Power System Technology
ISSN:1000-3673

Received: 08-11-2025 *Revised: 15-02-2026* *Accepted: 26-03-2026*

An Adaptive Elliptic Curve Cryptography Framework for Robust, Scalable and Secure IoT Blockchain Applications

Usma Bibi

Department of Computer Science, University of Sargodha, Sargodha, Pakistan.,

Khalid Mahmood Aamir

Department of Information Technology, University of Sargodha, Sargodha, Pakistan.,

Abdul Jaleel

Department of Computer Science (RCET, GRW), University of Engineering and Technology, Lahore, Pakistan.,

Hafiz Muhammad Faisal Shehzad

Department of Computer Science, University of Sargodha, Sargodha, Pakistan

***ABSTRACT*—**Conventional blockchain systems in Internet of Things (IoT) applications encounter significant scalability, security, and efficiency problems that degrade their efficiency. Despite offering a secure, decentralized, and transparent framework, existing blockchain implementations in IoT systems face significant challenges, including rigid hash parameter configurations, potential security vulnerabilities, the computational complexity of algorithms such as RSA, and inherent limitations in scalability. The objective of this study is to design a cryptographic framework that (i) ensures quantum resistance, (ii) improves scalability for resource-constrained IoT devices, and (iii) reduces encryption overhead compared to RSA and SHA-256. We propose an Adaptive Elliptic Curve Cryptography (AECC) framework using a dual-layer Elliptic Curve mechanism, where the base point is adaptively derived from the underlying data, enhancing both security and scalability. Furthermore, a novel blockchain architecture is designed that leverages the mathematical properties of Elliptic Curves, effectively replacing traditional compression and encryption techniques. The framework primarily derives hash values from varying parameters whose base point G is unknown and then a Quantum safe cryptographic system employing Elliptic Curves instead of SHA 256 and RSA. Compared to currently available blockchain algorithms, the proposed AECC algorithm is relatively and statistically more efficient according to the results obtained from confusion and diffusion analysis, uniform distribution analysis, sensitivity analysis, and collision analysis. Our significant innovation is quantum-resistant security with randomized base points and dual-ECC layers that prevent precomputation attacks with near-ideal diffusion/confusion (0.0317) and collision resistance. The second innovation is computational efficiency whereby AECC minimizes key sizes by 12× compared to RSA (256-bit vs. 3072-bit) with comparable security, as well as 3× faster encryption speeds (1.5 ms per block). Another innovative addition includes IoT suitability that guarantees scalability with dynamic parameterization for resource-constrained devices with sensitivity analysis demonstrated (0.4995 bit-flip rate) and testing on real IoT datasets. Our empirical results establish AECC's superiority over RSA and SHA-256 in terms of security, energy efficiency, and adaptability, and hence a robust solution for future IoT-blockchain applications.

Power System Technology
ISSN:1000-3673
Received: 08-11-2025 Revised: 15-02-2026 Accepted: 26-03-2026

INDEX TERMS *Blockchain, Internet of Things, hashing, Elliptic Curve Cryptography, Scalability, data integrity*

1. INTRODUCTION

Blockchain technology has gained recognition as an effective solution for implementing secure, decentralized and transparent framework for managing transactions and data in various applications, specifically the integration of blockchain in Internet of things has gained significant attention with the potential for improving security, transparency and data integrity. However, it has been noticed that the conventional blockchain systems present several challenges when applied to IoT environments due to their limited scalability, security and computational efficiency [1]. Blockchain applications like cybersecurity, real estate, Asset management, supply chain management, cross-border transactions, healthcare, insurance, entertainment, finance, etc. have revolutionized the digital world. It becomes the perfect solution for giant businesses due to its decentralized, transparent, and safe character, facilitating reliable and effective transactions [2].

In IoT applications, blockchain provides a safe foundation to record, maintain, and authenticate ownership, data, and transactions. The general structure of blockchain is comprised of a decentralized network of nodes that verify and store a chain of data blocks connected through a cryptographic hash consisting of a collection of verified transactions [3]. This structure is applied to the IoT devices to safely record and manage devices' data, identities, and transactions by making use of a private blockchain or consortium with a changed consensus mechanism [4]. However, the traditional blockchain systems face many challenges when applied to small resource constrained devices as shown in Figure 1.1

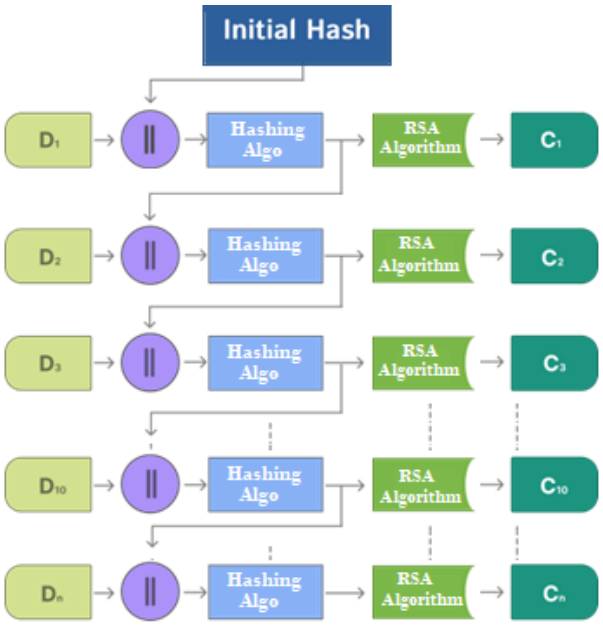

FIGURE 1.1 Traditional Blockchain in cryptography

The Internet of Things (IoT) has changed the way people interact with each other using devices connected to the web meanwhile it also comes with a few security vulnerabilities. One such example of an IoT application is the Teleoperated robotic systems to mitigate these security risks and safeguard IoT devices. Protecting these robotic systems is challenging due to the limited number of resources available in the IoT devices. Elliptic Curve Cryptography (ECC) has been presented as a viable solution to enhance the security of such robotic systems while

Power System Technology
ISSN:1000-3673
Received: 08-11-2025 Revised: 15-02-2026 Accepted: 26-03-2026

protecting the confidentiality and integrity of IoT devices data [5]. However, the existing blockchain frameworks face issues when attempting to operate on small devices within IoT networks, the challenges include computational complexity, fixed hash values that compromise security, and limited Scalability [6].

The key objectives of this paper are to:

1. Propose an adaptive ECC-based blockchain solution for IoT environments.
2. Enhance scalability and computational efficiency using variable ECC parameters.
3. Eliminate reliance on fixed hash values to ensure security and quantum resistance.

We use Elliptic Curve Cryptography to enhance the security and overall performance of blockchain applications in small devices [7]. The cryptographic hash function takes an input message of varying character length and produces an output of a fixed length of characters called a message digest or hash value. It provides IoT data integrity and reliability by detecting unauthorized alterations or tampering and different types of attacks like data impersonation, data manipulation, spoofing, and prevailing attacks while keeping the IoT device's data confidentiality, integrity, and authenticity [8]. Compared with the traditional cryptographic mechanisms, ECC offers a higher protection level at low-key size, as well as improved performance, making it particularly suitable for low power IoT devices.

1.1 ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic Curve Cryptography (ECC) is shown to be one of the most efficient means of implementing public-key cryptography, because it offers high level of security while using relatively smaller key sizes compared to traditional complex cryptographic algorithms such as RSA [9].

The elliptic curves are not ellipsis but reflected by the shapes as shown in Figure 1.2. The security of the ECC based cryptosystem is defined by mathematical problems. Describing the example problem as Where we have two points on a curve denoted as G and Y representing in a way that $Y = kG$ (such that Y is derived by adding G to itself K times), find out the integer k. This phenomenon is called the elliptic curve discrete logarithm problem. The existing methods are not very proficient for calculating the discrete logarithms of Elliptic curves while comparing with the conventional factorization methods [10].

