International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.
© 2022 Scholar AI LLC.

Vol. 42 No. 1 December 2023, pp. 399-409

Digital Signatures Chain and El Gamal Scheme Integration for Data Transmission Integrity in Digital Transaction

Boy Sampetua Sipahutar[1], Aulia Khamas Heikhmakhtiar[2], Rinaldi Munir[3]

[1,2]Science and Defense Technology Faculty
The Republic of Indonesia Defense University,
Bogor, Indonesia
[1]boy.s.sipahutar@gmail.com, [2]aulia.heikhmakhtiar@idu.ac.id

[3]Institut Teknologi Bandung
Bandung, Indonesia
rinaldi@staff.stei.itb.ac.id

Abstract—Digital signatures have been widely used by both private and government agencies. However, the use of chain digital signatures is still not widely used, especially in the military world. This results in a lack of ability to ensure data integrity, where it will be difficult to find out who has made changes to the document and to find out the original source of the document. This paper proposes a digital signature chain as a solution to guarantee data authenticity and prevent tampering during transmission. This technique involves creating a chain of digital signatures that are attached to data before it is sent over the network. The proposed method is expected to provide a more secure and efficient way to ensure data integrity, compared to traditional methods such as encryption and checksums. This paper evaluates the effectiveness of the proposed method through a series of experiments and shows that digital signature chains are an effective and reliable way to secure and maintain data transmission over networks. The proposed research aims to evaluate the effectiveness of digital signature chain technology in ensuring data security and integrity and to provide recommendations for its implementation.

Keywords— Digital Signature, Signature Chain, Secure Data Transmission, Data Transmission Integrity.

I. INTRODUCTION

In the modern era data transmission security and integrity become important [1]. It is to ensure that the transmitted information or data remains confidential and does not change during the transfer process. One technique that can be used is a chain of digital signatures [2]. A chained Digital Signature is a cryptographic method that is expected to provide a strong framework for verifying the authenticity and integrity of transmitted data. There are several significant advantages to be gained by implementing a serial digital signature, including ensuring that the sender of the data can be identified by the recipient and can also re-track who sent the data the first time [3]. Second, the chain structure guarantees the chronological order of data transmission, making it impossible for any malicious actor to modify or manipulate information without being detected.

Along with the increase of digital devices and networks used, there is also a growing need for secure and reliable methods of data transmission. Digital signature chain technology has emerged as a potential solution for secure data transmission, ensuring both data security and integrity [2]. The use of digital signature chain technology can help to prevent unauthorized access, modification, and tampering of sensitive data. However, there is still not much research regarding the application of digital signature chain technology. This study aims to address this gap by exploring the use of digital signature chain technology for secure data transmission over networks, with the goal of enhancing the security and integrity of data.

The increasing use of digital devices and networks has led to a new challenge, namely, to ensure data security and integrity when data is transmitted. Highly confidential data needs to be transmitted securely and reliably, to prevent unauthorized access, modification, and tampering. In this study, digital signature chain technology can be a potential solution to ensure data security and integrity. However, research regarding the application of this technology is still very minimal. The gap between this research and previous research is the use of digital signature chains to further improve data integrity, with a pattern like that used by blockchains.

II. RELATED WORK

A digital signature is a mathematical scheme used to prove the authenticity of a digital message or document [2]. This scheme ensures that data and information are indeed obtained from appropriate sources. A digital signature consists of a sequence of hash functions generated from a specific hash function algorithm and encoded (encrypted) using an asymmetric key cryptography algorithm [4]. The signature is then verified using the public key.

The digital signature is made by affixing a "sign" in the form of codes that are placed at the end of the document. These codes are generated from the process of encrypting messages with cryptographic algorithms [5]. With the existence of this digital signature, a recipient of the message can be sure that the documents they receive are correct and original, originating from the actual sender of the message, and that there are no modifications in the document by unauthorized parties or intruders [6].

The Digital Signature scheme aims to enhance security and efficiency in IoT applications by leveraging the cryptographic properties of elliptic curves [7] [8]. It provides a lightweight and computationally efficient digital signature solution suitable for resource constrained IoT devices. Digital signatures have been very widely used for the needs of the health sector, IoT, and other fields.

