Strengthening Digital Signature Schemes using Advanced Elliptic Curve Cryptography in Blockchain Technology

M Shanmugam Shoba[1*], Rekha B Venkatapur[2]

[1,2] Department of Computer Science and Engineering, K S Institute of Technology, Bangalore, Karnataka, Affiliated to VTU, Belagavi, Visvesvaraya Technological University, Belgavi-590018.

Abstract: Digital signature is important in ensuring authenticity, integrity, confidentiality of data. For providing security, digital authentication methods become more essential in IT security, blockchain technology is providing high security and has attracted significant attention in various fields. The key features pf Blockchain like decentralized ledger, transparency, immutability etc makes it a most popular and appealing with respect to data confidentiality and integrity. The existing digital signature schemes are explored, and their limitations and vulnerabilities are identified. The new enhanced digital signature mechanism using AECC-Advanced Elliptic Curve Cryptography is proposed. The integration of AECC aims to strengthen crucial security aspect such as decentralized trust, transparency and protection against tampering.

Keywords: Digital Signature Schemes; Security Enhancement; Authentication; Integrity; Immutable Ledger; Advanced Elliptical Curve Cryptography.

Introduction

In today's businesses worldwide internet has become most essential, enabling trade, purchasing, and interconnecting applications, which has driven global economic integration. However, this connectivity also introduces significant risks—attacks on critical assets can cause severe disruptions and require substantial time to recover. Traditional security systems employ privacy, authentication, and safety measures, but evolving fear of security has become more sophisticated and harder to mitigate. Conventional approaches, being centralized, suffer from limitations such as single points of failure, high costs, and lack of trust. A successful system-wide attack or unauthorized access can cripple operations, impacting both performance and efficiency. Moreover, constant maintenance is required to keep pace with emerging threats.

The decentralized, peer-to-peer network and other features of blockchain addresses these issues where transactions are securely recorded across multiple nodes. Blockchain distributes data, reducing vulnerability to attacks like denial-of-service and enhancing resilience, transparency, and trust.

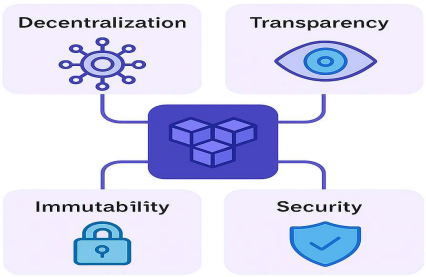


Fig. 1. Properties of blockchain

A denial-of-service (DoS) attack occurs when excessive requests are sent to a system, overwhelming its capacity. In the context of blockchain, such an attack floods the network with fake transaction requests. Since blocks are generated at fixed intervals and have limited size, this overload can exceed storage capacity and make the service unavailable to legitimate users.

Blockchain, originally the core of Bitcoin, is been adopted by various other sectors. It offers a decentralized structure and maintains an immutable, time-ordered record of data. This makes it suitable for applications requiring digital proof, such as IoT, stock trading, electronic payments, and supply chain management. Beyond cryptocurrency, blockchain supports advancements in banking, commerce, and smart contracts. Digital signatures, often integrated with blockchain, are used to integrity of the data and to verify the authenticity.

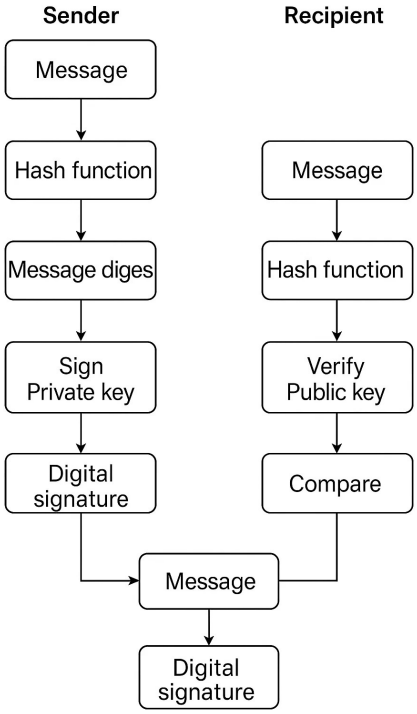


Fig. 2. Digital signature process based on RSA

Problem Statement

Electronic signatures play a vital role in modern digital transactions, especially in electronic commerce, making their security a critical concern. However, traditional methods remain vulnerable to threats such as counterfeiting, tampering, and unauthorized alterations.