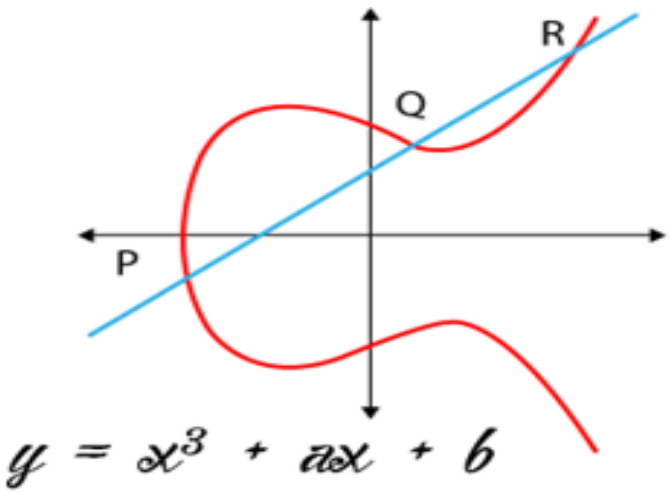

FIGURE 1.2. Elliptic curve representation

Power System Technology
ISSN:1000-3673
Received: 08-11-2025 Revised: 15-02-2026 Accepted: 26-03-2026

ECC offers a safe mode of data transmission and authentication while using the mathematical principles of Elliptic Curves. Therefore, ECC is now widely adopted by multiple sectors in a variety of industries including finance, healthcare, commerce, and technology. ECC promises the validity, confidentiality, and integrity of Electronic Commerce transactions. In SET protocols, ECC offers strong security and ensures the protection of online transactions [11], and it has become an essential tool for initiating safe communication, protection of sensitive information, and establishing secure digital signatures because it uses the smaller key sizes and provides the same level of security as RSA [10]. ECC has widespread use in various applications of IoT devices. However, ECC-based signcryption techniques are reported as inefficient and insecure for encryption by the studies [12]. Therefore, a new ECC-based signcryption scheme has been presented to overcome these challenges. Signcryption combines the features of digital signature and encryption in a single phase. The signcryption is introduced with a lower cost of computation to provide authentication, message secrecy, confidentiality, and message integrity to the low power devices [13].

To address the challenges faced by traditional blockchain architecture, this paper proposes an Adaptive Elliptic Curve Cryptography based approach to enhance the security, scalability and overall performance of the IoT devices. Unlike conventional cryptographic methods like RSA, adaptive ECC introduced a lightweight and efficient method of encryption improves the security of the small IoT networks. This paper proposes a parameterized ECC in Blockchain, replacing traditional RSA to improve small devices' security, Scalability, and computing efficiency. This methodology addresses the constraints of conventional blockchain architectures in IoT, guaranteeing a safe, decentralized, and transparent foundation for IoT devices.

In summary, the main contributions of this work are:

- A novel blockchain architecture leveraging Elliptic Curve Cryptography (ECC), replacing traditional compression and encryption algorithms to enhance efficiency and security.
- The use of the mathematical properties of ECC to overcome the limitations of traditional blockchain architectures for IoT security, scalability, and computational efficiency.
- The design of a more suitable and secure EC based hashing algorithm for resource-constrained IoT devices for strong encryption and low computational cost compared to RSA.
- A quantum-resilient cryptographic framework based on ECC, hence eliminating reliance on traditional complex algorithms and enhancing future-proof security.
- An ECC based architecture with varying parameters to improve security and scalability and solve problems like fixed hash parameters and computational inefficiencies.
- We implemented the AECC algorithm in MATLAB R2023 using publicly available greenhouse IoT sensor datasets (Tikrit University). The environment included 64-bit Windows, Intel i7 processor, 16 GB RAM.

The remaining paper is organized into four sections. In Section II an extensive literature review is given on Blockchain-based IoT systems, ECC applications in digital surroundings, data security issues, and the hash algorithm. Section III, Research Methodology outlines the specific methods employed in the research. It explains the model selection, and data collection, and discusses the datasets used for the study. Section IV presents the findings of our study in the Results and Discussions section and presents the findings of the learning. Finally, Section V presents the conclusion to summarize our key contributions and future implications.

Power System Technology
ISSN:1000-3673
Received: 08-11-2025 Revised: 15-02-2026 Accepted: 26-03-2026

2. LITERATURE REVIEW

In this section, we present an overview of the literature on blockchain based applications, Blockchain integrated IoT applications, and challenges faced by blockchain architectures along with cryptography. We also present the existing work on ECC based blockchain architectures and conventional cryptographic algorithms.

2.1 ELLIPTIC CURVE CRYPTOGRAPHY FOR IOT SECURITY

Blockchain technology is a decentralized, dispersed ledger system that secures the transactions between two parties. Once data is entered in a block of the blockchain, editing or deleting it is not possible due to its immutability feature. As it is a trustful and transparent way of data management, blockchain has been applied more frequently on Internet of Things. However, when incorporated into small IoT network devices, this blockchain framework faces challenges like limited scalability and low processing capacity. ECC has been proposed by researchers as a solution that enhances the security and efficiency of blockchain for small devices, replacing the conventional cryptographic methods [14] . In Internet of Things (IoT) people interact with each other using devices connected to the web but face a few security vulnerabilities. One such example of an IoT application is the Teleoperated robotic systems to mitigate these security risks and safeguard IoT devices. Protecting these robotic systems is challenging due to the limited number of resources available in the IoT devices. Elliptic Curve Cryptography (ECC) has been presented as a viable solution to enhance the security of such robotic systems while protecting the confidentiality and integrity of IoT devices data [13].

The rapid expansion of the Internet of Things needs more secure and reliable methods of authentication. This problem is resolved by proposing a general security framework for authentication that leverages edge computing and employs fully hashed Elliptic Curve Menezes-Qu-Vanstone (ECMQV). This framework holds the ability to maintain scalable and robust security protocols for IoT data communication [15]. By adopting blockchain, IoT devices are protected against hacking and misuse of data by malicious persons.to resolve the possible security issues a blockchain-based application for proof-of-concept has been proposed [16]. Thus, the integration of Blockchain presents a promising solution to address these security concerns. Protecting IoT devices is a rather difficult task due to their limited resources and capacity [17].

In a study based on blockchain and cryptography, a Lightweight cryptographic technique has been recommended to secure small IoT devices, with more than 50 methods available. To optimize the security of these devices, Outsourcing RSA decryption alongside lightweight cryptography has been proposed. However, existing systems have turned out to be ineffective and vulnerable [18]. A new scheme using the Chinese Remainder Theorem (CRT) has been proposed for wearable devices that are gaining traction in multiple areas, more specifically in healthcare. However, these devices have limited resources and therefore pose significant security challenges. To overcome these challenges a lightweight authentication scheme has been introduced to enhance the security of these devices [19]. An improved lightweight anonymous authentication protocol for the Internet of Medical Things (IoMT) is presented by implementing Elliptic curve cryptography. This scheme identifies vulnerabilities and builds a secure communication channel between patients and healthcare providers [20]. In a blockchain-based solution, Manoj Kumar et al addressed the security and privacy problems associated with safe IoT data sharing and authentication using elliptic curve integrated encryption through diverse networks. The study aims to improve IoT devices security with blockchain technology and elliptic curve cryptography [21].

Arunkumar et al. presented a secure IoT framework for smart cities using techniques like Logistic Regression and Elliptic Curve Cryptography (LRECC) to prevent, detect, and mitigate threats. In this methodology ECC algorithm is implemented for key generation and distribution sharing

Power System Technology
ISSN:1000-3673
Received: 08-11-2025 Revised: 15-02-2026 Accepted: 26-03-2026

while the Logistic Regression machine learning technique is applied for transmitter selection, leading to dependable routing paths with little overhead and saving 29.95% computation time [22]. Faton Kabashi and Halil Snopce proposed the implementation of Elliptic Curve Digital Signatures (ECDSA) within blockchain technology for secure and decentral management of certificates in Higher Education. This approach facilitates the maintenance of the integrity and immutability of student credentials [23].

An improved smart card-based authentication protocol ESEAP is introduced using Elliptic curve cryptography as a foundation for secure communication. This protocol provides a wide range of security features, including resilience against different types of attacks, as well as incorporating the features of mutual authentication and key agreement. The proposed scheme results in improvements in both computation and communication costs [24]. According to the research by the Author, RegKey is an implementation of register-based ECC signature algorithms for the security enhancement of cryptographic method implementations. This work is motivated by the goal of increasing speed while protecting against one-time memory disclosure attacks through the partitioning of ECC signing into two segments, reducing register utilization and performance overhead, and guaranteeing that the plaintext private key and the random number are limited to registers. RegKey offers robust protection against cold-boot and warm-boot attacks and is an appropriate option for embedded devices or offline systems where physical threats are the major issues [25]. Besides ECC, many other cryptographic algorithms like RSA and El-Gamal have been proposed to secure IoT devices. Unfortunately, these algorithms have been proven to be insecure and inefficient. A comparative analysis of these algorithms is crucial to identifying the most suitable algorithm for IoT devices [26]. The detailed comparison of existing studies is shown in Table 2.1.