Back in the years, Leslie Lamport, in his paper from 1981, proposed a method for password authentication, based on sequential hash calculations starting from a given initial value [9]. This study departs from the method carried out by the hash chain. A hash chain is generally defined as the iterative application of a cryptographic hash function to a given data asset. This type of cryptographic hash can be very useful in certain security settings. By providing successive chains, hash chains make it more difficult for snooping hackers to hijack data assets by applying a single input [10]. The same thing can be applied to digital signatures where each signature will be linked sequentially. Hash chains are much like block chains [11], in that they both use cryptographic hash functions and create links between two nodes. However, blockchains are generally intended to support distributed agreement around public ledgers (data) and incorporate a set of rules for data encapsulation and associated data permissions [12].

III. METHODOLOGY

This study is to investigate the application of digital signature chain technology for securing data transmission over networks. This study aims to evaluate the effectiveness of digital signature chain technology in ensuring data security and integrity, as well as to identify its advantages and limitations. The research will also provide recommendations for the implementation of digital signature chain technology. This study is expected to contribute to the development of best practices for implementing digital signature chain technology, as well as to the understanding of its effectiveness in ensuring data security and integrity. This study will provide valuable insights for military organizations and other sectors that rely on secure data transmission.

The research will use a mixed-method approach, including a literature review and a case study. The literature review will provide an overview of existing research on digital signature chain technology and its application in various contexts, including the government sector. The case study will involve the implementation of digital signature chain technology, and its evaluation based on various parameters such as data security, integrity, and efficiency. To ensure data integrity during network transmission, we propose the digital signature chain process as shown in figure.1 below.

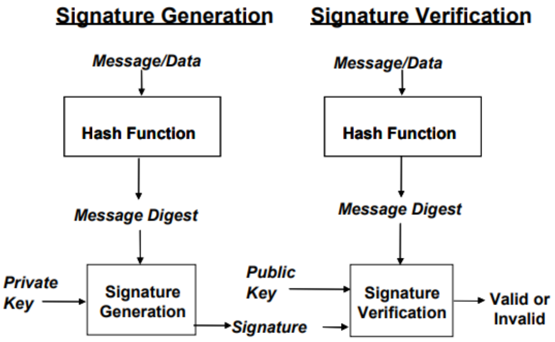


Fig. 1. Digital Signature Processes

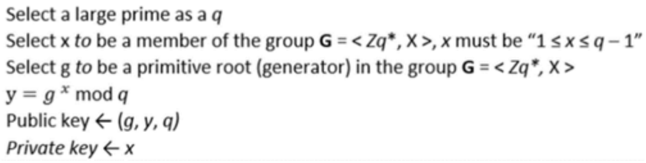
Data will be signed by the sender using their private key to be sent to the recipient. And then the recipient of the data will verify the signature to ensure the authenticity of the signature using the sender's public key. In addition to maintaining data security and integration, the use of digital signature chains also provides non-repudiation, meaning that the sender cannot deny having sent the data (message or document) because their digital signature is proof of their identity.

Digital signature chains have been applied in various contexts, including mobile applications [13], finance, healthcare, and government but it still needs further research on the application of this technology in many sectors where data security and integrity are of utmost importance. Kim [14] in his paper, proposed a hash chain-based electronic signature model to ensure authentication and integrity of routing and forwarding messages in a sensor network. That's because the public key-based digital signature has some disadvantages: it costs a lot to use, and it takes a long time during the process of generating and verifying digital signatures. Therefore, it is confirmed that this hash chain-based digital signature model is more proper in a sensor network where routing and forwarding messages can frequently happen.

At the sign process, the signature will use El Gamal Scheme digital signature to build the signature chain [13] [14] [15]. The ElGamal signature scheme is a digital signature scheme which is based on the difficulty of computing discrete logarithms. It was described by Taher Elgamal in 1985 [16]. The ElGamal signature scheme is a digital signature scheme based on the algebraic properties of modular exponentiation, together with the discrete logarithm problem. The algorithm uses a key pair consisting of a public key and a private key. The private key is used to generate a digital signature for a message, and such a signature can be verified by using the signer's corresponding public key.

