BioGecko

Vol 12 Issue 02 2023
ISSN NO: 2230-5807

Digital Signature to enhance Authenticity and Confidentiality

Dr. Puspita Dash[1], Saiprasad J[2], Barathraj S[3], Akkash K[4]
[1] Assistant Professor,Dept. of Information Technology, Sri ManakulaVinayagarEngineering College,Puducherry, India
[2,3,4] Dept. of Information Technology, Sri ManakulaVinayagarEngineering College, Puducherry, India

ABSTRACT
In this modern world each and every millisecond an enormous amount of file transmission takes place around us either through wired or wireless medium. And these wired or wireless file transmissions are protected by various protocols and firewalls. Even though there occurs a data breach. So we need an efficient mechanism to maintain authenticity, integrity, confidentiality of a file/document/message. So in practice we use a digital signature; it is a mathematical technique equivalent to handwritten signatures or stamped seals. It is based on hashing and asymmetric cryptography. But digital signatures lack confidentiality of a file and moreover it is prone to some security vulnerabilities. So in this report we have proposed an enhanced mechanism to overcome these problems. This to achieve confidentiality and data integrity with the project presents a more radical and modern approach for a safe and secure file transmission confidentially between the respective users. Digital signature follows a single encryption process only with the sender's private key and decryption process only with the sender's public key. But we are going to implement the double encryption process help of both sender and receiver keys and introducing an open public hash linked key storage space to ensure authenticity and to eradicate the third party certificates.

Keywords: Digital Signature, Public key-Private Key, Cryptography, Third Party Digital Certificates.

INTRODUCTION

The prefix "crypt" means "hidden" and the suffix graphy means "writing". It is a mathematical technique used in computer networks for secure and confidential file transmission. Cryptography consists of two techniques they are encryption and decryption. Encryption is a technique used to convert a readable and understandable format into a non-readable and non-understandable format. So, that only the respective user can view the message. Decryption is the reversible format of encryption in which it converts the non-understandable encrypted format to the original readable format.

1.1 TYPES OF CRYPTOGRAPHY

1.1.1 Symmetry Key Cryptography

Symmetry Key Cryptography uses a single key for
both encryption and decryption process. So there are many problems with key breach.

1.1.2 Asymmetric Key Cryptography

Asymmetric Key Cryptography uses two keys. They are public key and private key. Public key is used for encryption and private key is used for decryption. Sometimes viceversa based on the applications. Asymmetric Key Cryptography is used in various computer network applications like SSL/TLS Certificates, Digital Signature, Web Browser, Email etc.,. In which Digital Signature is widely used in many industries and applications to prevent secure file transmissions.

1.2 DIGITAL SIGNATURE

A digital signature is an electronic, encrypted, stamp of authentication on digital information such
as email messages, electronic documents. A signature confirms that the information originated from the signer

and has not been altered. It ensures authenticity, data integrity and non-repudiation of a file. It is based on Asymmetric PKI Infrastructure and it involves Hashing technique to produce message digest in order to generate Digital Signature.

1.3 HASHING

Hashing is the process of transforming a given string input into a shorter and fixed unreadable format. The main reason for using hashing is the hashed value cannot be tampered. The function used in hashing is known as hash function which consists of mathematical operation and algorithms and the output of the hash function is known as Message Digest(MD).

1.4 DIGITAL SIGNATURE GENERATION PROCESS

1. The sender file is first given as an input to the hashing function so that we will obtain a Message Digest.
2. This Message Digest is encrypted with the sender's private key, such that we have successfully generated the Digital Signature.
3. The Digital Signature is attached with the original file and transmitted to the receiver.
4. The receiver decrypts the Digital Signature with the help of the sender's public key obtained from the open public space, so that we will obtain the sender's message digest.
5. After obtaining the sender's message digest, the receiver hashes the received file and generates the message digest using the same hashing algorithm.
6. If the sender's message digest and the receiver side generated message digest are the same, then it is an appropriate file.
7. If the file is tampered or if the file is not from the appropriate sender then the message digest can't be decrypted and matched correctly.

