Int. Jrl. of **Computational Learning & Intelligence**
Vol. 02, Issue 02 (April), 2023

LITERATURE / REVIEW ARTICLE

Digital Signatures in Digital Communications: A Review

Naveen Chandra Gowda . Harshith Savanth K . Sagar Shaw . Tharun Deepika M

School of Computer Science and Engineering,
REVA University, Bengaluru, India.

Received: 23 February 2023 / Revised: 11 March 2023 / Accepted: 22 March 2023

Abstract – Nowadays data sharing over the internet is a major and critical issue due to security problems. So more security mechanisms are required to protect the data while sharing through an unsecured channel. Open network transactions of messages be they of any kind demands the digital signature technique. Being one of the most important developments in public key cryptography, the digital signature provides a collection of security patches that help in providing at most authenticity and security. The digital signature is related to the secure Hash function. In this paper, we have reviewed the most recent and efficient Digital signature algorithms in digital communications and summarized the respective gaps.

Index Terms – Digital Signature, Public Key Cryptography, Security Patches, Authenticity, Security and Hash Function

I. INTRODUCTION

Ever since the Internet was made available to users, it's been the major mode of transportation of information. The information that we send can be of any type and might or might not be confidential, if it is confidential then we need to provide it with high security. Security can be applied using many different algorithms and techniques which help in the encryption and decryption of messages which form cryptography. One part of cryptography is the Digital Signature, which is our topic for this paper, a digital signature is an electronic form of a conventional signature that is used to authenticate the document and identify the user. Digital Signature helps in not only assuring the information sent but also assures the genuinely of the sender. The digital signature concept can be better understood using Figure 1. In general, the digital signature algorithm works as given below

Key generation: In this step, the sender generates 2 keys, one being the private key and the other being the public key. The private key is not shared with anyone but, the public key is made available to all the receivers.

Message Hashing: In this step, the message that must be sent is taken and is hashed using the cryptographic hash function which generates a fixed-length message digest.

Generation of the Signature: In this step, the sender generates a digital signature for the got message digest using his private key which was got in step 1.

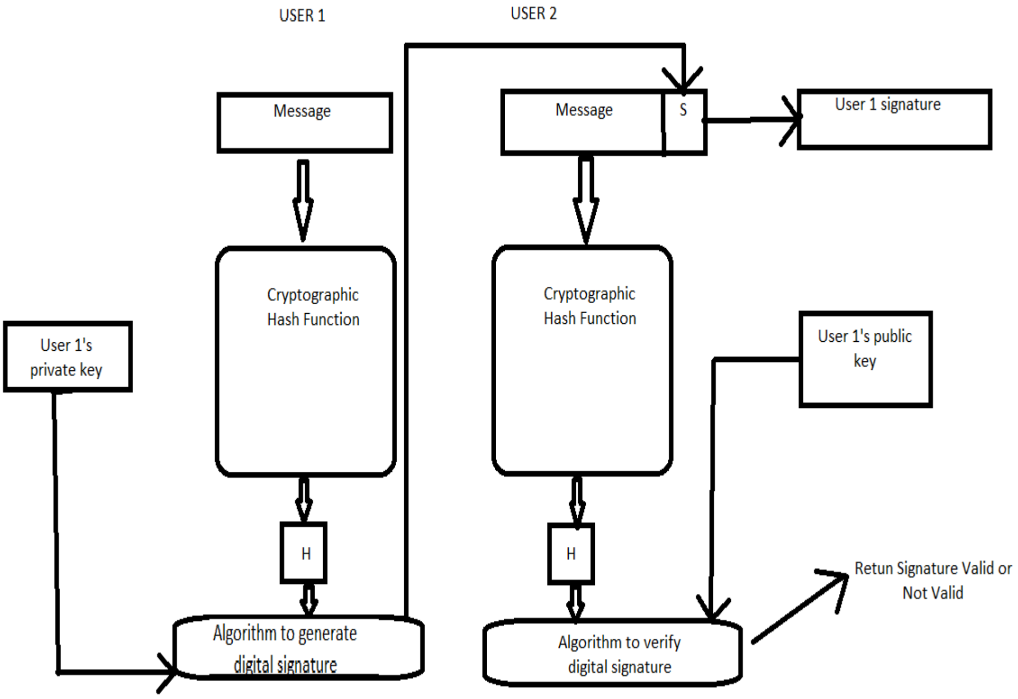
USER 1
USER 2
Message
Message
S
User 1 signature
Cryptographic Hash Function
Cryptographic Hash Function
User 1's private key
User 1's public key
H
H
Retun Signature Valid or Not Valid
Algorithm to generate digital signature
Algorithm to verify digital signature

