IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-7, Issue-4, April 2019 E-ISSN: 2347-2693

A Comprehensive Study on Digital-Signatures with Hash-Functions

Arvind K. Sharma[1*], Satish.K.Mittal[2]

[1]Dept. of Computer Applications (MMICT&BM), Maharishi Markandeshwar University, Mullana, Ambala (Haryana), India
[2]University School of Engineering & Technology, Rayat Bahra University, Sahibzada Ajit Singh Nagar (Punjab), India

Corresponding Author: arvind.sharma@mmumullana.org

DOI: https://doi.org/10.26438/ijcse/v7i4.604607 | Available online at: www.ijcseonline.org

Accepted: 15/Apr/2019, Published: 30/Apr/2019

***Abstract*:** — From last three decades people from all around the world continuously using services provided by Information Technology industry most probably in every area, in order to fulfill the needs of business to personal activities, but from decade ago demand tremendously increased. Though as we have lots of benefits of using IT services which made our current life smoother, easier and less-hardworking as compare to past yet there is strong need arises to protect our digital world by managing Confidentiality, Integrity, Availability, Authenticity of our resources from those who unwantedly wants to look into ours privacy whether by passive or active attacks. Digital Signature is most important part from Public-key Cryptography that provides a set of security capabilities that would be difficult to implement in any other way especially for proving the authenticity of data.

***Keyword*:** *Algorithm, Authenticity, Avalanche-Effect, Certificates, Confidentiality, Digest, Firewall, Integrity, Hash Function, Non-Repudiation.*

I. INTRODUCTION

There are many types of systems, packages developed by Security Industry which is the back-bone of IT to provide protection with respect to demand, such as Cryptographic algorithms to manage confidentiality of data, Hash algorithms to prove integrity of data, Firewalls to filter the upcoming messages from different location and takes necessary actions as per data arrived and so on. Even though after having such type security suits available with us something was missing like: We're seeking about if everything going well how to prove the authenticity i.e. Does the person who is performing in either direction Genuine one? From that notion 'Digital Signature' came in light. A Digital Signature is an authentication mechanism which enables that creator of a message to attach a secret code with the message that acts as a signature [3] [4] [10]. That secret code is made with the help of deducing the digest of message and then protecting it with sender's private key [5]. The signature guarantees the source and integrity of the message. Otherwise in the absence of this facility many dispute occurs between parties even if we have security mechanism available like: Case-1: An electronic fund transfer takes place, and receiver increase the amount of fund transferred and claim that larger amount had arrived from the sender i.e. Receiver making something wrong. Case-2: Even 'Person-A' sent a message to 'Person-B' but latter on denying that I had not sent and we have nothing to disprove his statement i.e. '**Non-Repudiation'**. Digital Signatures are a standard element of most cryptographic protocol suites that are commonly used for Software-Distribution, Financial Transactions, and in other cases where it is important to detect forgery or tampering. There are two types of algorithms used in construction of digital signatures, which are 'Cryptographic Hash Functions Algorithms' and 'Digital Signature Algorithms'. Let go bit about these two algorithms.

Hash Algorithm(s)

The term 'Cryptographic-Hash-Function' [2] [7] has been used in Computer Science and IT which refers to a function that compresses a message ('m') of arbitrary length to a message of fixed length ('h') called Message Digest/Fingerprint. However if it satisfies some additional requirements, then it can be used for cryptographic applications and then known as Cryptographic Hash functions.

$$h = H(m) \quad \textbf{(1.1)}$$

Where — $H: \{0, 1\}^* \rightarrow \{0, 1\}^n$

— '*' (arbitrary length), 'n' (fixed length)

One-way Hash Function(s) defined by Merkle which is the base for SHS (Secure Hash Standards) evolved by NIST [2] i.e. a hash function 'H', must satisfies the following properties:

1. 'H' can be applied to Block of data (collection of bits) of any length. (any length means size of Block must be greater than size of Digest we conclude at the end).
2. 'H' produces a fixed-length output i.e., Fingerprint/Message Digest.
3. Given 'H' and 'x' (any given input), it is easy to computer Message Digest H(x).
4. Given 'H' and H(x), it is computationally infeasible to find x.
5. Given 'H' and H(x), it is computationally infeasible to find x and x' such that H(x) = H(x').