This research will also use AES encryption to encrypt the signature. Advanced Encryption Standard (AES) is a cryptographic symmetric encryption algorithm that is quite popular in the IT world [17] [18]. AES (Advanced Encryption Standard) is a continuation of the obsolete DES (Data Encryption Standard) encryption algorithm [18]. The AES algorithm is used to secure data [20]. AES encryption has a very strong key on your box that can only be unlocked with a very specific key. The lock is so strong that it would be very difficult for someone to crack it and open the box without the proper key.

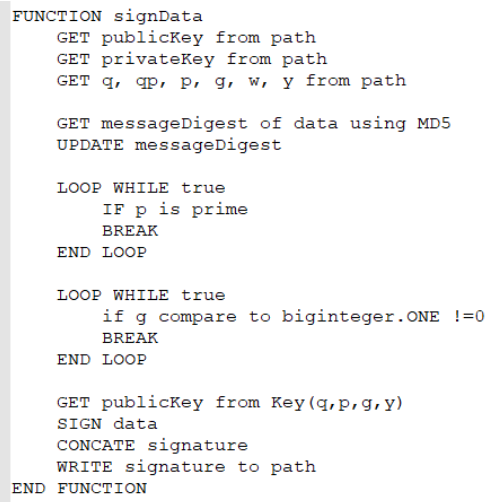
Following are the captures of the generated pseudo code, conducted while research process:



```
Select a large prime as a $q$
Select x to be a member of the group G = < $Zq^*$, X >, $x$ must be "$1 \le x \le q - 1$"
Select g to be a primitive root (generator) in the group G = < $Zq^*$, X >
$y = g^x \bmod q$
Public key ← $(g, y, q)$
Private key ← $x$
```

Fig. 2. Key generating process.

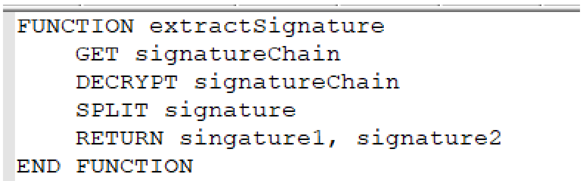
This function is used to generate, for further explanation, you can refer to ElGamal Digital signature scheme, Key Generation section.



```
FUNCTION signData
    GET publicKey from path
    GET privateKey from path
    GET q, qp, p, g, w, y from path

    GET messageDigest of data using MD5
    UPDATE messageDigest

    LOOP WHILE true
        IF p is prime
        BREAK
    END LOOP

    LOOP WHILE true
        if g compare to biginteger.ONE !=0
        BREAK
    END LOOP

    GET publicKey from Key(q,p,g,y)
    SIGN data
    CONCATE signature
    WRITE signature to path
END FUNCTION
```

Fig. 3. Sign Process

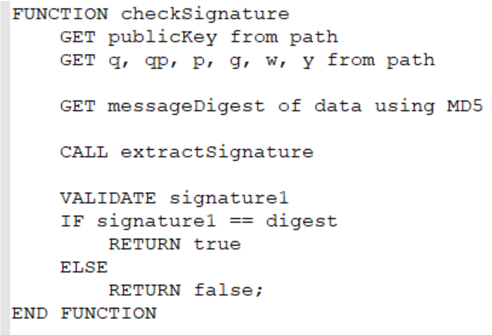
This function is the main function for the signing process, in the first line the function will take of the data message digest and then do the ElGamal signature signing process. After the signing process, the function will combine the signature with the previous signature using the specified delimiter or initiate it, if it does not exist, and then generate a new signature into the file at the specified path and data ready to deliver.



```
FUNCTION extractSignature
    GET signatureChain
    DECRYPT signatureChain
    SPLIT signature
    RETURN singature1, signature2
END FUNCTION
```

Fig. 4. Extracting Signature chain

On the other side process, the data recipient will do the opposite process to verify the data, the first process is to extract the signature and then decrypt it to get the original signature data. After the signature is decrypted, the next process is to split each signature using a defined delimiter and then return it as an array of signatures.



```
FUNCTION checkSignature
    GET publicKey from path
    GET q, qp, p, g, w, y from path

    GET messageDigest of data using MD5

    CALL extractSignature

    VALIDATE signature1
    IF signature1 == digest
        RETURN true
    ELSE
        RETURN false;
END FUNCTION
```

Fig. 5. Validating Signature

This is the main function for signature validation, after the function collect the message digest, then the function will extract the signature and validate it using private key if the signature identically with the message digest it will return true as a result. This process will repeat to validate each of the signatures.