Fig. 1 – Working of digital signature

Signature verification: In this step, the receiver verifies the messages' authenticity by using the public key of the sender and then decrypts the signature to get back the message digest, then they must hash the original message and check if the result got from the hash of the original message and decrypted message digest are the same. If they are the same, then the signature is valid and the proves that message has not been altered during the process of transportation.

Comparison between conventional and digital signatures

Inclusion: A conventional signature is included in the document. That is, it is part of a document, whereas digital signatures are sent as separate documents.

Verification method: Once the receiver gets the document in the conventional method, they compare the signature on the document with the signature on the file, whereas in digital signature the receiver has to run a set of sets which is explained above to verify the authenticity of the signature.

Relationship: Conventional Signatures usually have a one-to-many relationship, whereas in digital signatures we have a one-to-one relationship.

Duplicity: In a conventional signature, a copy of the signed document can be distinguished from the original one which is on file, whereas in a Digital signature, there is no such distinction unless there is a factor of time on the document.

II. LITERATURE SURVEY

[1] paper proposes a new attribute-based signature scheme based on elliptic curve cryptography (ECC) [30], which according to them has an edge over the existing traditional schemes, this paper then gives a detailed explanation of the underlying principles, the key generation process and the signing and verification processes of their new scheme. This new scheme is more efficient and scalable while keeping the security standards as high as possible. They talk about the traditional signature scheme and how they cannot handle complex access control scenarios especially when the user has different degrees of authorization to access specific resources [31]. They together have reviewed many attribute-based signature schemes namely, the Boneh-Franklin scheme, Lewko-Waters scheme, and the Goyal- Pandey-Sahai scheme. They have made an in-depth analysis of these schemes and got to know their drawbacks, a few of which are their computational costs, lack of scalability, and inability to handle a large number of attributes. The overall review of this paper is that there are a lot of drawbacks to the existing schemes and there is a need to find a new more efficient scheme, one such scheme which is very efficient is discussed in detail.

[2] This paper proposes a new approach that ensures the authenticity and versioning of learning objects using the digital signature infrastructure of Costa Rica and also portraits the uplifting the existing digital signature infrastructure of Costa Rica [32]. This infrastructure is accessible and affordable by most of the users and still ensures protection against attacks. In the literature review of this paper, the author has discussed about many existing approaches to ensuring the authenticity and versioning of learning objects and their limitation, they also go on to talk about how these approaches are not sufficient when advanced attacks are made. They provide a detailed description of their infrastructure, the major leap in this paper is the case study which shows how it can be used to ensure the authenticity and versioning of learning objects in the context of the virtual learning environment. Overall, this paper provides an overview of the existing approach to maintaining authenticity, then goes on to see the flaws of the other methods and writes in detail about a new digital signature infrastructure of Costa Rica using a case.