This study focuses on evaluating and enhancing the security of digital signature schemes by leveraging hash-based blockchain technology. By integrating blockchain's decentralized and immutable nature, the aim is to reinforce digital signatures against manipulation while ensuring transparency and trust in transactions. The research seeks to validate the proposed approach's effectiveness and robustness in maintaining the reliability and integrity of digitally signed documents in today's digital landscape.

Motivation

1. **Increasing Reliance:** With the rapid rise of online transactions, the need for secure electronic signature methods to ensure the authenticity and accuracy of digital records is more critical than ever.
2. **Existing Security Risks:** Traditional electronic signature systems face vulnerabilities such as forgery, tampering, and unauthorized modifications, which undermine their reliability.
3. **Risk Reduction through Blockchain:** Integrating electronic signature mechanisms with hash-based blockchain technology helps mitigate these risks by ensuring transparency, immutability, and enhanced security.
4. **Real-World Significance:** Strengthening the integrity of digital signatures fosters trust and confidence in electronic commerce across key sectors, including legal, financial, and healthcare industries.

Related Works

Blockchain technology combines encryption with mechanisms that ensure traceability, integrity, and non-repudiation, transforming modern industries and businesses. Most blockchain systems and cryptocurrencies rely on the Elliptic Curve Digital Signature Algorithm - ECDSA, commonly using the secp256k1 curve. This curve is uniquely structured for efficiency, though ECDSA has vulnerabilities, particularly when random numbers are not securely generated, leading to potential key exposure.

In blockchain, each block stores data, its own digital signature, and the hash of the previous block, ensuring immutability and linking blocks securely. This design prevents tampering and eliminates the need for centralized authority, providing transparency, legal clarity, and enhanced trust in digital transactions.

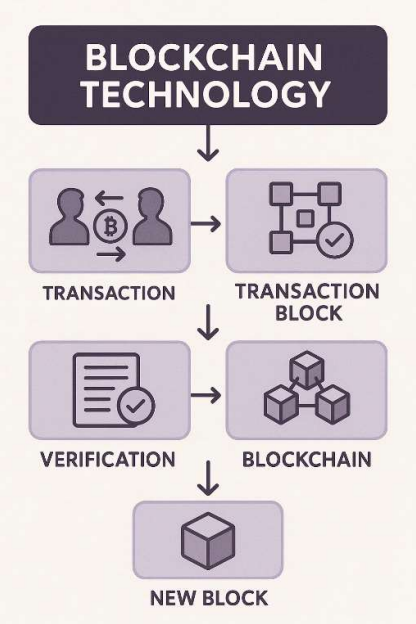


Fig. 3. Process structure of Blockchain Technology

Research Gap

1. **Limited Integration:** While blockchain enhances the security of digital signature systems, research on integrating hash-based blockchain mechanisms tailored to the specific security requirements of electronic signatures remains limited.
2. **Implementation Challenges:** Even though there exist models for merging blockchain with electronic signatures, practical challenges—such as regulatory compliance, scalability, and interoperability—have not been thoroughly addressed.
3. **Performance Evaluation:** Comprehensive performance assessments are necessary to gauge the feasibility and sustainability of blockchain-based digital signature systems. Key metrics should include throughput, latency, and resource consumption.
4. **User Adoption and Usability:** Research on user perceptions, adoption barriers, and usability considerations is scarce, but this features are crucial for ensuring successful implementation and widespread use.
5. To fully leverage the potential of blockchain-integrated digital signature solutions in enhancing the reliability and trustworthiness of electronic transactions across diverse sectors, these research gaps must be addressed.

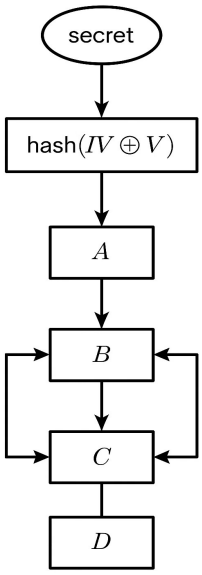
3 Proposed System

The proposed system represents a significant advancement in cybersecurity by enhancing the security of digital signature schemes through the integration of Advanced Elliptic Curve Cryptography (AECC). Its primary objective is to improve the integrity and trustworthiness of digital signatures by leveraging the inherent security features of blockchain technology.

