistics contained in the Certificate.

A. Benefits

- While digital signatures have caught the fancy of many corporates and executives, what exactly is it? Simply positioned, a digital signature is your electronic fingerprint.
- It lets you sign a document electronically and it validates the signer.
- It is a mathematical code that authenticates the document from the sender and ensures the document remains unaltered in reaching the recipient.
- Fears about the security of digital signatures is reasonable, however, it uses an accepted format called a Public Key Infrastructure, which provide a very high level of security making it difficult to duplicate.
- Digital signatures make office paperwork far more efficient, but laws regarding this technology vary between countries.

- The benefits of digital signatures have more offices and companies getting on the bandwagon in favor of **e-signatures,** making for a far more efficient and secure workplace, digitally.

II. LITERATURE SURVEY

This phase discusses the studies works conducted to date by way of diverse researchers to implement EGovernance protection the use of several varieties of digital signature schemes.

Table 1: Literature survey on Digital Signatures

Paper title	Authors	Description
Fast ECC Digital Signature Based on DSP	Ying Qin, Chengxia Li, ShouZhi Xu [2]	Since Elliptic Curve Digital Signature Algorithm (ECDSA) is one of the freshest topics within the area of data protection, in this paper the authors have proposed a variable window mechanism method thereby combining NAF and variable length sliding window to reduce the computational complexity of point multiplication of ECC.
Optimistic Fair-exchange Protocols Based on DSA Signatures	WANG Shaobin, HONG Fan, ZHU Xian [2]	The problem of fair exchange is one of the major threats in the field of secure electronic transactions. In this paper the authors have presented a multi signature scheme based on DSA, Which describes a method of constructing efficient fair-exchange protocols based on improved DSA signatures.
A Comparative Analysis of Signature Schemes in A New Approach to Variant on ECDSA	M.Prabu, Dr. R.Shanmugalakshmi [1][2]	The authors have proposed a variant scheme level of ECDSA which produces high level security with the help of parameters. To prove the efficiency of this model, the authors have also provided a comparative result with other signature schemes.
A Digital Signature Schemes Without Using One-way Hash and Message Redundancy and Its Application on Key Agreement	Hua Zhang, Zheng Yuan, Qiao-yan Wen [2]	Digital signature schemes based on public-key cryptosystem are vulnerable to existential forgery attack which can be prevented by use of one-way hash function and message redundancy. In this paper the authors have proposed an forgery attack over the digital signature scheme proposed by Chang and Chang in 2004. The authors have additionally proven stepped forward scheme the use of new key agreement protocol over the Chang and Chang model which honestly lacks the usage of one way hash function and redundancy padding.
Implementation of SHA-2 Hash Function for a Digital Signature System-on-Chip in FPGA	M.Khalil, M.Nazrin, Y.W. Hau [1][2]	With the widespread application of E-mechanisms, the use of secure crypto-systems has become the most important factor for information security. These demanding requirements can be achieved by integrating the cryptosystems into designs based on System-on-Chip (SoC). In this paper the authors have designed and implemented a crypto hash SHA-2 logic core in reconfigurable hardware and also discussed a public-key crypto SoC, which uses the SHA-2 hash core in conjunction with a 2048-bit RSA coprocessor to perform a digital signature security scheme.
Scheme for digital documents management in networked environment	Guifen Zhao, Xiangyi Hu, Ying Li, Liping Du [2]	In this paper the authors have presented a digital documents management scheme based on three-layer structure using symmetric cryptography, combined key and hardware encryption technology to implement the functions of encryption digital signature, authentication and authorization. The authors also claim that this proposed scheme can be easily integrated with available office automation system to promote the management level, work efficiency and resource sharing.