[3]This paper is written on the digital signature scheme using the self-certified public key, this paper mainly deals with disproving the improved digital signature scheme given by Shao et.al [33]. With the rapid improvement in the internet and computer techniques, one has to be careful about ensuring the integrity and originality of the digital message, this can be achieved using a digital signature. The Digital signature has two major components that are a public key and a private key, the private key should be known only by the sender, and the public key is known by all the receivers. The author then talks about how we need to ensure the authenticity of the public key by using the certificate authority. Tseng et al proposed a way to authorize the public key using a self-certified public key [34]. After this being disproved

by Shao et al attack, they proposed an improved version of the scheme. The author of this paper then analyses the scheme provided by Shao et al and his attack and proved that the attack is very weak, and the improved scheme is vulnerable to middle-in-man attack. Overall, this paper provides detailed proof of their attack which shows that Shao et al attack is not powerful, and the authors also prove that Shao et al scheme is open to very frightful attacks over the internet transaction majorly the middle-man attack.

[4] The paper proposes a digital signature system that uses biometric fingerprint recognition with a fingerprint sensor on a smartphone. The authors aim to develop a secure and convenient method for digitally signing documents, particularly in the context of remote or online transactions. The paper provides a brief overview of digital signatures, biometric fingerprint recognition, and smartphone sensors [35]. It then describes the proposed system's architecture, which consists of a fingerprint sensor, a smartphone app, a server, and a database. The system works by capturing a user's fingerprint and converting it into a digital signature, which is then verified by the server. The paper also discusses the system's security features, including encryption, authentication, and authorization. The authors tested the system's performance and accuracy using a sample dataset of 100 fingerprints. The results showed that the system had an accuracy rate of 95%, and the digital signature generated by the system was accepted by a digital signature verification tool. However, the paper could have benefited from a more comprehensive discussion of the limitations and potential drawbacks of the proposed system, as well as a comparison with other existing digital signature solutions. Overall, the paper presents a valuable contribution to the field of digital signatures and biometric authentication, and it is likely to inspire further research and development in this area.

[5]This paper is written on a new approach to increase and enhance data trustworthiness by using assured digital signing [36]. The authors talk about the importance of digital signing which helps in checking the data integrity and authenticity, they have also compared different digital signing techniques and got out their limitations which tell us about how they are vulnerable to attacks such as key compromise, middleman attack, and relay attack which are all a part of active attack. By seeing all these drawbacks, the authors then propose their new approach to enhancing trustworthiness by using assured digital signing. They talk about how their work is a combination of digital signing and other trusted computing technologies such as Intel SGX which in turn provides us with a higher level of assurance and protection against attacks. They talk about their approach in detail starting from key generation to verification and validation procedures. They then go on to compare their approach with other digital signature approaches and go on to tell how their approach has outperformed to rest in terms of security, scalability, and efficiency. They talk about the need to come up with a technique to enhance trustworthiness, one such approach is spoken in detail in this paper which is very promising and can take this system to greater heights.

[6] The paper highlights the importance of user authentication in digital signatures. The Digital Signature mechanism is completely based on public key cryptography and the Authors have provided an in-depth analysis of the security mechanisms and have also proposed a model[26]. They provide a detailed description of the system architecture, which includes components in the Dsign signature creation process including DsignUI, DSign Controller, DSign Database, and Code-Image Generator. DSign UI takes user inputs for the documents, DSign Controller checks for duplicate records and creates a new record, this

Controller is connected to DSign database using an API call, and a hash key is generated, which is used as input to Code-Image Generator. In the final step, we obtain a QR code and a barcode which are used to verify the authenticity of the user. Dsign process provides various advantages over traditional paper-based signatures including improved security, reduced costs, and improved efficiency.

[7] To enhance Data integrity and security, the Authors have introduced a system that uses a combination of both Digital watermarking and Digital Signature. The system works by embedding a unique digital watermark in the data, which acts as a digital signature. The watermark contains information about the data, such as the author, the date of creation, and the intended recipients. The watermark is then encrypted using a private key, which is only accessible to authorized users[27]. There are very fewer chances of alteration of data because the data is embedded in image form and then it is sent. The system into divided into 3 sections namely, Calculating the hash value using Secure Hash Algorithm (SHA). During the final stage, the integrity is checked where the hash value which is generated is matched with the original hash value. If both matches, then we can conclude that there is no alteration in the image. By using this technique audio, videos, and 3D models can be watermarked.