This approach addresses key weaknesses in traditional signature generation by incorporating hash-based mechanisms. A core component of the system is a comprehensive analysis of existing digital signature methods to identify potential vulnerabilities. By integrating AECC, the system provides an added layer of protection against fraud, tampering, and unauthorized alterations.

Another essential aspect of the design is practical implementation guidance. The solution facilitates smooth adoption by providing detailed strategies by integrating the features of blockchain technology into current electronic signature infrastructures. Additionally, performance evaluation is included to ensure efficiency and scalability, addressing concerns related to processing overhead and resource utilization.

To promote user adoption, the system emphasizes usability by incorporating user feedback and offering intuitive interfaces. The overall architecture of the proposed authentication framework is illustrated in Fig. 4.



Authentication and block transmissi-

Fig. 4. Authentication and block transmission structure in the CBcA method

3.1 Advanced Elliptic Curve Cryptography

With the advent of digital communication technologies, traditional physical methods of securing information, such as locks and manual signatures, have become obsolete. However, ensuring secure data transactions remains critical, now achieved through encryption and digital signatures in electronic documents.

The ElGamal signature scheme, an early approach to digital authentication, required excessively large key sizes—around 2,000 bits—to provide minimal security, which limited its efficiency. Modern electronic authentication builds upon the principles of Public Key Cryptography, relying on the computational complexity of integer factorization and discrete logarithm problems.

Elliptic Curve Cryptography (ECC) emerged as a preferred alternative due to its ability to enhance the security using a smaller key size, making it ideal for resource-constrained environments. For example, according to IEEE-1363 standards, a 172-bit ECC key offers security comparable to a 1024-bit RSA key. ECC's strength lies in the difficulty of solving discrete logarithm problems.

AECC represents a refined subset of ECC, incorporating more sophisticated features such as larger key sizes and optimized curve structures. These enhancements provide stronger resistance against brute-force and discrete logarithm-based attacks while maintaining computational efficiency. AECC aims to deliver higher levels of security without compromising performance, making it a robust choice for modern cryptographic applications.

The following are a few AECC characteristics and methods:

- Bigger Key Sizes: By making the discrete logarithm issue more computationally hard to solve, larger elliptic curve parameters—like the prime factor or the base point's order—can improve safety against brute-force assaults.
- Particular Curve Structures: Relative to conventional Weierstrass curves, some curve structures, such as twisted Edwards's curves or Montgomery curves, provide benefits in terms of speed and safety. These curves could be resistant to particular kinds of assaults or tailored for particular cryptographic processes.
- Pairing-Based Cryptography: To employ cryptographic basics like identity-based encrypting attribute-based encrypting and cryptography combinations, sophisticated ECC algorithms may also make use of pairing-friendly elliptic curves. Improved features of pairing-based cryptography are available for use in a range of cryptographic situations.
- Post-Quantum ECC: Since the emergence of quantum computing, efforts are underway to develop quantum-resistant encryption methods, particularly for Elliptic Curve Cryptography (ECC).The study of novel elliptic curve designs and techniques that uses cryptography to resist any kind of assaults by quantum computers is known as post-quantum ECC.

All things considered, sophisticated ECC methods are essential to contemporary cryptography since they improve safety and effectiveness for a variety of cryptographic uses, such as key exchange procedures, electronic signatures, and encryption.

In the elliptic curve ,each point is a double of the generating point G, that's the point generated by fulfilling the Weierstrass solution for a specific elliptic curve. The essential process in ECC is point multiplying. The quantity

of scientific research required to determine the value "k" that satisfies the equation Q = kP when Q and P are known may be described as the issue of discrete logarithm, if "P" is a point on an elliptic curve over Fp and "k" is an integer within the order of Fp. Even with both other values provided, obtaining 'k' becomes computationally impossible if 'k' is a greater value. In public key techniques like ECC, mutual coordination between communication entities over a set of constants known as domain variables is one of the requirements.

• a,b: 'a' and 'b' are known as elliptic curve variables that describe the elliptic curve. These are the set of domain variables specified for a certain elliptic curve.

• q: The parameter q determines the prime field's size.

• G(x,y): An elliptic curve's generator point, or G(x,y), is where all other points on the curve may be obtained.

• n: The value of 'n' represents the order of base point G or the total amount of components in the elliptic curve.

Since point additions and point doubles are the fundamental blocks of point addition, their successful execution of them is significantly affected by these field manipulations.