Teleoperated robotic systems in medicine encounter safety issues and security constraints. Elliptic ECC overcomes these concerns with its superior security and efficiency. This study introduces a high-performance SM2 ECC architecture with reduced latency and rapid computing [27]. Alongside ECC, various cryptographic algorithms have been suggested to enhance the security of teleoperated robotic systems, such as RSA and El-Gamal. Nonetheless, these algorithms have demonstrated inefficiencies and vulnerabilities. An analysis of these algorithms is crucial to identifying the most appropriate option for teleoperated robotic systems [28].

Another research introduces a homomorphic hashing technique utilizing elliptic curve encryption (ECC) to securely store and process data in cloud environments, overcoming the shortcomings of current homomorphic hashing methods. The proposed method exhibits enhanced efficiency and security, corroborated by mathematical models, actual applications, and experimental findings [29]. Javad Doliskani et al [30] have created a variation of the CGL hash method that achieves an exponential speedup compared to the original approach, with a performance ratio of$(5.7n + 110)/(13.5\,log\,n + 46.4)\,for\,n = log\,p$, where p represents the characteristic of the finite field. This optimization results in a notable acceleration, with specific speedup factors of 33.5 and 47.8 for 256-bit and 384-bit quantum preimage security levels, respectively [30]. Email communication has gained significant traction across multiple domains. Securing email communication presents substantial challenges because of its vulnerability to interception and misuse. PGP has been suggested to secure email communication; however, it has been identified as susceptible to key-sharing attacks. Blockchain technology has been proposed to enhance the security of PGP key sharing [31].

Power System Technology
ISSN:1000-3673
Received: 08-11-2025 Revised: 15-02-2026 Accepted: 26-03-2026

Table 2.1: A Comparison of Existing Works of ECC in IOT based on Objectives, Contribution, and Challenges Identified

Author (Year)	Paper Objectives	Major Contribution	Challenges Identified
Kabashi, [23]	Implementation of ECDSA in blockchain technology for certificate management in Higher Education	Secure and decentralized certificate management, automation of certificate issuance and verification, increased efficiency and reduced administrative costs	Scalability, Interoperability, Regulatory frameworks implemented in academic institutions.
Abbas et al[28]	Summary of Elliptic Curve Cryptography (ECC), including its algorithmic procedures, essential protocols, frameworks, and applications.	Comparison of ECC vs RSA, Analysis of Key Size and Overhead, Graphical Representations of the Cryptographic Process	Issues about data security and confidentiality during communication
Kharche [15]	Deployment of blockchain technology in IoT networks for scalable Intelligent Transportation Systems (ITS) in India.	Augments security, transparency, and efficiency in transportation. Facilitates real-time traffic optimization and enhances safety measures.	Incorporation with the current Intelligent Transportation Systems infrastructure. Requirement for the dependability and sustainability of blockchain systems.
Das [19]	Wearable device security	Proposes a streamlined authentication protocol for wearable devices in healthcare applications.	Securing wearable devices is challenging owing to limited resources.
Mallouli [26]	Cryptographic algorithms for the Internet of Things (ECC, RSA, El-Gamal)	Analyses ECC, RSA, and El-Gamal for IoT, identifying inefficiencies; recommend comparative studies to choose appropriate algorithms.	Current encryption techniques for IoT are ineffective and vulnerable.
Thakor [16]	Security of IoT devices, lightweight cryptographic methods	Highlights lightweight cryptography (over 50 methods) and the necessity for comparative analyses to determine the optimal strategy for IoT security.	Ensuring the security of resource-limited IoT devices is difficult.
Xiao [27]	Security of teleoperated robotic systems	Proposes Elliptic Curve Cryptography (ECC) for the security of teleoperated robotic systems, including comparing cryptographic methods such as RSA and El-Gamal.	Resource limitations hinder the acquisition of teleoperated robotic devices.
Kumar et al. [21]	Security and privacy in distributed Internet of Things (IoT) framework, proposing a blockchain-	They proposed a blockchain-based approach with EC integration for IoT security—	- Data protection & Ownership - IoT security & privacy

Power System Technology
ISSN:1000-3673
Received: 08-11-2025 Revised: 15-02-2026 Accepted: 26-03-2026

	based approach with elliptic curve integrated encryption.	secure data sharing & authentication mechanism.	- Scalability & interoperability.
Arunkumar et al. [22]	A secure IoT structure for smart cities using logistic regression and ECC.	Proposed an LRECC approach for secure key generation and distribution and reliable routing with less delay	IoT privacy and security issues, routing overhead and delay.
Hossain [31]	Securing email communication with Blockchain and PGP	Proposes utilizing blockchain technology to secure PGP key distribution in email correspondence.	PGP framework is vulnerable to key-sharing attacks.

2.2 INTEGRATION OF ECC AND HASHING IN BLOCKCHAIN

Integration of Elliptic Curve Cryptography (ECC) and hashing in blockchain technology offers a safe and transparent data management facility. Adopting Hashing along with the Secure Hash Algorithm (SHA) provides robust security, data integrity and authenticity [32]. A maximum confusion diffusion results show near to the theoretical bounds ensuring that every input bit affects the maximum output bits, making it a promising solution for value-based applications. This integration of ECC and Hash promotes trust, accountability, and clarity in blockchain technology, optimizes business processes, and provides a protected environment for data exchange [8], as shown in Table 2.2. The existing literature highlights the challenges and limitations of ECC hashing including implementation complexity, vulnerabilities and the potential risk factors. In recent advance studies, an approach is presented where ECC is implemented with Machine learning. An overview of efficiency and security of both the algorithms are presented to improve the security and performance of ECC through ML applications. The main objective is to generate optimal parameters for Elliptic curve cryptography methods by integrating machine-learning techniques [33].

A new hash-based method for balancing security and efficiency of sensitive data through ECC is presented in [34].

Table 2.2: Summary of Current ECC Frameworks with Hashing Techniques, Algorithms used, Limitations, and Security Level

Authors	Summary	Algorithms	Limitations	Future Work	Security Level
Jihane Jebrane et al. [33]	Overview of integrating ML with ECC to enhance security and performance.	ECC, AI-based Hashing	High computational cost in ML-based ECC models.	Optimize ECC-ML integration for lightweight devices.	128-bit classical security; vulnerable to quantum attacks.
Abel C. H. Chen. [29]	Proposes an ECC-based homomorphic hashing function to secure data in cloud.	ECC, Homomorphic Hashing	Theoretical model; lacks real-world testing.	Implement and benchmark on various cryptographic platforms.	192-bit security (Classical); more resistant to quantum attacks but not future-proof.
Younes Lahraoui et al. [34]	Introduces a hash-based technique for	ECC-521, SHA-3	High memory requirements for hash storage.	Reduce computational	256-bit classical security; SHA-3 reduces to 128-bit