III. PROPOSED APPLICATION AREAS

From the above mentioned literature survey, it is clear that digital signature have already been implemented in various sectors of electronic mechanism. These sectors include the key agreement protocol, contract signing protocol, chip level programming, fault tolerance technique, web based assessment system, identity based authentication, object oriented software engineering, etc. The Key agreement protocol establishes a secure method between two entities who wants to agree on key information secretly over a distributed medium [8]. This protocol should be tough enough to defend the active attacks (i.e. when the intruder subverts the message transmission) and passive attacks (i.e. when the intruder listens the message transmission). Similar techniques can be applied during transactions in E-Governance, E-Shopping, E-Voting, E-Learning, etc. An authenticated key establishment protocol is called identity-based if users use their identity based asymmetric key pair, instead of a traditional public/private key pair, in the protocol for authentication and determination of the established key [9] [14]. This device can be extra affordably applied the usage of ECDSA, ECRSA, EC ElGamal virtual signature algorithms inside the identification primarily based smart card programs in numerous sectors like banking, training, insurance, employment, and so forth. in the developing nations like India. Object oriented software engineering is the industry standard cost effective and faster methodology to develop a software application. This technique cuts the development time and overheads to produce more flexible and easily maintainable software systems. These are the names of the few sectors from the exhaustive list where the digital signatures have been implemented.

IV. DISCUSSION

A. Cryptographic Hash Function

A hash feature maps a variable duration message into a fixed length hash cost or message digest without the usage of any key. The hash characteristic wished for security applications is known as a cryptographic hash characteristic that is computationally infeasible to locate either a message that maps to a pre-unique hash fee or messages that map to the same hash value. In different phrases, a cryptographic hash characteristic should have the one way belongings and the collision resistant property. With the aforementioned residences, a cryptographic hash value is used to decide whether or not the corresponding message has been changed. However, the hash value must be protected [16].

B. Digital Signature

A digital signature is a bit sample that depends on the message being signed and uses some information unique to the signer. The message M is fed into a cryptographic hash feature ensuing in a hash value h or a message digest. The hash fee h which depends at the message M is encrypted the usage of the signer’s non-public key generating the signature. To verify whether or not the digital signature is valid, the result hash value of the message M’ is compared to the value from decrypting the signature using the signer’s public key. If each value is same, the owner of the public key's the writer of the message. Otherwise, the signature is invalid. Digital Signature Standard (DSS) includes three techniques, namely; the Digital Signature Algorithm (DSA), the RSA digital signature algorithm, and the Elliptic Curve Digital Signature Algorithm (ECDSA).

The security of the digital signature relies upon at the cryptographic hash function and the public key cryptographic set of rules. For breaking a digital signature, an attacker may create a fraudulent digital signature by creating a new message for an existing digital signature which is an attack on the Cryptographic hash feature or via constructing a fraudulent virtual signature for a given message that is an assault on the general public key cryptographic algorithm. The hash feature must be collision resistant and the general public key algorithm ought to be sturdy towards attacks. The approved techniques are considered secure. It is computationally infeasible to forge a digital signature. The digital signature provides authentication and non-repudiation. Therefore, if the signature is legitimate, the writer of the message can't deny developing the message [15] [16].

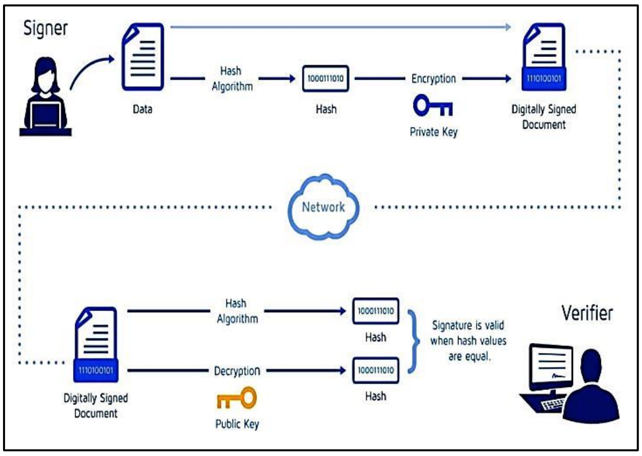

Fig. 1**:** Work Flow of Digital Signature

C. Certificate Authority

Who is Trust Service Providers (TSP) provides digital certificates to ensure that the keys generated and documents signed are created in a secure environment.

D. Digital-ID

A digital illustration of data based at the ITU-T X.509 v3 widespread, related to a person or entity. It is stored in a password included report on a computer or community, a USB token, a smart card, and many others. A digital ID contains a public key certificate, a private key, and other data.

E. Digital certificates

Help to validate the holder of a certificate. Digital certificates contain the public key of the sender and are digitally signed by a Certificate authority.