The two points are represented as A(i_1, i_1) and B(i_2, i_2), then ECC operation known as point addition results in another point C(i_3, i_3) , C = A + B calculated as:

$$i_3 = m^2 - i_1 - i_2$$

$$j_3 = m(i_1 - i_3) - j_1$$

Where $m = \frac{j_2 - j_1}{i_2 - i_1}$ is the slope of the line between A and B. Addition of same points A(i_1, i_1) to itself results in C(i_3, i_3) on the curve through another group operation called point doubling where C = A + A = 2A is computed as follows:

$$i_3 = m^2 - 2i_1$$

$$j_3 = m(i_1 - i_3) - j_1$$

Where $m = \frac{3i_1^2 + a}{2j_1}$

4 Results and Discussions

The Integrated Encryption Scheme in Elliptic Curve (ECIES) is a amalgam of cryptographic method that combines the efficiency of symmetric encryption with the security of asymmetric elliptic curve cryptography (ECC). It encrypts data using a private key and decrypts it with the corresponding public key, ensuring secure key exchange, authentication, and data protection. ECIES is widely used in cloud and mobile environments because ECC gives high security with less key size such as 256-bit ECC offering security comparable to 3072-bit RSA—resulting in lower bandwidth usage and faster computation. The scheme operates on an elliptic curve defined by the equation y2=x3+ax+by^2 = x^3 + ax + by2=x3+ax+b, where a base point GGG generates public-private key pairs through Q=kGQ = kGQ=kG, making the reverse computation of the private key computationally infeasible. By leveraging discrete logarithm problem, ECIES ensures high security for applications like blockchain, SDN, and secure communication, while delivering efficiency and scalability.

ECIES algorithm key generation method Sender generates a random private key (RP_AP_A) and the takes a point on an elliptic curve (G) and then determines sender public key (PK_A):

$$PK_A = RP_A \times G \; \& PK_A = P_A \times G$$

Gand PKA are thus points on an elliptic curve. Sender then sends PKA to receiver. Next receiver will generate: R = r× G, S = r × PK_A and where r is a random number generated by receiver. The symmetric key (S) is then used to encrypt a message. Sender will then receive the encrypted message along with R and sender will be able to determine the same encryption key with:

$$S = RP_A \times R$$

Similar as the key that receiver also generated secret key consists of 100 - mobile nodes of the IOT devices.