[8]Researchers have proposed various authentication mechanisms, such as biometrics, one-time passwords, and smart cards. These are prone to replay attacks and physical attacks and Hence Authors have moved towards Two-Factor-Authentication to enhance security. Two-factor authentication is achieved by Biometric identification and OTK (One-Time-Key). OTK is a randomly generated code. Users can sign in if and only if their biometric data is matched with the previously stored data in the database. The generation of signature and its Verification process is done in a cloud platform and hence requires an active internet connection. A public key Algorithm like RSA is used to generate pair of keys and these keys are stored in the central server. The authors used HSM(Hardware Security Module) to the application server to enhance the security level for the private key. Nowadays mobile devices come with fingerprint detectors hence reducing the need for other biometric verification technology. Two-factor authentication is widely used in E-Commerce, E-Government, and E-Health.

[9] Authors have come up with “SCORES” to determine to what extent a document is evaluated as there is no common ways for validation and verification of documents that are digitized. Authors have proposed an IDStack system based on IDStack Technology which is used to verify the document and it also provides the score to the document and a co-relation score to a set of documents. Multiple digital signatures can be verified efficiently. In IDStack protocol partitioned architecture is used. The 3 modules namely: the Data Extraction module, this module creates a document that is in machine-readable format i.e JSON, and it is signed by the extractor. Contents. The digital signature of both the extractor and signers are included in the same JSON document [28].The user may see past digital signatures and add new signatures to the document using the Data Validation module. The module, Relying Party, assesses a document or a collection of papers, rates each one's coherence and signature, and then provides the score.

[10] A generalized digital certificate (GDC) architecture has been suggested by the authors for user authentication and key formation in secure communications. A GDC does not contain the user's public key, but it does contain other information such as the user's public information, such as the information from a digital birth certificate or driver's license, as well as a digital signature of the public

information that was created using the user's private key and verified by a reputable certificate authority (CA). Verifier uses the public key of the CA to validate the data[29]. In GDC, the owner just needs to communicate certain information about the digital signature rather than having to give the verifier access to the digital signature in plain text. The protocol is based on Diffie-Hellman’s assumption and traditional DL-based digital signature.

[11] The paper introduces a novel framework for real-time online signature verification, which employs feature extraction and Gaussian Mixture Model (GMM) classification[19]. The framework is designed to work with digital pens, specifically the Anoto digital pen, which can record handwritten text digitally. The proposed system can be integrated with electronic ID cards to store behavioral biometric data[20]. The framework is evaluated on two datasets, and its performance is tested for both online and offline signature verification. The Anoto pen is synchronized with a computer or mobile device and transmits data to the Anoto Software Development kit (SDK). The signature data is then passed to the signature verification module, which uses a GMM-based approach for processing the signature. The framework is capable of determining whether a claimed identity is genuine or forged based on probability values. The author intends to extend this framework to other areas of interest in the future. Overall, the proposed framework offers a promising solution for real-time online signature verification, which can enhance security and prevent fraudulent activities in various domains.

[12] The paper proposes a solution to prevent cybercrime problems in electronic prescription using digital signature techniques with an RSA 2048-bit algorithm. The Secure Electronic Prescription (SEP) combines confidentiality, authentication, and non-repudiation services using QR-code encryption with NIST standard. The paper discusses protection schemes and verification schemes and performs black box and white box testing for input value tests[16]. E-prescribing is beneficial for accessing patients' previous records, reducing errors of adverse events, and saving prescriber's time and effort[17]. The paper explains the use of RSA algorithm in signature generation and verification and the advantages of QR codes over traditional barcodes. An Android-based system is designed and developed using GUI in android development. The system generates a public key and sends it to the pharmacist for verification, and the prescription is signed by the doctor's private key and sent as a QR code to the pharmacist. The result shows an accurate output in black-box testing and an error density value of less than 12 in white-box testing for a project with less than 16,000 lines of code[18].