Power System Technology
ISSN:1000-3673
Received: 08-11-2025 Revised: 15-02-2026 Accepted: 26-03-2026

	embedding messages into EC points to secure data exchange.			overhead for IoT security.	under Grover's attack.
Jeremy Maitin-Shepard et al. [35]	Presents ECC-based multiset hashing to enhance efficiency and security of data.	ECC-384, Multiset Hashing	Requires further analysis on security robustness.	Validate security for blockchain applications.	128-bit classical security; partially resistant to quantum threats.
Mahender Kumar. [36]	Explores the use of Pairing-Based Cryptosystems (PBC) with ECC for security at low key sizes and computing costs.	ECC, Pairing-Based Cryptography	Computational intensity of pairing operations poses challenges for constrained devices.	Optimize pairing calculations to reduce computational overhead.	Depends on ECC size; vulnerable to quantum threats.
Svitlana Kazmirchuk et al. [37]	Proposes an improved digital signature algorithm based on ECC to enhance security and efficiency.	ECC, Schnorr Signature Algorithm	Theoretical proposal; lacks practical implementation and testing.	Develop practical implementations and assess performance in real-world scenarios.	128-bit classical security; vulnerable to quantum attacks.
Felipe Tellez, Jorge Ortiz. [38]	A comparison between two artificial intelligence algorithms for ECC optimization	Genetic Algorithm (GA) and Particle Swarm Optimization (PSO),	Focus on pre quantum era only, not represent real world scenario	Quantum resistant ECC parameters optimization and integration in real world e commerce environment.	128-bit classical security, vulnerable to quantum attacks.
Kohei Nakagawa, Hiroshi Onuki [39]	Introduces SQIsign2D-East, a new signature scheme using 2-dimensional isogenies for post-quantum security.	Isogeny-Based Cryptography	High computational complexity requires further optimization.	Enhance efficiency and assess security against emerging quantum attacks.	Designed to be quantum-resistant; security depends on isogeny problem hardness.
Olusogo Popoola et al. [40]	Combining ECC-256r1with AES 128 for security of smart home healthcare	ECC-256r1 and AES-128 in EAX	Designed for smart homes and IoT only not applicable for the security of other domains.	Post quantum computing algorithm to secure smart home healthcare.	128-bit quantum resistant security comparable with AES

Power System Technology
ISSN:1000-3673
Received: 08-11-2025 Revised: 15-02-2026 Accepted: 26-03-2026

This method addresses the issues of embedded messages into the elliptic curve points that will disturb security and efficiency. A hash-based technique with random parameters is used along with a secret shared point generated from Diffie-Hellman algorithm to improve the security of the model. The proposed scheme is validated against various attack models, and through statistical tests. The result shows how effective the method is in terms of security and integrity. The algorithm also meets additional criteria for security and operability [34].

Another study introduces a scheme naming ECMH based on multiset homomorphic hash function. In this study, the author explains the use of Elliptic curve cryptography to address the challenges and limitations of existing studies. This scheme, Elliptic Curve multiset hashing achieves optimal hash sizes and shows exceptional processing speed by combining traditional hashing with efficient encoding into binary elliptic curves. This approach can process over 3 million set elements at one second at 128-bit security level. This method provides secure solutions for many applications including database integrity verification, network coding and streaming set comparison to improve the overall performance and efficiency of ECC while facing new security challenges [35].

Another study investigates the usage of pairing-based cryptosystem integrated with ECC to get high security at lower key sizes and computational overhead. According to the exploration, the limited computational capacity of resource-constrained devices, poses a security challenge that needs continuous authentication [36]. Recent research explores Elliptic curve cryptography to efficiently improve the digital signature schemes at smaller key size and fast computation time. Digital signatures are crucial for security in providing message integrity and authenticity. In this scenario, a Schnorr signature algorithm is a suitable approach to handle security concerns. However, existing method implementation has limitations, so here a new digital signature scheme is proposed to address these limitations [37].

A new approach called homomorphic hashing is proposed using ECC to keep sensitive data safe in cloud. In this method, a unique code is generated for each piece of information and saved on cloud. Therefore, when someone gets access to the information, they will not be able to understand the real information. The validity of the method is tested through mathematical models and real-world examples and results show that this one is the efficient way to protect data, however this cannot be applicable and suitable for all scenarios [29].

In another study a comparison of AI algorithms including Genetic Algorithm and particle swarm optimization algorithms is given for enhancing Elliptic curve cryptography parameters for secure e-commerce transactions. The study shows considerable computational cost when using artificial intelligence techniques to ECC and a tradeoff between security and performance in E-Commerce system. The future research in this area is required with a focus on developing hybrid AI methodologies to efficiently optimize ECC and improve security protocols while maintaining system performance in a real time E-Commerce setup [38].

Based on the hardness of the basic mathematical problem the Isogeny based cryptographic method is presented for NIST PQC standardization. This signature scheme is called SQIsign uses very short key size and signature for signature verification. This method enhances efficiency and security against attacks but depends on isogeny hardness problem [39]. The study explores the latest advancements, trends and applications of ECC. It signifies the limitations and challenges of implementing ECC in the form of risks of errors and several vulnerabilities. According to this study, the traditional ECC techniques are prone to quantum attacks and lack of standardization. There should be a focus on developing frameworks that are quantum resistant and reduce complexity of ECC implementation to prevent vulnerabilities and get a standardized compatibility [40].

In another paper, the mathematical foundations of Elliptic curve cryptography are explored with a comparison of security, efficiency and implementation challenges specifications. The

Power System Technology
ISSN:1000-3673
Received: 08-11-2025 Revised: 15-02-2026 Accepted: 26-03-2026

mathematical complexity of ECC makes it difficult to implement correctly and the incorrect implementation results in security vulnerabilities. There need to be future efforts to simplify the ECC process and develop strong cryptographic libraries for safe and correct implementation [41].

This study presents a review on the advantages of Elliptic curve cryptography as a lightweight algorithm for IoT devices and embedded systems. It also highlights the resource limitation, a challenge for implementing the ECC on low power IoT devices and shows that power consumption is also a big challenge for battery-operated devices having limited storage and power capacity. The work directs future research towards ECC optimization for low power devices and a comparative study of ECC with another lightweight cryptographic algorithm [42].

A multiset elliptic curve hash method is introduced in [43], this method encrypts the hash functions into binary elliptic curves to improve security and efficiency. The major challenge highlights in this study are collision resistance and needs further evaluation to reduce the implementation complexity through required modifications to the traditional systems. They also suggest crucial security assessment steps for robustness and performance improvement for ECC adoption in real world [43].

In conclusion, ensuring the security of IoT devices presents a significant challenge because of their limited resources. A range of cryptographic algorithms has been put forward to enhance the security of IoT devices. The findings show an increasing focus on applying ECC within blockchain technology for IoT, emphasizing its capability to solve the issues present in current blockchain systems. The increasing trend of blockchain technology in various domains including finance, healthcare and IoT have raised issues of security and scalability. Among the cryptographic tools adopted in blockchain, ECC has been recognized as one of the most effective methods of ensuring security while requiring less space than other methods. However as the size of the blockchain network grows it becomes complex due to which the traditional ECC deployment methods face challenges of computational overhead, delays and resistance to quantum attacks [44], [45].

The literature highlights the following specific issues:

- *Scalability: The s*calability issue arises due to the computational load required for ECC on nodes in decentralized blockchain environments which then slows processing and utilizes energy in limited resource environments.
- *Security:* The advancements in nature and architecture of complex computation pose a significant risk to ECC. Thus, it becomes critical to explore various post quantum elliptic curve variants for implementing blockchain systems that will be safe n secure in future.
- *Blockchain Integration:* Although implementing blockchain improves data integrity and traceability, it has been observed that integration of ECC based protocols with smart contracts etc. is challenging [7].
- *Implementation in specific use cases:* Various applications including healthcare, internet of things (IoT), and finance and supply chain management are now using blockchain for the efficient and secure management of data [46], [20], [23], [28] [47], [44]. However, these domains have specific characteristics that make it difficult to adopt and integrate the blockchain based ECC.

To summarize, while ECC-based approaches offer improved security for IoT, prior methods suffer from fixed parameters, limited scalability, or lack of quantum resistance. Our contribution addresses these gaps via a dual-layer ECC architecture with dynamically adjusted base points, ensuring attack resilience and efficiency for IoT applications.

Power System Technology
ISSN:1000-3673
Received: 08-11-2025 Revised: 15-02-2026 Accepted: 26-03-2026

3. METHODOLOGY

This work proposes an adaptive ECC protocol aims at providing scalability, security and data integrity with a lower key size algorithm suitable for a resource constrained environment, addressing the challenges of computational efficiency, decrease delays, and provide resistance against attacks. Figure 3.1 presents our methodology for designing the adaptive Elliptic curve-based framework.

FIGURE 3.1 Methodology Steps to Design the Adaptive Elliptic Curve-based framework

The cryptographic approach is discussed with cryptographic system architecture, the simulation setup and the insights to address the challenges of the blockchain based IoT applications.