IV. RESULTS AND DISCUSSION

The study was conducted by using ElGamal digital signature scheme, and then adding some process after signing the data, before transmitting it over the network.

4.1. Implementation of Digital Signature Chain

This study proposed the digital signature chain using ElGamal signature scheme, with the following steps:

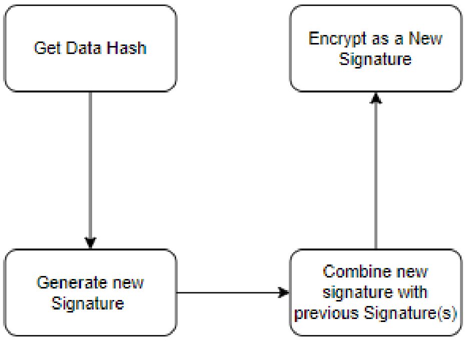

Get Data Hash
Generate new Signature
Combine new signature with previous Signature(s)
Encrypt as a New Signature

Fig. 6. Signature Chain Proses

After generating the public/private key, and then collecting the data hash, the hash then signed the data. After that the new signature will combine with the previously encrypted signature and then encrypt it. The process will remain the same for the next data transmission.

At the recipient, the process will be as follows, first, the signature will decrypt back to get the original signature, then extract to get 2 signatures, and then validate the first signature with the public key. To validate the previous signature the second signature will decrypt back to get a pair of signatures (new signature and previous decrypted signature) the process flow as shown below on figure 7.

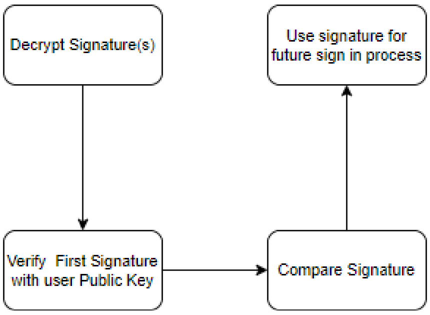

Decrypt Signature(s)
Verify First Signature with user Public Key
Compare Signature
Use signature for future sign in process

Fig. 7. Signature Validation Process

4.2. Analysis of Experiment Results

After doing research and creating a simulation program, as well as conducting several trials, the following results were obtained.

4.2.1. Positive Test Case

The positive test case will be using 3 steps of signature and 4 step verification, the process will start by generating public and private keys, once the key is generated then the file will be signed by the user and then the signature will combine with the previous signature chain and then encrypted using current user public key. Below is the test result:

TABLE I. PUBLIC AND PRIVATE KEY GENERATION

User	**Private Key**	**Public key**			
		q	***P***	***g***	***y***
User_1	187	179	359	136	135
User_2	414339	581743	12798347	5352526	10284232
User_3	130	199	797	412	196

Using the key above, the test file is signed for further storage as a digital signature chain, with the result as follows:

TABLE II. SUCCESSFUL SIGNATURE PROCESS

User	**Signature**		
	s1	***s2***	***Encrypted Chain***
User_1	227513045666800227530559047085985563875	9	Z/on3Fx752NMKGUATbnnBLudZsmaaery8Eg0TxvMLWT/4zXUcpGnHWXm7aqgm+jc
User_2	309653934047846926082640053862585731101	213096	c8b56SrkRADPyqWLO7yDT5v9oUcwaDF4oKHUT1R1ucSVKp67GfygdB5SzHB7O+cI7T0F6C6E59fM NmszaF7JVabZ4S2FlYTyxIoM0D47mdlSFVsQ0huVK9NvjmIjpbS4Jp9gBgc+t7Uhb7d6rwp0ng==
User_3	239584861191002191280975423061868420105	164	XaS/kt9fU0Des8nuSvDtDUKnQttSxvqQDwaRu+P14hMTyvlkyxt4oLa9MaoUMxw1Kwo3mys2NI2H gjv3JFltkwMtswWt9LzvS/ckm/NfB8KKR5FNF5m2A22bttLWYL7psnv2MZVaYX+qcQphsdnu7h1y NgQiBTZgIANA5BeC71I6gbFZakDXdaY+9IXpGbCSywgxt24Z/6Df9faCJvGNinq6bmFpa/ALGIPj k/j4BWDrxVh46M4l2sbaDEaB6Z8roWb73WvH8zpskCVkdMO9NQ==

The signature chain will encrypt and decrypt using AES Encryption by using the public key as a secret key to encrypt and decrypt the signature chain. The signature chain will consist of:

signature1: signature2_previousSignatureChain

Each signature is also verified simultaneously, user_1 signature will be verified by user_2 signature and then user_2 signature will also be verified by user_3 and finally user_4 will verify all signatures in one time process. The previous signature can contain one or more signatures.

The sign and verification process are shown as below:

```
User 1 signing data [TestObject.pdf]

------------------------------------------------------------------------------

Signature 1 :2275130456668002275305590470859855638 75

Signature 2 :9

Previous chain: null

Current Encrypted Chain:

New Chain to encrypt:

22751304566680022753055904708598556387 5:9_

User Public Key (used to encrypt/decrypt) :179359136135

Encrypted New Chain:

Z/on3Fx752NMKGUATbnnBLudZsmaaery8Eg0TxvMLWT/4zXUcpGnHWXm7aqgm+jc

==================================================


User 2 verifying User 1 signature

------------------------------------------------------------------------------

Current Encrypted Chain:

Z/on3Fx752NMKGUATbnnBLudZsmaaery8Eg0TxvMLWT/4zXUcpGnHWXm7aqgm+jc

User Public Key (used to encrypt/decrypt) :179359136135

Decrypted chain:

2275130456668002275305590470859855638 75:9_

Previous Signature 1 :2275130456668002275305590470859855638 75

Previous Signature 2 :9

Previous chain: null

Signature Validation

VALID Signature, using ElGamal Digital signature scheme.

==================================================
User 2 signing data [TestObject.pdf]

----------------------------------------------------------------------

Signature 1 :3096539340478469260826400538625857311O1

…

[intentional chunk]

….

Encrypted New Chain:

c8b56SrkRADPyqWLO7yDT5v9oUcwaDF4oKHUT1R1ucSVKp67GfygdB5SzHB7O+cI7T0F6C6E59fM
NmszaF7JVabZ4S2FlYTyxIoM0D47mdlSFVsQ0huVK9NvjmIjpbS4Jp9gBgc+t7Uhb7d6rwp0ng==

============================================


User 3 verifying User 2 signature

----------------------------------------------------------------------

Current Encrypted Chain:

c8b56SrkRADPyqWLO7yDT5v9oUcwaDF4oKHUT1R1ucSVKp67GfygdB5SzHB7O+…

[intentional chunk]

VALID Signature, using ElGamal Digital signature scheme.

============================================


User 3 verifying User 1 signature

------------------------------------------------------------------------------

User Public Key (used to encrypt/decrypt) :179359136135

[intentional chunk]

VALID Signature, using ElGamal Digital signature scheme.

============================================


User 3 signing data [TestObject.pdf]

----------------------------------------------------------------------

Signature 1 :2395848611910021912809754230618684201O5

Signature 2 :164

[intentional chunk]

============================================
User 4 verifying ALL signature.

----------------------------------------------------------------------

___User 3 signature validation___

Current Encrypted Chain:

XaS/kt9fU0Des8nuSvDtDUKnQttSxvqQDwaRu+P14hMTyvlkyxt4oLa9MaoUMxw1Kwo3mys2NI2Hgjv3JFltkwMtswWt9Lz
vS/ckm/NfB8KKR5FNF5m2A22bttLWYL7psnv2MZVaYX+qcQphsdnu7h1yNgQiBTZgIANA5BeC71I6gbFZakDXdaY+9IX
pGbCSywgxt24Z/6Df9faCJvGNinq6bmFpa/ALGIPjk/j4BWDrxVh46M4l2sbaDEaB6Z8roWb73WvH8zpskCVkdMO9NQ==

User Public Key (used to encrypt/decrypt) :199797412196

Decrypted chain:

2395848611910021912809754230618684201O5:164_c8b56SrkRADPyqWLO7yDT5v9oUcwaDF4oKHUT1R1ucSVKp67Gfyg
dB5SzHB7O+cI7T0F6C6E59fMNmszaF7JVabZ4S2FlYTyxIoM0D47mdlSFVsQ0huVK9NvjmIjpbS4Jp9gBgc+t7Uhb7d6rwp0
ng==

…

[intentional chunk]

….

___User 1 signature validation___

User Public Key (used to encrypt/decrypt) :179359136135

Decrypted chain:

22751304566680022753055904708598556387 5:9_

Previous Signature 1 :227513045666800227530559047085985563875

Previous Signature 2 :9

Previous chain: null

Signature Validation

VALID Signature, using ElGamal Digital signature scheme.

        ================================================
```