The first three requirements are must for practical applications of a cryptographic hash function for '**Message Authentication**' and '**Digital-Signatures**". The fourth requirement also known as pre-image resistance or one way property, states that it is easy to generate a message code of given message but hard to generate a message back from given fingerprint/digest. The fifth requirement also known as Second pre-image resistance or Collision resistance property guarantees that an alternative message hashing to the same code as a given message cannot be found. We already provided enough information about cryptographic hash functions in my previous research cum review papers [7] [8], so in this time we're just focusing on digital signature scheme.

Digital Signature Algorithm(s)

The 'Digital Signature Standard' (DSS) proposed by NIST in 1991 and adopted as FIPS-186 in 1994 [7] [10] with continuous revision afterwards. Digital Signature Standards utilizing an algorithm that is specially designed to provide only the digital-signature function. Unlike RSA [5], it cannot be used for encryption or key exchange i.e. we're not saying it just a public key scheme. DSS approach for generating digital-signatures actually works with RSA like algorithms [1]. In the RSA approach, the message to be signed is input to a hash function ('H') that produces a secure hash code of fixed length called digest/fingerprint. This hash code is then encrypted using the sender's private key to form the signature. Both the message and the signature are then transmitted. The recipient takes the message and produces a hash code. The recipient also decrypts the signature using the sender's public key. If the calculated hash code matches the decrypted signature, the signature is accepted as valid else something happen in between the transmission (i.e. integrity effected). Let's have a small diagrammatic representation of how digital signature work:

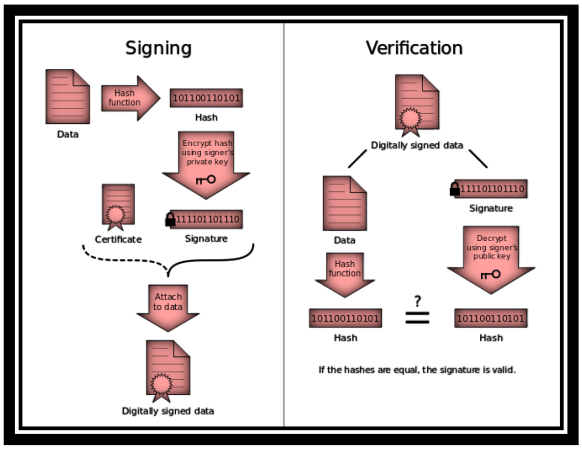

Fig 1.1: Digital Signature Process

Algorithm: Digital Signature (p, q, M, h).

Choose global elements a prime no. 'q' and 'α' i.e. 'α' is primitive root of 'q'.

User-A: Sign the Message 'M'.

Key Pair:

a) Choose random Integer PR_A such that: $1 < PR_A < q-1$
b) Compute $PU_A = (\alpha)^{PR}A \bmod q$.

Sign the Message:

a) Compute h = H (M) such that: $0 < m < q-1$
b) Choose random Integer K such that $1 < K < q-1$ and gcd (K, q-1) = 1.
c) Calculate $S1 = (\alpha)^{K} \bmod q$.
d) Compute $K^{-1} \bmod q-1$.
e) Compute $S2 = K\text{-}1\ (h - PR_A S1) \bmod q-1$.
f) Signature have (S1, S2) pair.

After creation of signature pair, it has to add to ongoing message, which recipient can validates.

USER B: Verify the Message 'M' by signature.

a) Compute $R1 = (\alpha)^{h} \bmod q$.
b) Compute $R2 = (PU_A)^{S1}(S1)^{S2} \bmod q$.
c) If R1 = R2 then Signature is valid else not.

Note: gcd is greatest common divisor, h is hash function.

Organization of the Paper: The rest of the paper is organized like: Section-II covering detail properties of Cryptographic Digital-Signature Scheme, Section-III just focusing on Applications with advantages and bit disadvantages of that particular scheme, In Section-IV we're concluding the work, at the end Reference provided.

II. PROPERTIES OF DIGITAL SIGNATURE

Digital Signature must have following properties in it, so that it will be used successfully for Internet-Security Services, properties are:

- ✓ Signature must have be unique one which means the recipient should understand that the signer signed the document not the adversary.