3.1 Research Design

In our research, we analyzed the current literature on elliptic curve cryptography and its applications. We selected Elliptic curves instead of RSA to get the same level of security at lower key size. ECC is computationally less expensive than RSA, therefore suitable for IoT devices with limited resources. Next, we used the varied parameters in ECC to increase security and flexibility. When the cryptographic parameters vary dynamically and are not fixed, they reduce the risk associated with fixed hash parameters making the system flexible to the varying security conditions in IoT environments. The next step is the generation of hash value; in our system, we replace the traditional systems where hash values are generated using SHA 256 and RSA.

Our proposed work is designed to make it irresistible against attacks. When G is known there is the possibility of Quantum Attacks. In our research, we have not fixed G; it varies from record to record. Base point G is defined by the data itself and is not known to the attacker. In this situation, attackers shall have an infinite space for G. Therefore, the proposed methodology is not breakable to QAs. As the base point is not known, Elliptic curves are generated with different data records, and no one can possibly know the exact value of the records. This is the major difference between working with fixed parameters where base points and end points are known and the attacker, if finds out the initial value they can break the hash. But here in our case, as the base points are not known and next values are also randomly generated, therefore the attacker

Power System Technology
ISSN:1000-3673
Received: 08-11-2025 Revised: 15-02-2026 Accepted: 26-03-2026

cannot find out the values to access the hash. In our work, we generate next hash values using Elliptic curves feed forward from the previous hash, instead of compression and encryption algorithms. The hash values generated in this way consume less energy with faster processing. Then, we developed an algorithm for implementing elliptic curve cryptography using MATLAB. We employed a dataset of random numbers to evaluate the algorithm's efficiency and security. Then, we perform an analysis of our results. We assessed the simulation results to evaluate the algorithm's performance.

3.2 Cryptology

Cryptology is the discipline that examines encryption and decryption methods, converting messages into unintelligible formats and vice versa. It consists of two primary branches: cryptography and cryptanalysis. Cryptography emphasizes information security by examining mathematical techniques to guarantee reliability, data integrity, and authentication while tackling potential transmission challenges. The primary objective is to safeguard information between the sender and recipient. Conversely, cryptanalysis seeks to decode encrypted signals, revealing the original content [32]. Secret keys are utilized to regulate the encryption process for security purposes. We will use a novel cryptographic technique for data integrity and security against quantum attacks, including key generation, encryption, and decryption, to guarantee a secure connection. We employed hash functions to ensure data integrity [34]. The cryptography related discussion is described in nine steps given in Figure 3.2.

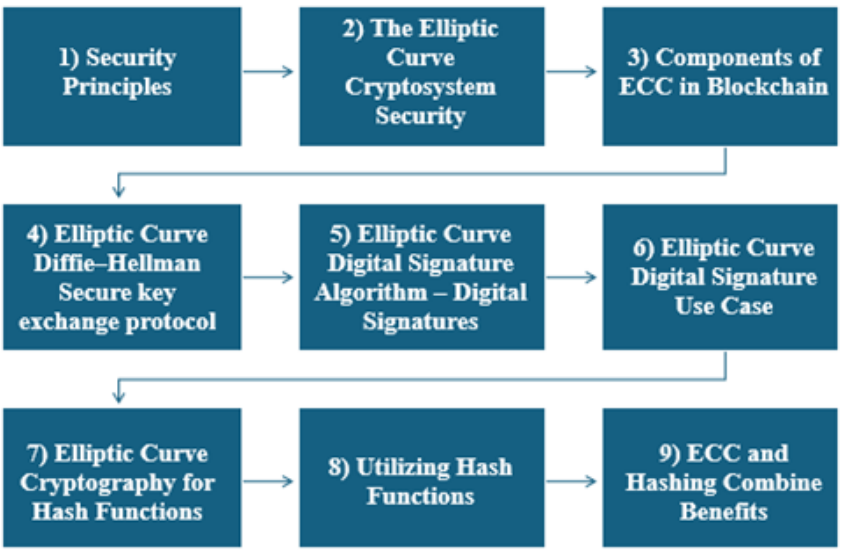

FIGURE 3.2. Steps to define and incorporate Cryptography in ECCA

1) Security Principles

To guarantee the secure transfer of information, specific security principles of cryptology are expected to be followed by the utilized communication technologies [48]. These principles are essential to ensure the safe transmission of information and the integrity of received data, which can be accomplished using cryptographic algorithms and hash functions. The security principles are shown in Figure 3.3.

Power System Technology
ISSN:1000-3673
Received: 08-11-2025 Revised: 15-02-2026 Accepted: 26-03-2026

FIGURE 3.3. Cryptography security principles

We adopt a practical methodology for our research to address the problem practically. We utilize freely accessible datasets of IoT devices to achieve our objectives. In this study, we employ elliptic curves and hashing to construct a blockchain and generate a hash output. The research methodology for our work includes using elliptic curve cryptography and hashing to build a blockchain for secure data transmission in IoT devices.

2) The Elliptic Curve Cryptosystem Security

Like all public-key cryptosystems, Elliptic curve cryptosystems rely on a challenging mathematical problem as a base for security. One such problem is the discrete logarithm problem for an EC. The problem is taking two points, G and Y, on an EC so that we must find the integer k in such a manner that $y = kG$. Here, G is the base point, and Y is a point on the Elliptic curve [14]. An elliptic curve over a finite field has its basic equation given in Eq. 1.

$$y^2 = x^3 + ax + b \qquad (1)$$

An elliptic curve must meet the criterion where a, and b are integers that fulfill the requirement given in Eq. 2.

$$4a^3 + 27b^2 \neq 0 \qquad (2)$$

It guarantees that the curve possesses no more than one root and that the integers a and b are authentic. Furthermore, the elliptic curve needs a zero point, or infinity, denoted by the symbol O [10]. That ensures that the resultant curve satisfies the prerequisite conditions for an elliptic curve. Here, we apply a lightweight cryptographic method called ECC to ensure safe communication and data integrity in blockchain-based IoT networks. Compared with conventional systems like RSA, ECC offers a high level of security with lower key sizes and provides a high degree of security that fits IoT devices running on limited processing capacity and memory.

This lightweight cryptographic operation in IoT devices reduces computational overhead while maintaining security. ECC demands very low-key sizes and fewer computational resources, therefore it reduces energy consumption and improves system processing efficiency, making it suitable for resource-limited IoT Blockchain security applications. To secure the IoT networks the ECC framework is incorporated into the system into the transaction layer, network layer, and storage layer. ECC ensures security at these layers by using ECDSA for transaction signing and verification, implementing ECDH for securing device-to-device communication, and through an

Power System Technology
ISSN:1000-3673
Received: 08-11-2025 Revised: 15-02-2026 Accepted: 26-03-2026

ECC-based hashing mechanism to store cryptographic keys. Each device generated and maintained ECC key pairs which guarantee confidentiality, integrity, and data authentication. This cryptographic algorithm improves blockchain security for IoT by using ECC to ensure efficient key exchange, authentication, and lightweight encryption. For IoT networks, ECDH for secure key exchange, ECDSA for transaction security and optimized encryption methods provide scalable, low power, and highly secure blockchain solutions [32].

3) *Components of ECC in Blockchain*

The following components are defined for ECC in blockchain.

(a) Elliptic Curve Diffie–Hellman Secure key exchange protocol

The objective is to create a safe route of communication between IoT devices without previous key distribution. Two distinct IoT devices agree upon an Elliptic Curve and a public generator point. Both devices select a private key (a, b) and compute the matching public key (aP, bP). Here the shared secret will be computed as Eq. 3.

$$S = a\,(bP)\; = b\,(aP) \qquad (3)$$

This guarantees a safe key exchange among IoT devices in the blockchain network since attackers cannot compute S without knowing either device's private key [42].

(b) Elliptic Curve Digital Signature Algorithm – Digital Signatures

The Elliptic Curve Discrete Logarithm problem (ECDLP) forms the foundation of ECC security, as it is computationally difficult to derive private key from public key. The objective of the ECDSA algorithm is to verify transactions and guarantee non-repudiation in the ledger of blockchain development [10]. The method is defined below.

- A **sender** signs a transaction they generated using his private key. The signature is computed as Eq. 4.

$$S = (r, s) = (x(kP), \frac{Hm+dr}{k}\ mod\ n) \quad (4)$$

Here k is denoted as a random number, (Hm) is the hash of the message and d is the private key.

- The **receiver** uses the public key of the sender to confirm the transaction using Eq. 5.

$$r' = x(H(m)P + rdP) \qquad (5)$$

The validity of the signature is shown if r^'=r which confirms the message's authenticity.