$$S = RP_A \times (r \times G)$$

$$S = r \times (RP_A \times G)$$

$$S = r \times PK_A$$

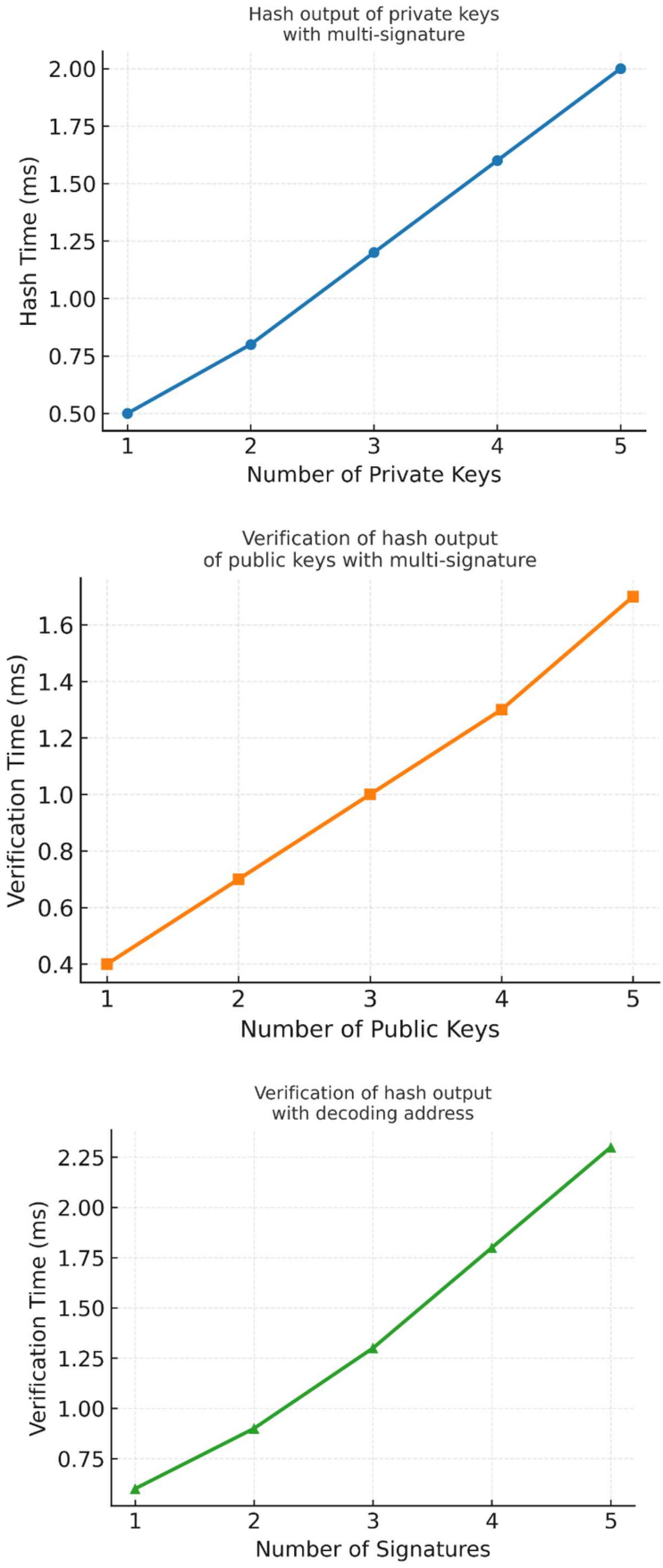


Fig. 5. (a) Private keys with multi signature hash output (b) Public keys with multi signature-verification of hash output (c) Multi signature with decoding address generate results graph- Verification of hash output

ADR: The amount that is determined by dividing the total number of incursions by the number of accurately identified intrusions [21]. Equation (3) establishes the ADR.

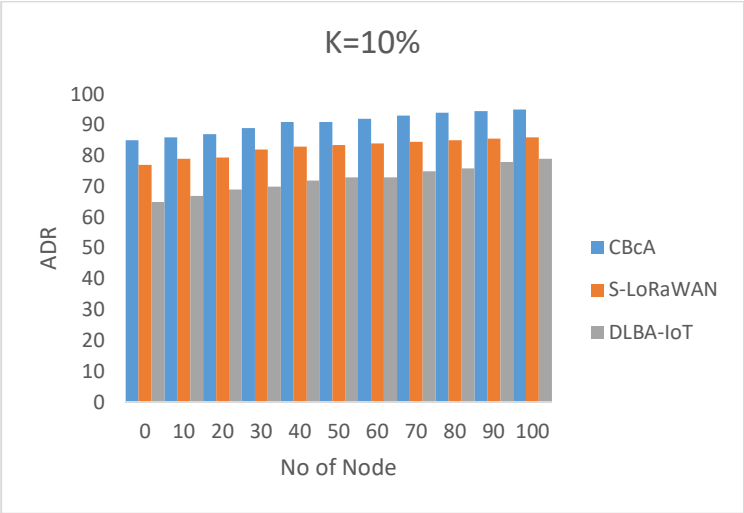
$$AFP = \left(\frac{AFP}{AFP + ATN}\right) ATP = \left(\frac{ATP}{ATP + AFN}\right)$$

$$AFN = \left(\frac{ATP + ATN}{All}\right) ATN = \left(\frac{ATN}{ATN + AFP}\right)$$

$$AT = \left(\left(\frac{1}{Ex}\right) * \left(\frac{\sum_{x=1}^{n} A_x * E_s}{D_p - D_T}\right) * \left(\frac{8}{100}\right)\right)$$