F. Public key infrastructure (PKI)

Includes rules, protocols, regulations, humans, and structures that resource the distribution of public keys and the identity validation of users with virtual certificate and a certificates authority.

G. Private Key

PKI system, used to validate incoming messages and sign outgoing ones. A Private Key is continually paired with its Public Key in the course of the ones key generations.

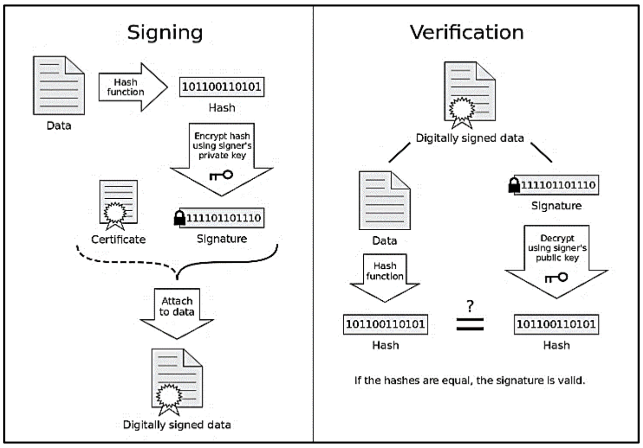

Fig 2**:** Digital signatures and digital certificates work together.

H. Digital signatures are legally valid across many countries of the world.

- The Uniform Electronic Transactions Act (UETA) 1999 and The E-sign Act 2000, USA
- The European Union's Electronic Signatures Directive, Directive 1999/93/EC
- The Information Technology Act 2008, India
- The Electronic Communications and Transactions Act 2002, South Africa
- UNCITRAL Model Law on Electronic Signatures 2001

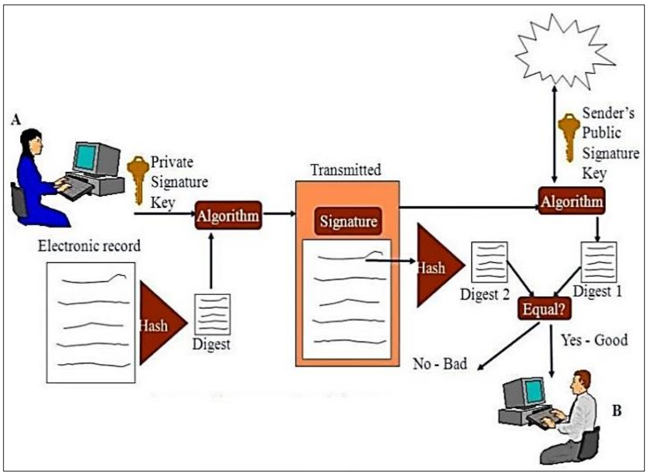

Fig. 3: how the digital signature is verified

The electronic record with the sender's Digital Signature is received by the addressee. The addressee can then test the message digest with the digest received by means of the usage of the sender's public key. If these two digests match, the addressee can be assured that the document has been sent by the sender. In case any adjustments had been made to the report in transit, the digests gained in shape ensuring integrity of the record.

Table 2**:** security services fulfilled by the Digital Signature

Service	**What it means**	**How it is fulfilled**
Privacy/ Confidentiality	Protection against access by unintended recipients	By encryption using the recipient's Public Key
Authenticity	Proof that the sender is actually who he claims to be	By Signing using the sender's Private Key, which can be verified by the recipient using the sender's public key
Non Repudiation	Proof that the sender has actually sent the signed message	
Integrity	Any changes in the original signed message should be detected	

V. CONCLUSION

The Digital Signature is one of the most secure data during online transactions, over the internet. The digital signature has become a significant tool in international commerce. Further 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 upgraded irrespective of the domain specific application of digital signatures, the primary focus is always over the implementation of authentication and integrity of data. Apart from this, non-repudiation, cost efficiency, time efficiency, imposing industry standards, flexibility, etc. had also been taken into account by the researchers. As the client requirements will increase day by day, the new horizon for application of digital signatures using object oriented modelling will get explored. This paper presents the comprehensive information about the digital sign and benefits of same.

REFERENCES

[1] Digital Signature Standard (DSS), FIPS PUB 186-3, 2009.