4.2.2. Negative Test Case

The negative test case will be using 3 steps of signature and 4-step verification, but after user_2 signed the data, the signature will be changed on purpose, to get the negative result. The public and private keys will use the same key with a positive test case. Below is the test result:

TABLE III. FAILED SIGNATURE PROCESS

User	Signature		
	s1	***s2***	***Encrypted Chain***
User_1	9586923035615014795994832334459904 2072	158	DscMNJJa3jJ2W5P7qj+vqHsbzZn8Ra+KXos+EOhn2j7CC1InX4KHFGssMbQqeQa9
User_2	28503083272229452200987573610 0378479805	188907	SSKwSTip+0AV5PSxlithPDf1j+zeiE3arTE0eSRnuEahnmZ+4nd7dN4mO05yVowNDgHWBI3aA+ba 5Cn8Wo8Uu7FI2s9wdIDmYJ18fOG6FTg93ysSi4cWKOmao/IlCWQiULI1DCq4xkVMd2YRKQY7Fw==
User_3	Failed, caused by javax.crypto.IllegalBlockSizeException:		

4.3. Advantages and Limitations of Digital Signature Chain

Digital signature chains have been applied in various contexts, including mobile applications [13], finance, healthcare, and government but it still needs further research on the application of this technology in many sectors where data security and integrity are of utmost importance. Kim [14] in his paper, proposed a hash chain-based electronic signature model to ensure authentication and integrity of routing and forwarding messages in a sensor network. That's because the public key-based digital signature has some disadvantages: it costs a lot to use, and it takes a long time during the process of generating and verifying digital signatures. Therefore, it is confirmed that this hash chain-based digital signature model is more proper in a sensor network where routing and forwarding messages can frequently happen.

The basic advantage of using digital signatures is that there is a guarantee of the integrity of the data that is transmitted, but with the application of chain digital signatures, there are more advantages, namely that it is easy to track back to find out and ensure the previous data source and to find out how many times the data has been transmitted. Behind the gains, there is a disadvantage with the use of digital signatures, namely that the recipient must have the public key of each signer, which will require extra effort to keep all those public keys.

V. CONCLUSION

From the study conducted, it was found that the use of chain signatures will further improve the security and integrity of the data sent because each signature will also have the previous signature that was encrypted. This automatically improves data security and maintains the integrity of the transmitted data because the signature can be verified by the person who signed it for the first time so that the initial source of the data can be identified. Based on this study, future research may explore the use of a shared public key for multiple signers while still ensuring the ability to identify the individual who signed the data.

REFERENCES

[1] S. Duggineni, "Impact of Controls on Data Integrity and Information Systems," Science and Technology, 2023.

[2] R. &. K. A. Kaur, "Digital signature," In 2012 International Conference on Computing Sciences (pp. 295-301). IEEE, 2012.