(c) Elliptic Curve Digital Signature Use Case

Let in a community users want to enter in secure communication using ECC method. For an elliptic curve-based group Eq (a, b) with parameters q, a, and b and basepoint G ∈ Eq (a, b).

Person A: Select his private key as X_A and generate his public key from private key $Y_A = X_A \times G$

Now his private key is X_A

His public key is = $Y_A = X_A \times G$

Person B: He selects his private key called X_B and generates his public key from the private key $Y_B = X_B \times G$

Now Person B's private key is = X_B

Person B's Public Key is: $Y_B = X_B \times G$

Power System Technology
ISSN:1000-3673
Received: 08-11-2025 Revised: 15-02-2026 Accepted: 26-03-2026

THE ECDH secret key exchange will be done as follows

Person A can see the key as: X_A, Y_A, Y_B

He also has knowledge of: X_B, Y_B, Y_A

Now A will calculate the session key: $K_A = X_A \times Y_B$

B will calculate the session key: $K_B = X_B \times Y_A$

The public key of A is $Y_A = X_A \times G$

The public key of B is $Y_B = X_B \times G$

The key calculation includes: $K_A = X_A \times Y_B$

$$= X_A \times (X_B \times G)$$

4) *Elliptic Curve Cryptography for Hash Functions*

The cryptographic method for secure electronic communications to which the current technology relates is the use of hashing functions that use Elliptic curve cryptography. One-way hash functions are used as a primitive for many cryptographic applications, such as public-key methods, digital signatures, authentication, and integrity verification. Hash functions convert data of any size into a fixed-length message digest or signature, guaranteeing one-way, fixed-length, secure, and unique hash values. An effective hash function should explicitly be deterministic, exhibiting uniform outputs for the same inputs and exhibiting sensitivity to minor changes in input data. These characteristics of hash functions make them an important element of secure communication systems. Elliptic curves can be used with varying parameters to ensure data integrity while generating hash values [32].

5) *Utilizing Hash Functions*

The application of hash functions in Elliptic Curve Cryptography (ECC) allows for the creation of secure digital signatures and authentication schemes efficiently. This property permits the creation of a unique digital fingerprint (or message digest) using hash functions in association with ECC for authenticating and integrity verification of a message. To accomplish this, they hash the message with a one-way hash algorithm such as SHA256 and then encrypt that resulting hash value using ECC [21]. The encrypted hash-value is effectively used as a digital signature to be authenticated by the recipient using the associated public key [34]. This method ensures that any modification or change of the message will result in a different hash value, making it identifiable by the recipient. We define the properties of Hash Functions as i) one-way preimage resistance, ii) weak collision or second preimage resistance, iii) strong collision resistance, and iv) uniform distribution.

6) *ECC and Hashing Combine Benefits*

Robust Authentication: ECC provides a robust authentication method using digital signatures. We can use ECC along with hashing techniques such as SHA-256 to be able to make the signed message reliable. Hashing verifies that a very small change to the message will result in a different hash value, signing to imply that if someone tries to tamper with the message it will be detected [49].

Preventing Collision Attacks: The confusion function can face collision attacks, which happen when two different inputs produce an equal hashed output. Combining ECC with hashing techniques mostly reduces collision attack risk. Due to the cryptographic properties of an ECC, it is difficult for attackers to take advantage of a collision, regardless of whether one occurs [21].

Power System Technology
ISSN:1000-3673
Received: 08-11-2025 Revised: 15-02-2026 Accepted: 26-03-2026

Effective Key Management: ECC reduces the key sizes compared to RSA without sacrificing the security level, and hence it is an efficient key management system. In environments where resources are constrained this is particularly helpful, for example in mobile platforms or the Internet of Things network [50]. In addition to ECC, hashing methods can also be used to optimize the data that is being processed while maintaining security. As compared to RSA, ECC is prone to major attacks. Data integrity and authenticity protection against significant attacks can be only provided by hash functions.

Enhanced protection Layers: Combining hashing methods and ECC provides increased layers of security. Hashing guarantees data consistency and non-repudiation provides data integrity. Meanwhile, ECC provides security and integrity while encrypting data.

Standardization and Interoperability: Many cryptographic protocols and Hash values combine to improve the interoperability between diverse platforms and systems. Standardized algorithms are used to adopt the best practices and optimize the performance of the existing system thus making the overall system secure [34].

3.3 Experiment Method

To achieve the study's goals, we will utilize publicly accessible IoT datasets concerning ECC security. This paper explores the implementation of blockchain technology utilizing elliptic curves in connection with hashing techniques. We take three inputs, X as the initialization parameter, C as curve parameters, and K as messages, and find a point on the elliptic curve as a cipher. Then input cipher and initialization parameter for the next curve and so on to make Blockchain of the elliptic curve also used another set of elliptic curves as previous with X', P' and C' and then apply ECs to produce Hash output and so on. In existing models of blockchain, they use only one EC in place of SHA as EC provides the same levels of security, which SHA provides, and the Curves generated are not changing values. Some of the blockchain models also use two ECs at a time, one in the place of compression algorithm and second in the place of encryption. However, when they generate the Curves, they never change base points, which enhances the vulnerabilities to attacks. In our contribution, we use two Elliptic Curves in place of compression algorithm and encryption algorithm but in a way that the result of the first iteration becomes the base point of the next iteration. Means our base points changes for each iteration and generated curves are attack resistance. Changing base points make the cipher secure as no one can find the exact character due to randomly changing base points, which are hash of the previous iterations result. The generated curves also show no singularity, which is the ideal condition for ECC.

3.4 Proposed Methodology

In Figure 3.4, we presented the steps involved in our proposed methodology

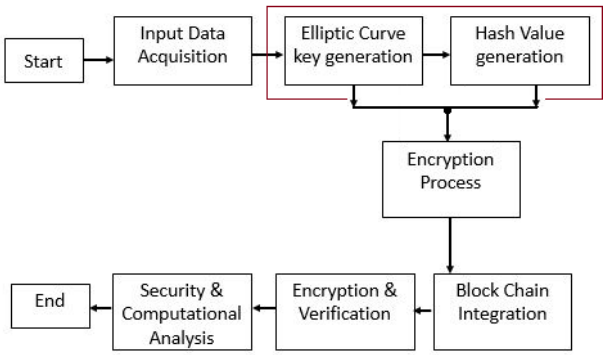

Figure 3.4. Blockchain Implementation using Elliptic Curve

Power System Technology
ISSN:1000-3673
Received: 08-11-2025 Revised: 15-02-2026 Accepted: 26-03-2026

Our proposed research is designed to make ECC secure against Quantum attacks. To break ECC, an attacker could try to discover XA from G and YA using Eq.6, where G is the generator point on the elliptic curve and Y is the resulting point.

$$[YA = XA \times G] \quad (6)$$

This is possible by Quantum attacks (QAs), when G is known.

In our research, we have not fixed G; it varies from record to record. Basepoint G is defined by the data itself and is not known to the attacker. In this situation, attackers shall have an infinite space for G. Therefore, the proposed methodology is not breakable to QAs. When G is known there is the possibility of Quantum Attacks. In our research, we have not fixed the initialization parameter G, and we also use two layers of ECs to make it secure. As the base point is not known, the Elliptic curves are generated with different data records, and no one can possibly know the exact value of the records. This is the major difference between working with fixed parameters where base points and end points are known and the attacker if finds out the initial value can break the hash. But here in our case, as the base points are not known, and the next values are also randomly generated therefore the attacker cannot find out the values to access the hash.

In our framework, through the input values of $X1, P$,

and C we will first compute a point on EC1 where base point is not known. This will be achieved by mapping the message P on Curve $C1$. The next step is to compute the cipher using X and $C1$'s base point G and use this value of hash as input for $C2$. Repeat the process for multiple curves to create a blockchain of ECs. At the end, generate the final hash output for each curve value for data integrity. $H1, H2 \ldots and\ Hn$ represent the hash values.