- ✓ Signature to be used for a particular document and can't be used in another document.
- ✓ Alteration in any means should not be possible if once created.
- ✓ Signature must use/follow 'Public-Key' cryptographic standards (i.e. pair of keys, scheme).
- ✓ Signature creation algorithms must use 'Hash-Functions' [2] [3] inside for computing digest.
- ✓ Signature should full fill 'non-repudiation' property i.e. if signer signs a document then afterward signer can't be able to claim that he/she haven't signed.

Conception behind using digital signatures technology raising its head due to fulfilling three primary goals of Internet Security which are: 'Data or User's Authentication', 'Data Integrity' and 'Non-Repudiation'.

Data-Authentication (Proof-of-Origin): Before using upcoming message its authenticity have to be proved due to security reasons so, while the verifier going to validate the 'Digital-Signature' attached with actual message using 'Public-Key' of a sender, he/she is assured that signature has been created just by sender who've corresponding secret 'Private-Key' and no one else like adversary.

Data-Integrity: It may be the case an attacker/adversary who is analyzing traffic has access to the data and alter it before it reaches to destined receiver. The digest of altered data and the output provided by the verification algorithm will not match i.e. verification fails. Hence due this receiver can safely deny the message with strong hypothesis that data integrity has violated. Which prove easily by introducing avalanche-effect while comparison operation comes as rescue?

Non-Repudiation: Since it is assumed that only the signer of the message has enough information of the signature keys, so he's the only one who can create unique signature on a given message (bits) [8]. Thus the receiver can be able present data and the digital-signature attached with that message to a third party as evidence/proof if any dispute occurs in the future to put his/her point with confidence.

III. APPLICATIONS WITH PROS AND CONS

Even though digital signatures have many benefits in industry yet have bit drawbacks too, in this section we're focusing on advantages and disadvantages of digital signatures.

Pros of Digital-Signatures

Better Customer Experience: The digital-signatures provide the convenience of signing crucial documents whenever & where ever required without caring about person's location to sign. Now customer care executive don't have to wait for the customer's visit to offices i.e. documents can be signed at the door step easily. Now the customer has the freedom to be anywhere in the globe and, engage with a company, making services and businesses far more easy and user friendly.

Business Efficiency: As compared to the benefits cost involves in integrating digital-signatures into the work processes is relatively small. With quicker contract turnaround time & reduced the work flow time, digital signatures are ideal for corporates.

Cost Saving: Corporates see significant cost benefit with little or no expense in ink, paper- printing, scanning and, travel apart from this indirect costs such as filing, re-keying, archiving, and, tracking is very less.

Future & Legal Validity: The digital-signatures hold the validity into future i.e. Electronic Signature and Infrastructures (ETSI) PDF Advanced Signatures with its Electronic Identification, Authentication and Trust Services (eIDAS) requirements have validity well into the future with its long term signature formats. As well as legally this can stand in any court of law like any other signed paper documents. Digital time stamping and ability to track and easily archive documents improve and simplify audit and compliance.

Global Acceptance: Corporates in different countries are accepting digital-signatures to legally bind documents because of their belief that the security services/protocols offered by vendors such as '**DocuSign**' are in compliance/fulfilling with International Standards in this field. Majority of the world's governments recognized digital-signatures provided by '**DocuSign'** and other similar third party companies, and industry have blind faith on these third parties because of many valid reasons.

Independent Verification: The digital-signatures offered by companies like '**DocuSign**' can withstand stringent independent verification and can't be altered by unauthorized parties.

Long Term Retention and Access: The signatories to a digital-signature file don't need to rely on a single vendor's continued presence in the marketplace in order to continue to verify its authenticity. Many other kinds of e-signature offering companies have their protocols of regulating and safeguarding their data, but yes they haven't achieved universal legal acceptance. If a customer later switches to another vendor, he could lose access to signatures stored with the original company and have to buy fresh services.

Save Time: Now no longer person have to wait for senior dignitaries to return back from holidays or business tours for signature. Digital-Signatures ensure that businesses save on cost and time with documents and contracts signed off with just a click. There are maximum savings in cost and time especially when the person required to sign in distinct

geographical locations. Documents can be signed off frequently from anywhere.

Security: The digital-signature offers more security than an electronic-signature reason behind this is, a unique identifying "digest/fingerprint" permanently embedded within a document which was made with Hash-Functions [2]. Sign document if altered can be easily detected w.r.t. the properties of hash functions.