The produced output password for a private key and messages with multiple signatures for various hash methods is displayed in Fig. 5, along with the output hash confirmation for public keys with multiple signatures and the output hash verification for multiple signatures with the decoding addresses. The message keys and secret keys can be multiplied separately for getting hashing bytes as shown in Fig. 5a. The tiny hash result produced by SHA 224 and SHA 256 is 32 bytes. Therefore, an attacker may quickly identify the keys. The hash value generated by SHA 384 and SHA 512 is 56 bytes. The hash result of the message digest method is 64 bytes, which is comparable to SHA3-224. SHA3-256 and SHA3-384 generate a hash result of 96 bytes when used with a multi-signature secret key. The hash result from the elliptic curve encryption method with SHA3-512 is 128 bytes. However, it only takes input keys of up to 256 bytes. Up to 128 bytes of input key are produced as hash output by these cryptographic hash routines. Up to 512 bytes of input key are generated as hash output by the MECC-MSS method. In the confirmation step, Fig. 5b displays the examination of multiple signatures using a public key. The bytes of the public key can be divided by the hash of the private key. The hash output of the private key is altered if an attacker attempts to decipher it. By filtering attack bytes, weaknesses can be exploited to retrieve private keys. Verification of the multi-signature with the decoder address is shown in Fig. 5c. Following validation during the testing stage, the sent bytes are converted into various addresses. To verify that the address is genuine, the message bytes and encrypted addresses are extracted in this step. Even in the case of many transactions, the production and validation of signatures yield an identical hash value.

The proposed work is superior to DLBA-IoT and SLoRa WAN methods for two reasons: first, it registers every device in the IoT network, preventing devices without registration numbers from engaging in transmitting data operations; second, it assesses each block and authorizes it all, preventing malicious operations by outside parties. The suggested approach examined the mean amount of time it took for blockchain-based Internet of Things devices to connect over a range of time intervals (e.g., 5, 10, 15, and 20 s). The findings are displayed in figure below.



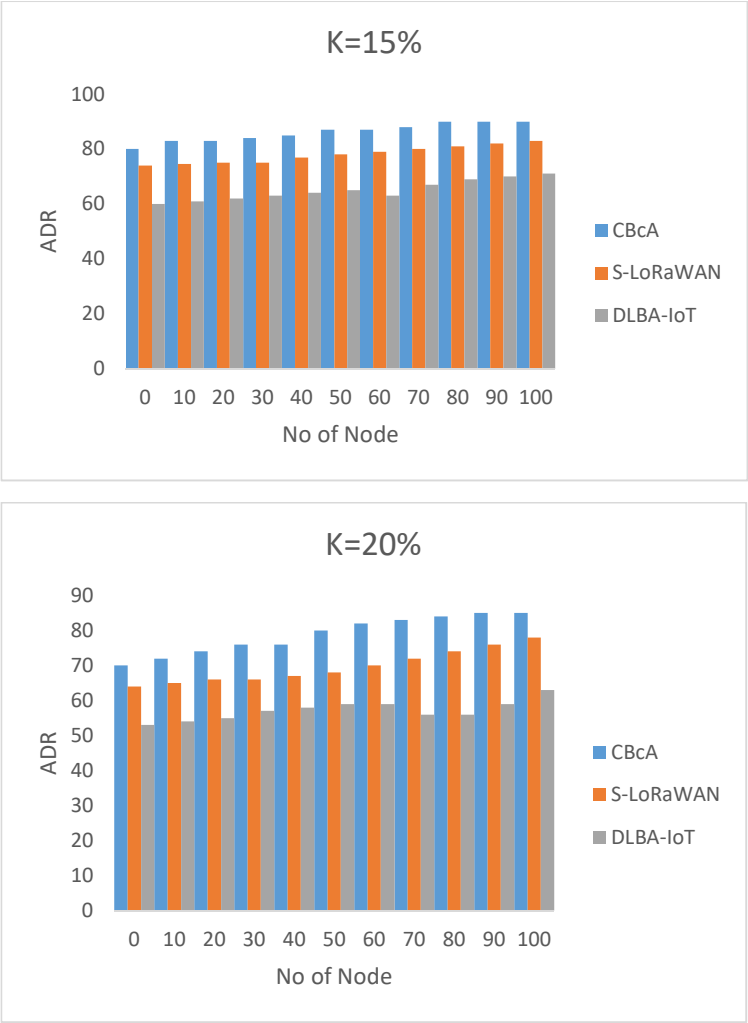


Fig. 6. ADR of the suggested CBcA model and other models in intruder identification

Conclusions

The proposed work focuses on enhancing non-repudiation and integrity of data in blockchain through improved digital signature mechanisms. By analyzing existing signature schemes, it highlights how advanced elliptic curve cryptography (ECC) can enhance the security against emerging threats. Advanced ECC, with larger key sizes and optimized curve structures, significantly improves the resilience and efficiency of digital signatures, ensuring transaction validity and integrity. The integration of blockchain adds decentralization and immutability, reducing risks of fraud and manipulation while increasing transparency. Practical implementation insights and performance evaluations demonstrate the feasibility and adaptability of the proposed approach in real-world environments. Overall, combining hash-based blockchain with advanced ECC represents a major step toward secure, reliable, and trustworthy online transactions in today's connected digital landscape.