In traditional methodologies, we mostly input $X1$, lain text, and CF (Compression functions) to calculate a hash and then apply RSA to generate the encrypted hash. In the next step, feedforward the same hash without any change in number and input this number along with $X1$ and P to calculate the next value of hash and so on [48]. Here in the updated method the encrypted hash is stored and is not used in the calculation of the next hash value. In our work, we input $X1$, P with EC to generate the hash value and then again apply Elliptic Curves to generate the Encrypted hash values. This encrypted hash will then be forwarded to calculate the value of next encrypted hash. The major difference in our work with previous work of EC is that we forward the previous Hash Value as input for the next block but with varying parameters (Changed numbers) to calculate the next hash value through ECs and again apply EC instead of RSA to generate the encrypted hash value. In this way, we generate ciphers with varying parameters to achieve scalability as shown in Figure 3.5.

Most of the conventional blockchain algorithms use only one elliptic curve in place of SHA as EC provides the same levels of security, which SHA provides at lower key size, and the curves are generated with fixed hash values creating security problems. Some of the blockchain models also apply two EC's, one in the place of compression algorithm and second in the place of encryption.

Power System Technology
ISSN:1000-3673
Received: 08-11-2025 Revised: 15-02-2026 Accepted: 26-03-2026

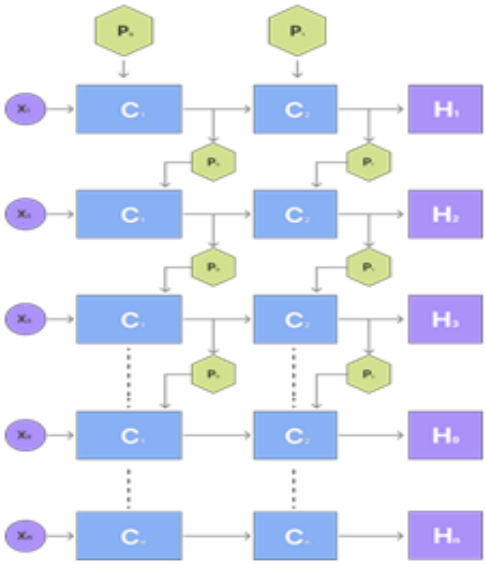

Figure 3.5. Blockchain Implementation using Elliptic Curve

However, when they generate the curves, they never change base points, which enhances the vulnerabilities to attacks. In our contribution, we use two Elliptic Curves in place of the compression algorithm and encryption algorithm but in a way that the result of the first iteration becomes the base point of the next iteration. This means our base points change for each iteration and the generated curves are attacking resistance. Changing base points makes the cipher secure as no one can find the exact parameters due to randomly changing base points, which are the hash of the previous iterations' results. The generated curves also show no singularity, which is the ideal condition for ECC. Our work is also tested through Confusion and diffusion analysis, Collision analysis, Uniform Distribution analysis, and Sensitivity Test. To make sure that EC does not have more than 1 root, $4a^3 + 27b^2 \neq 0$ and the integers a and b in this equation are authentic. An elliptic curve is defined as $y^2 = x^3 + ax + b$ if it meets the criteria that the curve possesses no more than one root, and the integers a and b are genuine. Furthermore, the elliptic curve needs a zero point, or infinity, denoted by the symbol O. This guarantees that the curve satisfies the required conditions for an elliptic curve [14].

3.5 Data Collection

This investigation employs publicly accessible IoT datasets to implement ECC on smart devices. The dataset for this study was collected from a smart greenhouse facility at Tikrit University [46]. The dataset comprises IoT sensor data from greenhouse's monitoring systems, establishing a robust basis for evaluating the effectiveness of lightweight hashing algorithms such as EC with hash. This dataset emphasizes the potential blockchain usage in IoT data, such as security, control, and real-time monitoring of the parameters. The dataset details are shown in Table 3.1.

Power System Technology
ISSN:1000-3673
Received: 08-11-2025 Revised: 15-02-2026 Accepted: 26-03-2026

Table 3.1: DETAIL OF THE DATASETS

Data	Data type	Data description
Date	datetime64	Timestamps ensure traceable, time-ordered, secure logging of IoT data on the Blockchain.
Temperature	Int64	Recorded temperature in Celsius; proper for analyzing environmental control needs.
humidity	int64	Humidity level as a percentage is valuable for environmental monitoring.
water_level	int64	Indicates the water level as a percentage, which could trigger automated responses through smart contracts.
N (Nitrogen)	int64	Soil nitrogen level (0-255 scale) could aid in monitoring soil health and crop growth.
P (Phosphorus)	int64	Soil phosphorus content (0-255 scale) is critical for ensuring consistent crop yield and tracking securely.
K (Potassium)	int64	Potassium level in soil (0-255 scale); supports environmental decision-making and record keeping.
Fan_actuator_OFF	float64	The indicator for the fan actuator's OFF state (0 or 1) allows for blockchain-stored control history.
Fan_actuator_ON	float64	Indicator for fan actuator ON state, facilitating climate control documentation on a secure ledger.
Watering_plant_pump_OFF	float64	Indicator of OFF state for plant watering pump, providing audit trail capability for irrigation actions.
Watering_plant_pump_ON	float64	ON indicator for the plant watering pump, they are enabling precise control monitoring.
Water_pump_actuator_OFF	float64	Indicates if the main water pump actuator is OFF (0 or 1), helping with blockchain-based state management.
Water_pump_actuator_ON	float64	ON indicator for the water pump actuator stores each activation on-chain for comprehensive audit trails.

3.6 Implementation Specification

The way of generating hash functions using elliptic curves for cryptography, comprising the steps:

- Take a publicly available database. The algorithm reads a line from the KM (K time M read) database.
- Get an Elliptic curve through the getcurve () function that satisfies. $y^2 = x^3 + ax + b$ equation and so on used point addition () function.
- Get the point on the elliptic curve using the get point () function and then check whether the point exits on a curve or not using the curve () function.
- Specify the basic point on the elliptic curve as the start point (x, y ε EC).
- Establish the set of coefficients (x, c, k) and base point on the curve as public information.
- Select a pair of randomly generated prime numbers, p0, p1; this pair is used as private information.
- Process a record bit string to construct a bit string that is a multiple of N bits.

Power System Technology
ISSN:1000-3673
Received: 08-11-2025 Revised: 15-02-2026 Accepted: 26-03-2026

- Compute an initial hashing point on the elliptic curve
- Using previous output as input for following curve values makes a chain of blocks of data
- Establish an integer i instead of an ith message records block set $i = 2$ and work as a loop.
- Repeating these steps pending the message numbers of blocks are processed and increment i at each step.
- Concatenating bits of the x-coordinate and the sign bit of the y-coordinate of a hashing point along with the x-coordinates and the y-coordinate of a hash point to form a hashed bit string.

We use Weierstrass curves over large prime fields (Fp) due to their better security profile over binary fields, as supported by Safe Curves. Though ECC is not quantum-proof, our adaptive base-point strategy enhances resilience against precomputation-based quantum attacks.

3.6 Scalability

In addition, our framework provides a scalable security layer, enabling the addition of ciphers for future revisions of the Blockchain. Although this approach enhances complexity and resource consumption. It also offers robust security and reduced key size, making ECC an optimal choice for blockchain technology. Security has enhanced as we implemented the application of blockchain with the help of ECC to offer guards against tampered information and unauthorized access through the Elliptic-Curve Digital Signature Technique (ECDSA) [51]. This confirms secure transactions and access controls to prevent unauthorized access to resources. While deploying this mechanism, we also monitored related resource utilization metrics, including these devices' CPU and memory consumption. We determined that the ECC-based techniques reduced resource consumption, making it an ideal approach for resource-constrained environments typically for IoT networks and mobile devices [52]. AECC supports scalable expansion as each hash block is independently computed using new base points. The configurability lies in parameter X, C, and K, which adapt to data characteristics. Flexibility comes from its modular design which is suitable for varying encryption needs and device constraints.

4. RESULTS AND DISCUSSION

This section discusses the results obtained using the proposed framework. A performance evaluation of the proposed blockchain implementation method in small-size IoT devices based on ECC with hashing is included in this analysis. The metrics investigated are storage management, computational efficiency, and security attack resistance. This research offers a comprehensive analysis and explanation of our findings. This segment also highlights the strengths, limitations, and significance of the proposed methodology in the context of IoT device applications. Our results from testing show that our proposed algorithm is much more efficient with the same level of security as RSA but with a low-key size.