Workflow Efficiency: With lesser delays, digital-signatures ensure better efficiency. The management and tracking of documents are easier, with lesser effort and time consumed. Many features of the digital-signatures help speed up the overall work process. At any instance, tiny email notification helps to remind the person about to sign, while status tracking helps to know at which stage the document is now.

Cons of Digital-Signatures

Key-Management: The private keys must have to be kept in a secured manner somewhere as well as its distribution, expriy of public-private key pair have to be manage separately.

Time Consumption: The process of generation and verification of digital-signature requires considerable amount of time as well.

The advantages greatly overshadow the disadvantages practically the only disadvantages of using digital signature are the weak laws regarding '**Cyber-Security**' which might cause any unnecessary hassles in case of a court case and that both parties have to purchase the '**Certificates**' for the digital-signature in order to use it instead of the one party courier charge. For using the digital-signature the user has to obtain pair of keys (Private and Public), the receiver has to obtain the digital-signature certificates too.

IV. CONCLUSION

The digital-signature continually gain it's important and has become a notable tool from last two decades especially in corporates world. So we can say that Digital Signature minimizes the risk of financial dealings as well as minimizes the risk of Forgery. It retains a high degree of the information security and identity. By using the strong 'Encryption' techniques and 'Hash-Functions' a fair unit of 'Authenticity', 'Confidentiality', 'Integrity', 'Access-Control' of data is maintained. Forthcoming it's requisites to check the penetrability of the system and develop a secure corporate environment.

REFERENCES

[1]. Rivest, MIT Laboratory for Computer Science and RSA Data Security, Inc, Request for Comments : 1321, April 1992.

[2]. FIPS180-3, Secure Hash Standard (SHS), National Institute of Standards and Technology, US Department of Commerce, Washington D. C., 2008.

[3]. Junling Zhang, 'A Study on Application of Digital Signature Technology', 2010 International Conference on Networking and Digital Society, 2010 IEEE, Pg.: 498-501, Wenzhou China, 30-31 May, 2010.

[4]. RavneetKaur, 'Digital Signature', 2012 International Conference on Computing Science, 2012 IEEE, Pg.: 295-301, India, 14-15 Sep 2012.

[5]. PriyankaYadev, 'Digital Signature', International Journal of Engineering and Management Science, Vol. 3(2), Pg.: 115-118, Year 2012.

[6]. PayelSaha, 'A Comprehensive Study on Digital Signature for Internet Security', ACCENTS Transaction on Information Security, Vol. 1(1), Year 2016.

[7]. Arvind Sharma, "Comparative Analysis of Cryptographic Hash Function", International Conference on Big Data, Computer Science and Information Technology (ICBDCSIT), Proceedings of 18th IRF International Conference, New Delhi, India, 09th September, 2018.

[8]. Arvind Sharma, "Attacks on Cryptographic Hash Function and Advances", IJICS, Vol 5, Issue-11, 2018.

[9]. William Stallings "Cryptography and Network Security Principles", 5th Edition.

[10]. Forouzan, "Data Communication and Networking", 4th Edition, McGraw Hill Pg.: 961-1023

[11]. https://en.wikipedia.org/wiki/Digital_Signature_Algorithm

AUTHOR PROFILE

Arvind K. Sharma working as Assistant Professor in Department of "MMICT&BM" M.M. University, Mullana, Ambala (Haryana). Previously he worked for Chandigarh University (CU) in Department of CSE, Mohali (Punjab) and Trinity College, Jalandhar (Punjab) in the Department of Computer Science as Assistant Professor. He is pursuing his Ph.D. from Rayat Bahra University, Mohali in the field of CSE in Networking and Security branch from 2016 onwards. He has received his M.Tech. CSE Degree from Lovely Professional University, Phagwara in 2015 and, MSc. Computer Science Degree from Guru Nanak Dev University, Amritsar in 2011. His Area of Interest is "Networking and Security", "Routing & Switching", "Programming", "R-DBMS".

Dr. S. K. Mittal is heading (Departmental Head: University School of Engineering & Technology) and (Dean: R&D Branch) in Rayat Bahra University, SAS Nagar, Punjab, India. He has nearly three decades of experience in industry, research and in Teaching. He's a renowned personality having 60+ research publications. He was former Scientist of 'Computer Society of India' CSI, Chandigarh.