[2] Abhishek roy And sunil karforma., 'A survey on digital signatures and its applications', J of Comp. and I.T. Vol.3(1&2) (2012).

[3] Sur C., Roy A., Banik S., A Study of the State of E-Governance in India, Proceedings of National Conference on Computing and Systems 2010 (NACCS 2010), January 29, 2010, pp- (a)-(h), organized by Department of Computer Science, The University of Burdwan, West Bengal, INDIA. ISBN 8190-774174.

[4] http://en.wikipedia.org/wiki Digital signature Date of access – 24th March (2012).

[5] Cryptography and E-Commerce, a Wiley Tech Brief, Jon C. Graff, Wiley Computer Publishing, ISBN- 0471-40574-4.

[6] Public Key Cryptography for the Financial Services Industry, the Elliptic Curve Digital Signature Algorithm (ECDSA), ANSI X9.62-2005.

[7] A. Sun et al., "The QR-code reorganization in illegible snapshots taken by mobile phones," in Proc. Int. Conf. on Computational Sci. and its Applicant. 2007, pp.532-538.

[8] Rajapakse HS. Barriers to the public key infrastructure (PKI) deployment and usage for authentic document transaction in Sri Lankan banking sector.2007:18-28.

[9] Hartman B, Flinn DJ, Beznosov K, Kawamoto S. Mastering web services security. John Wiley & Sons; 2003.

[10] Brickell EF, editor. Advances in cryptology-CRYPTO"92: 12th Annual international cryptology conference, santa barbara, California, USA. Proceedings. Springer; 2003.

[11] Sakib AN, Mahmud T, Mountain Munim S, Rahman MM. Secure authentication & key exchange technique for IEEE 802.16 e by using cryptographic properties.

[12] Hartman B, Flinn DJ, Beznosov K, Kawamoto S. Mastering web services security. John Wiley & Sons; 2003.

[13] Mauro Conti, Nicola Dragoni, and Viktor Lesyk , "A Survey of MAN-IN-THE-MIDDLE attacks" 2015 IEEE Communication Surveys & Tutorials.

[14] 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.

[15] Santi Jarusombat and Surin Kittitornkun, "Digital Signature on Mobile Devices based on Location," 2014 IEEE conference.

[16] Harigopal K.B. Ponnapalli and Ashutosh Saxena, "A Digital Signature Architecture for Web Apps", Infosys, India, March/April 2013.

[17] Carlisle Adams and Guy-Vincent Jourdan, "Digital Signatures for Mobile Users", 2014 IEEE Conference, Toronto, Canada.

ABOUT THE AUTHORS

Mr. J. Chandrashekhara has received the BSc. (Computer Science.) degree from Davanagere University and MCA (Master of Computer Applications) from Visvesvaraya Technological University (VTU), Belagavi Karnataka in 2013 and 2017 respectively and Present **Nine** International Research Papers in Various Journals. He presently works as a Lecturer in Department of Studies and Research in Computer Science, Davanagere University, Davanagere, and Karnataka since 2018. His research interest includes Artificial Intelligence and Machine Learning; Cloud Computing, Image Processing, IOT etc.

Ms. Anu V.B has received the BCA (computer Applications) degree from Davangere University and MCA (Computer Applications) from Visvesvaraya Technological University (VTU). Belagavi Karnataka in 2015 and 2018 respectively and present **Three** international Research Papers in Various journals. She presently works as a Lecturer in Department of studies and Research in Computer Science. Davangere University, Davangere and Karnataka since 2018 Her research interest includes Image processing and Networking; Internet Security, Big data etc.

Ms. Prabhavathi H has received the B.Sc.(Computer Science) degree from Davangere University and MCA(Computer Science) from Visvesvaraya technological University (VTU), Karnataka in 2014 and 2018 respectively. She presently works as a Lecturer in Department of Studies and Research in Computer Science, Davangere University, Davangere, and Karnataka since 2019.

Ms. Ramya B.R has received the BSc. (Computer Science) degree from Davangere University and MSc (Computer Science) from Davangere University, Karnataka in 2014 and 2017 respectively. She presently works as a Lecturer in Department of Studies and Research in Computer Science, Davangere University, Davangere, and Karnataka since 2018.