[13] The technique described in this paper uses access-controlled high-security verification and digital signatures to safely transfer programmable packets over a network. The suggested technique employs a digital signature algorithm to guarantee packet integrity and authenticity and a high-security verification key with access control to further boost security. The article additionally proposes an architecture with a sender, a receiver, and a secure controller for putting the suggested technique into practice. Using the approach suggested, the sender creates and signs programmable packets before sending them to the recipient. In order to confirm the integrity and validity of the received packets, the secure controller validates the signature using the access-controlled high-security verification key[21]. In the suggested technique, the signing and verifying key pairs almost have the same bit length, and the server that maintains the verification keys also serves as the key management server. This method uses a modified version of the public key digital signature. In a programmable network environment where

intermediate packet-receiving nodes are not set, this study proposes a safe method for sending programmable packets and carrying out calculations utilizing transformed digital signature techniques with message recovery[22]. The system described in this paper's conclusion allows only approved programmable nodes to verify signatures and execute instructions, and it also provides a storage server for verification keys.

[14] The randomly chosen test, the tiny exponent test, and the randomly numbered test are three methods for identifying erroneous signatures in batch verification that are compared and evaluated in this work. When there are numerous signatures in a batch, it is discovered that the random numbering test performs better than the small exponent test. The matrix-detection algorithm is condensed in the study to the term "random numbering approach"[23]. The authors assess the effectiveness of each test at the same level of security, taking into account factors like the presence of 2, 4, 6, or 8 incorrect entries divided into two sets and a possibility of 2–60 for faked signatures to pass each test. Combining a faulty signature from each set results in the creation of a pseudo-valid signature 2-set. For digital signature systems like DSA, elliptic curve digital signature algorithm, RSA, and certificate-less signature scheme, the study emphasizes the value of batch verification[24].

[15] Huang, Lin, and Leu propose the Matrix-Detection Algorithm (MDA) to validate signatures in a batch more accurately than current techniques. MDA is a matrix-based strategy that can identify all bad signatures when there are fewer than four or an odd number of bad signatures. MDA is safer and more efficient than the Small Exponent test (SET)[25]. MDA combines the threshold algorithm and matrix-based strategy to detect disparities between the template and the signature. The algorithm can be enhanced further by incorporating machine learning methods, such as neural networks. The paper makes a significant addition to the field of signature verification with applications in various sectors, including government, legal, and financial. MDA can address the issue of validating a batch of signatures that may contain flawed ones. The signature is regarded as invalid if the disparity is greater than the predetermined threshold. The maximum escape chance pmax of MDA is 5.3 x 10^5 for 1024 signatures with 4 bad signatures, and pmax decreases as the number of digital signatures or bad signatures rises.

III. SUMMARY OF THE SURVEY

Paper reference	Advantages	Disadvantages
[1]	Provides anonymity and un-traceability in the signature process.	1. Lack of implementation and performance evaluation.
[2]	Offers a practical solution for digital signature-based authenticity and versioning of learning objects	Limited discussion on the security analysis of the proposed solution.
[3]	1. Provides a critical review of the proposed digital signature scheme. 2. Highlights the security issues and limitations of the scheme.	Lack of proposed alternative solutions or improvements to the existing scheme.
[4]	Provides a practical solution for digital signature using biometric authentication on a smartphone.	Limited discussion on the security analysis of the proposed solution.