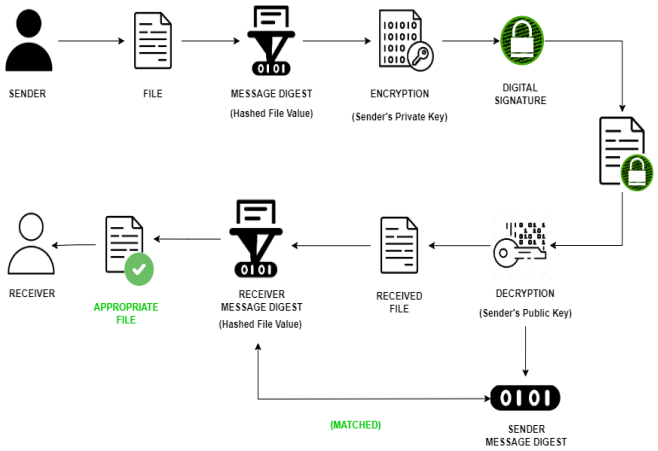

Fig 1. Digital Signature Architecture
(If it is from the appropriate sender)

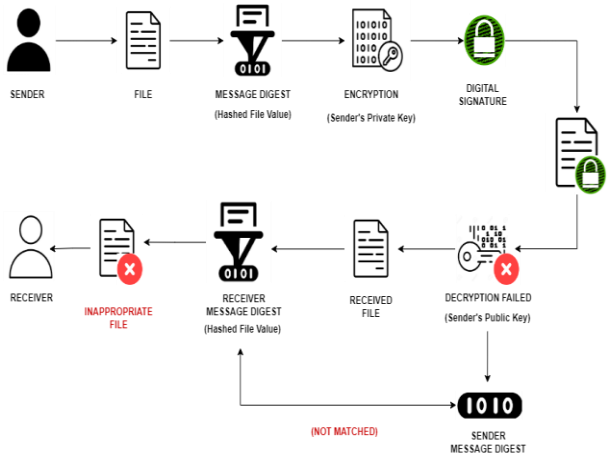

Fig 2. Digital Signature Architecture
(If it is not from the appropriate sender)

1.5 CRYPTOGRAPHIC ALGORITHM

Cryptography algorithms are the means of altering
data from a readable form to a protected form and back to the readable form. Cryptographic algorithms are used for important tasks such as data encryption, authentication, and digital signatures.

1.5.1 RSA Algorithm in Cryptography

RSA is an **asymmetric cryptographic** algorithm. RSA Algorithm works on a block cipher concept that converts plain text into ciphertext and vice versa at the receiver side. If the public key of User A is used for encryption, we have to use the private key of the same user for decryption.

Step 1: Select two prime numbers **p** and **q** where p not equal to q.

Step 2: Calculate **n= p*q** and **z=(p-1) *(q-1)**

Step 3: Choose number e: Such that e is less than n, which has no common factor (other than one) with z.

Step 4: Find number d: such that **(ed-1)** is exactly divisible by 2.

Step 5: Keys are generated using n, d, and e

Step 6: Encryption

c=m pow(e) mod n

(where m is plain text and c is ciphertext)

Step 7: Decryption

m= c pow(d) mod n

Step 8: Public key is shared and the private key is hidden.
Note: **(e, n)** is the public key used for encryption. **(d, n)** is the private key used for decryption.

The RSA algorithm has the drawback of being quite inefficient in cases in which large volumes of data must be authenticated by the same virtual machine. A foreign entity must substantiate the dependability of authentication tokens. Data is routed through middlemen, who may corrupt with the cryptosystem.

1.6 HASHING ALGORITHM

Hashing algorithm is used to create a unique output of a specific length. This output, called a hash value or a hash digest, represents the original data without making that original data known or available to access. This can be used for everything from data organization to file integrity verification.