Future directions

Future research on blockchain-integrated digital signature systems should address several key areas. Quantum-resistant cryptography is essential to counter the threat of quantum computing, requiring integration with advanced ECC and blockchain. Scalability and efficiency improvements through optimized consensus protocols can enhance performance, while interoperability and standardization will ensure compatibility across diverse systems. Enhancing privacy via zero-knowledge proofs and similar techniques, along with improving usability and user experience, will drive wider adoption. Additionally, compliance with legal and regulatory frameworks is crucial for global acceptance. Finally, exploring real-world applications in sectors such as finance, healthcare, law, and supply chains will validate practicality. Advancing these areas will strengthen digital authentication and ensure secure, trustworthy transactions in a digital-first era.

References

[1] B. Alex and K. Selvan, "Developing a Security Enhancement for Healthcare Applications Using Blockchain-Based Firefly-Optimized Elliptic Curve Digital Signature Algorithm," *Research Square*, 2024.

[2] W. El Sobky and S. Hamdy, "Elliptic Curve Digital Signature Algorithm: Challenges and Development Stages," *Journal of Innovative Technology*, 2021.

[3] S. Kavitha, J. Srinivasan, and P. Ramachandran, "Enhanced Cryptographic Performance and Security Using Optimized Edward-ElGamal Signature Scheme for IoT and Blockchain Applications," *Int. J. Smart Sensing and Intelligent Systems*, vol. 17, no. 4, 2024.

[4] D. Johnson, A. Menezes, and S. Vanstone, "The Elliptic Curve Digital Signature Algorithm," Certicom Whitepaper, 1999.

[5] G. Jayabalasamy and S. Koppu, "High-Performance Edwards Curve Aggregate Signature (HECAS) for Nonrepudiation in IoT-Based Blockchain Ecosystem," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 9, pp. 6294–6304, 2022.

[6] M. Y. Alshahrani, "Implementation of a Blockchain System Using Improved Elliptic Curve Cryptography Algorithm for E-Learning Performance Assessment," *Appl. Sci.*, vol. 12, no. 1, p. 74, 2021.

[7] G. Uganya and R. Baskar, "Modified Elliptic Curve Cryptography Multi-Signature Scheme to Enhance Security in Cryptocurrency," *Computer Systems Science & Engineering*, vol. 45, no. 2, pp. 183–196, 2023.

[8] G. Shankar and L. H. Ai-Farhani, "Improved Multisignature Scheme for Authenticity of Digital Document in Digital Forensics Using Edward-Curve Digital Signature Algorithm," *Security and Privacy Journal*, 2023.

[9] S. Kazmirchuk, A. Ilyenko, and S. Ilyenko, "The Improvement of Digital Signature Algorithm Based on Elliptic Curve Cryptography," in *Advances in Computer Science Research*, 2020.

[10] V. S. Prakash, K. S. Keerthi, and S. Jagadish, "An Elliptic Curve Digital Signature Algorithm for Securing the Healthcare Data Using Blockchain-Based IoT Architecture," *IEEE Int. Conf. Data Sci. Blockchain*, 2024.

[11] R. Anusha and R. Saravanan, "Revolutionizing Signature Scheme: Enhanced Edward Elgamal Extreme Performance Accumulate Signature for IoT and Blockchain Applications," *Soft Computing*, 2025.

[12] D. M. Sharma and S. K. Shandilya, "Maximizing Blockchain Security: Merkle Tree Hash Values Generated Through Advanced Vectorized Elliptic Curve Cryptography Mechanisms," *Concurrency and Computation: Practice and Experience*, vol. 35, no. 15, e7829, 2023.

[13] A. Kamala, H. A. El-Kamchochi, and A. El-Fahar, "Conic Curve Encryption and Digital Signature Based on Complex Number Theory for Cybersecurity Applications," *Scientific Reports*, 2025.

[14] B. Sowmiya, E. Poovammal, K. Ramana, and S. Singh, "Linear Elliptical Curve Digital Signature (LECDS) with Blockchain Approach for Enhanced Security on Cloud Server," *IEEE Int. Conf. Adv. Comput. Commun. Syst.*, 2021.