[5]	1. Offers a practical solution for digital signature-based data trustworthiness. 2. Provides tamper-evident and non-repudiation capabilities.	Limited discussion on the performance evaluation of the proposed solution.
[6]	Provides a practical solution for digital signature-based paperless operation.	Limited discussion on the performance evaluation of the proposed solution
[7]	Offers a combined solution of digital signature and watermarking for enhanced security and integrity of data.	1. Limited discussion on the security analysis of the proposed solution. 2. Lack of performance evaluation in terms of scalability and efficiency.
[8]	Provides an additional layer of security through 2-factor authentication.	May require additional hardware or software to implement 2-factor authentication, which could be costly or difficult to implement.
[9]	Offers a common protocol for document verification, which could improve interoperability between systems.	May not be widely adopted, which could limit its usefulness.
[10]	Provides a generalized digital certificate that could be used for various applications, which could save time and resources.	May not be compatible with all systems or protocols, which could limit its usefulness.
[11]	Provides a framework for verifying digital signatures in digital pen applications.	Limited to digital pen applications, which may not be useful in other contexts.
[12]	Enables the implementation of digital signature for secure electronic prescriptions using QR-code and Android smartphone.	Limited to electronic prescription applications and may require a specific smartphone model or software.
[13]	Provides a method for securely transferring programmable packets using digital signatures.	Limited to programmable packet applications, which may not be useful in other contexts.
[14]	Provides a performance analysis of batch verification methods for digital signatures, which could help inform system design.	Limited to batch verification methods and may not be useful for other types of digital signature applications.
[15]	Provides a method for verifying batches of bad signatures using a matrix-detection algorithm.	Limited to batches of bad signatures and may not be useful for other types of digital signature applications.

Gaps in the literature survey

The gaps that are listed below should be referred to as a few of many gaps which are derived from our literature review,

- Lack of comprehensive literature review on the state-of-the-art digital signature schemes, their strengths, and weaknesses.
- Limited analysis of the impact of different parameters on the performance and security of digital signature schemes, such as key sizes, hash functions, and elliptic curves.
- Limited research on the applicability of digital signature schemes in different scenarios, such as IoT, blockchain, and cloud computing.
- Limited focus on the usability and adoption of digital signature schemes, including user acceptance and integration with existing systems.
- Limited research on the legal and regulatory issues surrounding digital signatures, including their admissibility in courts and compliance with international standards.
- Limited analysis of the impact of quantum computing on the security of digital signature schemes and the need for post-quantum digital signature schemes.

IV. CONCLUSION

This paper is an attempt to understand the digital signature concept, how it works, and its major advantages and disadvantages over the conventional signature method. Then we had a look into the different digital signature algorithms that have come out recently and also a few standard approaches and did a literature review on the same, each paper's summary was jotted down for our convenience. This paper also makes a strike on showing the evolution of the Digital signature concept over time.