1.5.1 Secure Hash Algorithm 256 Bit

SHA 256 is a part of the SHA 2 family of algorithms, where SHA stands for Secure Hash Algorithm. Published in 2001, it was a joint effort between the NSA and NIST to introduce a successor to the SHA 1 family, which was slowly losing strength against brute force attacks. The significance of the 256 in the name stands for the final hash digest value, i.e. irrespective of the size of plaintext/cleartext, the hash value will always be 256 bits.

1.5.2 Steps in SHA - 256

The SHA - 256 Algorithm consists of five steps.

Step - 1 (Padding Bits)

The first step is to add some extra bits to the message, such that the length is exactly 64 bits short of a multiple of 512. During the addition, the first bit should be one, and the rest of it should be filled with zeroes

Step - 2 (Padding Length)

Now we can add 64 bits of data to make the final plaintext a multiple of 512. We can also calculate these 64 bits of characters by applying the modulus to your original clear text without the padding.

Step - 3 (Initialize The Buffers)

Now we need to initialize the default values for eight buffers to be used in the rounds as follows:

a = 0x6a09e667

b = 0xbb67ae85

c = 0x3c6ef372

d = 0xa54ff53a

e = 0x510e527f

f = 0x9b05688c

g = 0x1f83d9ab

h = 0x5be0cd19

Step - 4 (Compression Functions)
The entire message gets broken down into multiple blocks of 512 bits each. It puts each block through 64 rounds of operation, with the output of each block serving as the input for the following block.
Step - 5 (Generating Output)
With each iteration, the final output of the block serves as the input for the next block. The entire cycle keeps repeating until you reach the last 512-bit block, and you then consider its output the final hash digest. This digest will be of the length 256-bit.

LITERATURE SURVEY

2.1.1 RSA Double Encryption

In this paper the author proposed that double encryption helps us to enhance the confidentiality of the digitally signed document or file[1]. A double encryption process is performed on the sender side. The first encryption (i.e ENCRYPTION-I) uses the sender's private key to encrypt the generated message digest. The second encryption (ENCRYPTION-II) uses the receiver public key to encrypt the file to be transmitted to the receiver. On the receiver side the digital signature is first decrypted (i.e DECRYPTION-I) with the sender's public key and then the encrypted file is decrypted (i.e DECRYPTION-II) with the receiver private key and then the sender's decrypted message digest is checked with the receiver generated message digest. If it equals then it is an appropriate confidential file from the respective sender. This paper ensures File Confidentiality But even though this model is prone to Man in the Middle Attack.

2.1.2 Implementation of VPN Gateway

In this paper the author discussed the use of VPN (Virtual Private Network)to prevent Man in the Middle Attack. VPN stands for Virtual Private Network, it is used to encrypt the user identity details in the network[2]. So that the hacker performing the man in the middle attack can't be able to identify the targeted user. But at the same time it lacks authenticity because the receiver isn't able to verify whether it is from the verified sender because the Virtual Private Network Software encrypts the sender identity. So that this mechanism prevents Man in the Middle Attack. But it is based on Third Party Software Dependencies for establishing VPN networks and lack of Confidentiality and authenticity.

2.1.3 User Authentication Using Generalized Digital Certificates

In this paper, the author proposed the concept of generalized digital certificate (GDC) that can be used to provide user authentication and key agreement [3]. A GDC contains the user's public information, such as the information of the user's digital driver's license, the information of a digital birth certificate, etc., and a digital signature of the public information signed by a trusted certificate authority (CA). This technique maintains Authenticity and prevents Man in the Middle Attack. But it is dependent on a third party Certificate Authority(CA).

2.1.4 Inter Web Proxy Service Model to prevent Message Alteration

In this paper the author proposed Web Service Registration and Routing System and Inter Proxy Web Service that effectively prevents the message alteration attacks, Man-in-the Middle attacks and other types of attacks in order to secure Web service at message level.[4]New agents such as requester agent and provider agent have been deployed at the client and server side respectively. These two agents are responsible for effective monitoring and controlling of various messages and attacks at the message level. In addition to this, a security token is created for each user request to verify the validity of the service provider and service requester for effective and secured communication. It prevents Dos Attack and MITM Attack. But not optimal for Digital signature Mechanism. And this mechanism is not supported for all browsers.