[3] M. A. R. &. M.-K. M. Bisheh-Niasar, "Cryptographic accelerators for digital signature based on Ed25519," IEEE, 2021.

[4] A. &. I. A. Saepulrohman, "Data integrity and security of digital signatures on electronic systems using the digital signature algorithm (DSA)," Int. J. Electron. Commun. Syst, 1(1), 11-15., 2021.

[5] M. T. T. A. I. M. K. R. R. L. S. &. K. A. A. Sagar Hossen, "Digital signature authentication using asymmetric key cryptography with different byte number," In Evolutionary Computing and Mobile Sustainable Networks: Proceedings of ICECMSN 2020 (pp. 845-851). Springer Singapore., 2021.

[6] A. A. Aulia Nadzifarin, "Penerapan Elliptic Curve Digital Signature Algorithm pada Tanda Tangan Digital dengan Studi Kasus Dokumen Surat – Menyurat," Journal of Informatics and Computer Science, 2022.

[7] S. Z. J. D. N. H. M. T. U. F. &. Y. M. Ullah, "Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey," Computer Science Review, 47, 100530., 2023.

[8] M. Ms.B.V.SaranyaDevi, "A Robust Digital Signature Scheme for Secure and Efficient Communication for the Internet of Things," Computer Science, 2021.

[9] L. Lamport, "Password authentication with insecure communication," Commun. ACM 24(11), 770–772, 1981.

[10] R. &. D. A. Kundu, "Cryptographic Hash Functions and Attacks-A Detailed Study," International Journal of Advanced Research in Computer Science, 11(2)., 2020.

[11] V. Suma, "Security and privacy mechanism using blockchain," Journal of Ubiquitous Computing and Communication Technologies (UCCT), 1(01), 45-54., 2019.

[12] V. S. H. &. S. M. Bralić, "A blockchain approach to digital archiving: digital signature certification chain preservation," Records Management Journal, 30(3), 345-362., 2020.

[13] A. J. G. B. D. &. M. R. P. Ordonez, "Digital signature with multiple signatories based on modified ElGamal Cryptosystem," In 2018 5th International Conference on Business and Industrial Research, 2018, May.

[14] P. H. N. R. R. G. S. S. V. S. S. R. a. I. B. Y. S. Prakash, "Digital Signatures and El Gamal Scheme Integration for Secure Data Transmission in Digital Transaction Survey," 2022 International Conference on Augmented Intelligence and Sustainable Systems (ICAISS), Trichy, India, 2022.

[15] A. J. G. B. D. &. M. R. P. Ordonez, "Digital signature with multiple signatories based on modified ElGamal Cryptosystem," 5th International Conference on Business and Industrial Research (ICBIR), 2018, May.

[16] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Transactions on Information Theory, vol. 31, pp. 469-472, 1985.

[17] S. Heron, "Advanced encryption standard (AES)," Network Security, 2009(12), 8-12., 2009.

[18] F. P. V. A. F. &. M. J. Miller, "Advanced encryption standard," Alpha Press, 2009.

[19] D. E. Standard, "Data encryption standard," Federal Information Processing Standards Publication, 112., 1999.

[20] N. A. R. E. H. &. S. C. A. Fauziah, "Design and implementation of AES and SHA-256 cryptography for securing multimedia file over android chat application," International Seminar on Research of Information Technology and Intelligent Systems, 2018, November.

[21] Y. S. S. N. &. L. S. H. Kim, "Digital signature model of sensor network using hash chain," The 2nd International Conference on Computer and Automation Engineering (ICCAE), 2010, February.

[22] A. &. K. K. Prasad, "Digital signatures," In Emerging security algorithms and techniques, 2019.

[23] R. A. E.-K. A. N. &. S. B. M. Haraty, "A comparative study of ElGamal based digital signature algorithms," Journal of Computatiofnal Methods in Sciences and Engineering, 2006.

[24] G. Jain, "Digital signature algorithm.," International Journal of Innovations in Computing, 2012.

[25] T. &. M. R. Hidayat, "A Systematic literature review method on aes algorithm for data sharing encryption on cloud computing," International Journal of Artificial Intelligence Research, 2020.