REFERENCES

1. Ma, R., & Du, L. (2022). Efficient Pairing-Free Attribute-Based Blind Signature Scheme Based on Ordered Binary Decision Diagram. IEEE Access, 10, 114393-114401.
2. Alpizar-Chacon, I., & Chacon-Rivas, M. (2016, October). Authenticity and versioning of learning objects using the digital signature infrastructure of Costa Rica. In 2016 XI Latin American Conference on Learning Objects and Technology (LACLO) (pp. 1-6). IEEE.
3. Jianhong, Z., Hua, C., Shengnan, G., & Qin, G. (2009, May). Comment on a digital signature scheme with using self-certified public keys. In 2009 International Forum on Information Technology and Applications (Vol. 3, pp. 678-680). IEEE.
4. Rahmawati, E., Listyasari, M., Aziz, A. S., Sukaridhoto, S., Damastuti, F. A., Bachtiar, M. M., & Sudarsono, A. (2017, September). Digital signature on file using biometric fingerprint with fingerprint sensor on smartphone. In 2017 International Electronics Symposium on Engineering Technology and Applications (IES-ETA) (pp. 234-238). IEEE.
5. Dai, W., Parker, T. P., Jin, H., & Xu, S. (2012). Enhancing data trustworthiness via assured digital signing. IEEE Transactions on Dependable and Secure Computing, 9(6), 838-851.
6. Saha, G. (2017, April). Dsign digital signature system for paperless operation. In 2017 International Conference on Communication and Signal Processing (ICCSP) (pp. 0324-0328). IEEE.
7. Shukla, S. S. P., Singh, S. P., Shah, K., & Kumar, A. (2012, March). Enhancing security & integrity of data using watermarking & digital signature. In 2012 1st International Conference on Recent Advances in Information Technology (RAIT) (pp. 28-32). IEEE.
8. Chakraborty, N. R., Rahman, M. T., Rahman, M. E., & Uddin, M. S. (2016, December). Generation and verification of digital signature with two factor authentication. In 2016 International Workshop on Computational Intelligence (IWCI) (pp. 131-135). IEEE.
9. Lakmal, C., Dangalla, S., Herath, C., Wickramarathna, C., Dias, G., & Fernando, S. (2017, September). IDStack—the common protocol for document verification built on digital signatures. In 2017 National Information Technology Conference (NITC) (pp. 96-99). IEEE.
10. Harn, L., & Ren, J. (2011). Generalized digital certificate for user authentication and key establishment for secure communications. IEEE Transactions on Wireless Communications, 10(7), 2372-2379.
11. Malik, M. I., Ahmed, S., Dengel, A., & Liwicki, M. (2012, March). A signature verification framework for digital pen applications. In 2012 10th IAPR International Workshop on Document Analysis Systems (pp. 419-423). IEEE.
12. Sadikin, M. A., & Sunaringtyas, S. U. (2016, August). Implementing digital signature for the secure electronic prescription using QR-code based on android smartphone. In 2016 International Seminar on Application for Technology of Information and Communication (ISemantic) (pp. 306-311). IEEE.
13. Kim, Y., Han, J., Seo, D., & Sohn, S. (2005). U.S. Patent Application No. 10/836,928.
14. Guan, D. J., Zhuang, E. S., Chung, I. C., & Lin, Y. S. (2017, August). Performance analysis of some batch verification methods of digital signatures. In 2017 12th Asia Joint Conference on Information Security (AsiaJCIS) (pp. 10-14). IEEE.
15. Huang, Y. L., Lin, C. H., & Leu, F. Y. (2011, June). Verification of a batch of bad signatures by using the matrix-detection algorithm. In 2011 First International Conference on Data Compression, Communications and Processing (pp. 299-306). IEEE.
16. Wahono, R. S. (2003). Analyzing requirements engineering problems. In IECI Japan Workshop (Vol. 2003).