2.1.5 Digital Signature Based on ISRSAC

This paper proposed that PKI Infrastructure has been widely used in security in recent years[5]. The most used public key cryptography algorithm is RSA and its difficulty is based on the large integer decomposition problem.So that we are going with ISRSAC a security improvement model of the RSA algorithm which increases the complexity in factoring the value of modulus `n'. The ISRSAC is a proxy based signature algorithm

and it is based on two kinds of multi-signature algorithms that were presented, which includesequential multi-signature and broadcasting multi-signature. Even though this mechanism maintains file confidentiality, it is prone to MITM attack

2.1.6 Secure Generation using a Compromised Computer.

In this paper the author proposed two conditions. The first thing is receiving a secure confirmation of the target data and the second thing is secure activation of the signature process.[6] This paper describes a new signature system that meets these conditions by using virtual machines, a tamper-resistant module, and a cryptographic protocol. This proposed system is as secure as the underlying virtual machine monitor. This mechanism prevents the intruder from generating the user's legitimate signature against the user's intention. This mechanism is but this mechanism is more complex and increases the latency time during file/data transmission.

2.1.7 Digital Signature Based on Device Location

In this paper the author proposed a location based digital signature. It uses geo-encryption to generate digital signatures[7]. In this technique the sender's device geo-location is used for encryption and this geo-location is obtained from the Global Positioning System(GPS). So that if the intruder legitimate the transmission and sends his/her fake file, the location of the sender varies. So that the receiver can know that it's not from the appropriate sender. But if the intruder is also in the same location or if he corrupts the location using VPN then the receiver isn't able to identify the appropriate sender.

2.1.8 Digital Signature Verification Based on BioGamalALgorithm

In this paper the author proposed a secured digital signature algorithm [8]. It uses the concept of hybridization of secure hash code. DNA encryption/decryption technique and elgamal encryption/decryption techniques. The use of SHA algorithm generates a secure hash code and hybridization of encryption algorithm which reduces the computational complexity and this research method is then compared with existing Play Gamal algorithm with respect to encryption/decryption time complexity. It only focuses on strong encryption of the file from the intruder and thus it maintains confidentiality but it lacks focus on authenticity so that this technique is prone to MITM attacks.