17. Sadikin, M. A., & Sunaringtyas, S. U. (2016, August). Implementing digital signature for the secure electronic prescription using QR-code based on android smartphone. In 2016 International Seminar on Application for Technology of Information and Communication (ISemantic) (pp. 306-311). IEEE.
18. McConnell, S. (2006). Software estimation: demystifying the black art. Microsoft press.
19. Mariéthoz, J., & Bengio, S. (2002). A comparative study of adaptation methods for speaker verification. In International Conference on Spoken Language Processing ICSLP (No. CONF, pp. 581-584).
20. Gonzalez-Rodriguez, J., Fierrez-Aguilar, J., Ramos-Castro, D., & Ortega-Garcia, J. (2005). Bayesian analysis of fingerprint, face and signature evidences with automatic biometric systems. Forensic science international, 155(2-3), 126-140.
21. Sander, T., & Tschudin, C. F. (1998, May). Towards mobile cryptography. In Proceedings. 1998 IEEE Symposium on Security and Privacy (Cat. No. 98CB36186) (pp. 215-224). IEEE.
22. Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (2018). Handbook of applied cryptography. CRC press.
23. Huang, Y. L., Lin, C. H., & Leu, F. Y. (2011, June). Verification of a batch of bad signatures by using the matrix-detection algorithm. In 2011 First International Conference on Data Compression, Communications and Processing (pp. 299-306). IEEE.
24. Naccache, D., M'RaÏhi, D., Vaudenay, S., & Raphaeli, D. (1995). Can DSA be improved?—Complexity trade-offs with the digital signature standard—. In Advances in Cryptology—EUROCRYPT'94: Workshop on the Theory and Application of Cryptographic Techniques Perugia, Italy, May 9–12, 1994 Proceedings 13 (pp. 77-85). Springer Berlin Heidelberg.
25. Bellare, M., Garay, J. A., & Rabin, T. (1998). Fast batch verification for modular exponentiation and digital signatures. In Advances in Cryptology—EUROCRYPT'98: International Conference on the Theory and Application of Cryptographic Techniques Espoo, Finland, May 31–June 4, 1998 Proceedings 17 (pp. 236-250). Springer Berlin Heidelberg.
26. Melgar, M. E. V., Farias, M. C., de Barros Vidal, F., & Zaghetto, A. (2016, October). A high density colored 2D-barcode: CQR Code-9. In 2016 29th SIBGRAPI Conference on Graphics, Patterns and Images (SIBGRAPI) (pp. 329-334). IEEE.
27. Dittmann, J., Steinmetz, A., & Steinmetz, R. (1999, June). Content-based digital signature for motion pictures authentication and content-fragile watermarking. In Proceedings IEEE International Conference on Multimedia Computing and Systems (Vol. 2, pp. 209-213). IEEE.
28. Ahmed, S. T., Singh, D. K., Basha, S. M., Abouel Nasr, E., Kamrani, A. K., & Aboudaif, M. K. (2021). Neural network based mental depression identification and sentiments classification technique from speech signals: A COVID-19 Focused Pandemic Study. Frontiers in public health, 9, 781827.
29. Lakmal, C., Dangalla, S., Herath, C., Wickramarathna, C., Dias, G., & Fernando, S. (2017, September). IDStack—the common protocol for document verification built on digital signatures. In 2017 National Information Technology Conference (NITC) (pp. 96-99). IEEE.
30. Harn, L., Ren, J., & Lin, C. (2009). Design of DL-based certificateless digital signatures. Journal of Systems and Software, 82(5), 789-793.
31. Tsaur, W. J., Tsao, J. H., & Tsao, Y. H. (2018). An efficient and secure ECC-based partially blind signature scheme with multiple banks issuing E-cash payment applications. In Proceedings of the International Conference on e-Learning, e-Business, Enterprise Information Systems, and e-Government (EEE) (pp. 94-100). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).
32. Ahmed, S. T., Basha, S. M., Ramachandran, M., Daneshmand, M., & Gandomi, A. H. (2023). An Edge-AI enabled Autonomous Connected Ambulance Route Resource Recommendation Protocol (ACA-R3) for eHealth in Smart Cities. IEEE Internet of Things Journal.
33. Okamoto, T. (2001, May). Provably secure and practical identification schemes and corresponding signature schemes. In Advances in Cryptology—CRYPTO'92: 12th Annual International Cryptology Conference Santa Barbara, California, USA August 16–20, 1992 Proceedings (pp. 31-53). Berlin, Heidelberg: Springer Berlin Heidelberg.
34. Legislativa, A. (2005). Ley de certificados, firmas digitales y documentos electrónicos.
35. Shao, Z. (2004). Improvement of digital signature with message recovery using self-certified public keys and its variants. Applied mathematics and computation, 159(2), 391-399.

36. Tseng, Y. M., Jan, J. K., & Chien, H. Y. (2003). Digital signature with message recovery using self-certified public keys and its variants. Applied Mathematics and Computation, 136(2-3), 203-214.
37. Raja, D. K., Kumar, G. H., Basha, S. M., & Ahmed, S. T. (2022). Recommendations based on integrated matrix time decomposition and clustering optimization. International Journal of Performability Engineering, 18(4), 298.
38. Mudholkar, S. S., Shende, P. M., & Sarode, M. V. (2012). Biometrics authentication technique for intrusion detection systems using fingerprint recognition. International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), 2(1), 57-65.
39. Goldwasser, S., Micali, S., & Rivest, R. L. (1988). A digital signature scheme secure against adaptive chosen-message attacks. SIAM Journal on computing, 17(2), 281-308.