SYSTEM DESIGN

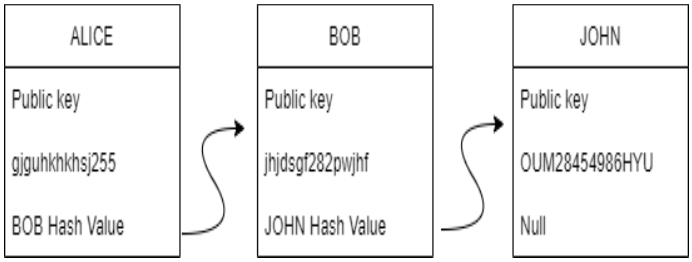

Fig 3. Open Space Key Storage Area Architecture

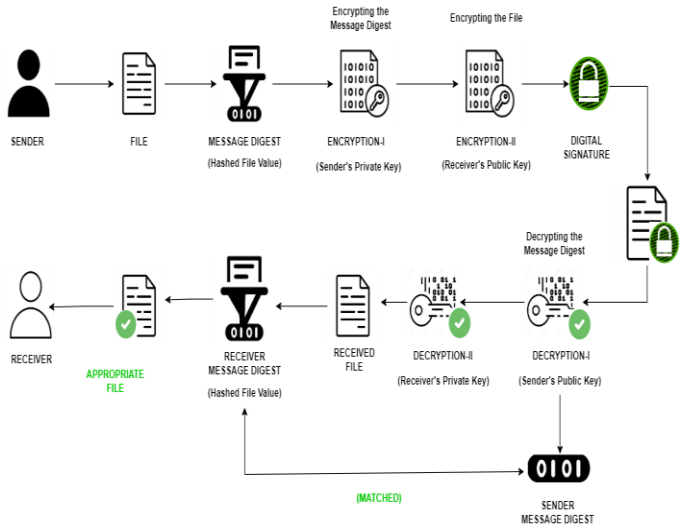

Fig 4. File Transmission Architecture

3.1 Modules

3.1.1 Transmission Module

3.1.1.1 Encryption

In order to achieve confidentiality in digital signature we perform double encryption on the sender side. The first encryption (i.e ENCRYPTION-I) uses the sender's private key to encrypt the generated message digest. The second encryption (ENCRYPTION-II) uses the receiver public key to encrypt the file to be transmitted to the receiver.

3.1.1.2 Decryption

On the receiver side the digital signature is first decrypted (i.e DECRYPTION-I) with the sender's public key and then the encrypted file is decrypted (i.e DECRYPTION-II) with the receiver private key and then the sender's decrypted message digest is checked with the receiver generated message digest. If it
equals then it is an appropriate confidential file from the respective sender.

3.1.2 Key Storage Module

In order to overcome the Man in The Middle Attack and to eradicate the third party dependency we are replacing the public key storage open space into a blockchain network to store the user's public key. So that the hacker isn't able to pretend like the sender by changing the sender's public key information or by creating a duplicate sender's public key information. Since blockchain prevents tampering of data such that once the public key information inserted by the user, can't be modified by the hacker or by anyone and moreover this information is open to everyone.

CONCLUSION

These papers give us a brief idea about digital signatures and various ways to prevent the digitally signed paper from alteration and from various attacks by the hacker. From these techniques we have clear that digital signatures are prone to MITM attack and it needs an independent trusty environment to verify the sender's profile and this can be done by creating a trusty open space key storage network.

ACKNOWLEDGEMENT

I would like to thanks the anonymous referees for their helpful guidance that has improved the quality of this paper. I would also like to express my gratitude and sincere thanks to ours guide Dr. Puspita Dash, Assistant Professor of Department of Information Technology for her valuable support, help and guidance in the completion of this paper.

REFERENCES

Sajal Jain, ShivamSharama, B.R Chnadravarkar, “Mitigating Man-in-the-Middle Attack in Digital Signature,” IEEE Xplore Issue : 15, October 2020.

Chen Fei, WhuKehe, Chen Kei, ZanhQuanyum, “The Research and implementation of VPN Gateway using SSL,” IEEE Xplore Issue : 24, October 2013.

Lien Harn, Jein Ren, “Generalized Digital Certificate for User Authentication and Key Establishment for Secure Communications,” IEEE Xplore Issue : 19, May 2011.

S. Chakravarthi, P. Visu, B. Balu, V. Vineshwaran, M.Yakshraj, ”Web service registration and routing system and inter web proxy service model prevents the message alteration attacks, man-in-the middle attacks,” IEEE Xplore Issue : 19, Oct 2017.

Teng Yang, Yanshou Zang, Song Ziao, Yimin Zhao, “Digital signature based on ISRSAC, ”IEEE Xplore Issue : 28, Jan 2021.

Hideki Tanaka, Shaochi Sasaki, Isao Eschizen, Hiroshi Yoshiura, “Secure Generation of Digital Signature on Compromised Computer,” IEEE Xplore Issue : 25, Feb 2008.

Santi Jarusombat, SurinKittitarkun, “Digital Signature on Mobile Devices based on Location,” IEEE Xplore Issue : 2, April 2007.

Rashmi Kasodhan, Neethesh Gupta, “A New Approach of Digital Signature Verification based on BioGamal Algorithm,” IEEE Xplore Issue : 29, Aug 2019.

W.Stanlings, “ Internet and Network Security,” Volume : 6, Issue : 2, April 2021.

S.R. Subramanya, “Digital Signatures,” IEEE Xplore Issue : 15, June 2022.

A.Eskicioglu,L. Litwin “Cryptography,”IEEE Xplore Issue : 1, Feb 2020.