4.1 Performance Metrics

To evaluate the performance of the proposed adaptive elliptic curve cryptographic algorithm, we performed several experiments. To verify the security and scalability properties of the proposed framework we performed collision analysis, uniform distribution of hash to check the bit change probability and bit flip probability. Also performed sensitivity analysis and compared computational efficiency with traditional system to measure processing time, energy and memory consumption of resource constrained devices. The presentation metrics in assessing the proposed Blockchain implementation framework using ECC with a hashing algorithm for smart devices include numerous vital aspects. They are computational competence, memory consumption,

Power System Technology
ISSN:1000-3673
Received: 08-11-2025 Revised: 15-02-2026 Accepted: 26-03-2026

attack resilience, and scalability [47]. The efficiency and appropriateness of the projected Blockchain using ECC with a hashing algorithm might be assessed by analyzing these measures, allowing for comparison with obtainable hashing techniques and identifying fields for improvement. Here, we use Elliptic curves instead of SHA 256 and RSA in a way that makes them data driven. We calculate experimental values that are ideal in results and are very close to theoretical values.

4.2 Implementation of Blockchain Using Elliptic Curves

The security of the proposed methodology evaluated using ECC and hashing. The methodology involves implementing a practical approach to resolve the problem using relevant datasets [46] and tools. The steps for generating hash functions using elliptic curves for cryptography are outlined, including taking a public database, getting an elliptic curve, specifying coefficients and base points, selecting private information, processing record bit strings, computing initial hashing points, and concatenating bits to form a hashed bit string. Overall, the methodology proposes a secure and efficient approach for data transmission in IoT devices using ECC and blockchain technology.

4.3 Confusion and Diffusion Analysis

In our experimental results shown in Table 4.1, the mean bit change is 31.9687 with a standard deviation of 4.0279 for a hash of 64 bits, which is very close to the theoretical value of 32. Moreover, the bit change probability is 0.4995 with a standard deviation of 0.0629, with 0.5 as the theoretical value. The SD value for bit changes is 4.0279 and 0.0629 is the SD value of the bit change probability. The result of the confusion and diffusion analysis after bit changes is 0.0317, approximately close to the theoretical bound, which is zero.

Table 4.1: Confusion and diffusion analysis

		Experimental Values	**Theoretical Values**
Mean of bits changed	$\bar{B}$	31.9687	32
Mean of bit change Probability	P	0.4995	0.5
SD of bits changed	ΔB	4.0279	0
SD of bit change Probability	ΔP	0.0629	0
Confusion-Diffusion Measure	*I*dc	0.0317	0

4.4 Uniform Distribution Analysis

As shown in Table 4.2, the possibility of bit flips in hash (Q) is 0.5, and our outcome is 0.5005 after uniform distribution analysis testing. The possibility of a bit flipping in hash (ΔQ) is zero; our outcome is 0.007. Here, our result shows a smaller value of 0.0005 and 0.007, which is smaller than the Q-0.5 value and shows a better avalanche effect.

Power System Technology
ISSN:1000-3673
Received: 08-11-2025 Revised: 15-02-2026 Accepted: 26-03-2026

Table 4.2: Uniform distribution analysis

	Experimental Values	Theoretical Values
Average Probability that a bit flips in hash(Q)	0.5005	0.5
|Q-0.5|	0.0005	0
SD Probability that a bit flips in hash(ΔQ)	0.007	0

Note: The smaller the |Q-0.5| and ΔQ, the better is the avalanche effect.

Figure 4.1 illustrates the distribution of bit flip probabilities to evaluate the security and efficiency of the proposed blockchain model based on elliptic curve cryptography (ECC).

The bit flip probabilities are nearly uniform across the 70 bits shown on the x-axis, indicating that the ECC-based blockchain implementation ensures consistent security properties across all data bits. Uniform distribution is very important for cryptographic systems since it represents balanced diffusion and confusion, ensuring no bit is vulnerable. The results of the average bit flip probability of 0.015625 and the low variance of 4.7413×10−8 show high stability and predictability in our proposed cryptographic system.

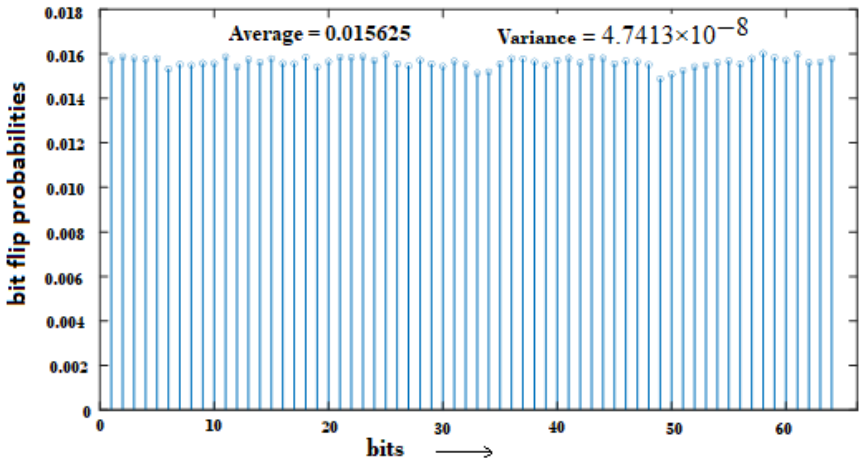

Figure 4.1. Distribution of bit flips

This result demonstrates the system's ability to maintain consistent behavior across different data inputs, necessary for robust cryptographic security. The uniformity and low variance also demonstrate that the algorithm exhibits resistance to vulnerabilities such as collision and sensitivity attacks, which are prevalent issues in blockchain-based systems. We validate the efficiency of the developed ECC algorithm in MATLAB and its application to IoT datasets with these results. By combining elliptic curves with dynamic parameters replacing RSA, the system generates a strong, evenly distributed hash output with no detectable patterns [49]. It shows increased diffusion and confusion strength, collision resistance, and high sensitivity. Integrating elliptic curve cryptography enhances the adaptability and scalability of the blockchain while also providing a strong solution to securely keep records or manage data in IoT applications [21].

Power System Technology
ISSN:1000-3673
Received: 08-11-2025 Revised: 15-02-2026 Accepted: 26-03-2026

These findings validate the objective of our research work to tackle critical issues in blockchain technology, such as fixed-length hash parameters, computational power, and limited scalability [49] while providing a transparent, decentralized, and secure framework.

4.5 Sensitivity Analysis

The robustness of the proposed elliptic curve cryptography (ECC) based blockchain model in IoT applications is demonstrated by sensitivity analysis shown in Figure 4.2. The changes in input parameters (such as initialization values, curve parameters, and messages) are highlighted with red marks indicating the high sensitivity of the algorithms. This behavior aligns with the avalanche effect and reflects the cryptographic systems' unpredictability, one of the important properties of strong encryption [48]. Over the course of subsequent rows, the increasingly denser deviations emphasize the model's flexibility and resistance to attack pattern predication, as even small changes in input observed profound changes in output, increasing security. The proposed methodology of varying ECC parameters and hashing techniques to build a blockchain of elliptic curves is validated by these results. This confirms the claims in the abstract that the model guarantees strong cryptographic strength and high sensitivity, and thus improved diffusion and confusion.

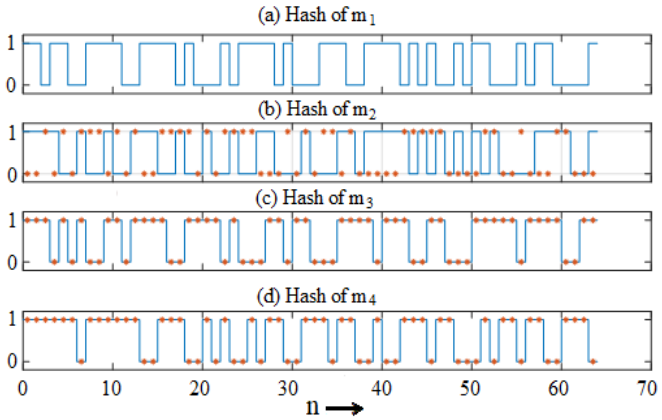

FIGURE 4.2. Sensitivity Analysis

Through integrating dynamic elliptic curve parameters and a different RSA based hashing approach, the research achieves a scalable, secure, and decentralized framework for IoT applications. The findings demonstrate that the algorithm can provide secure and efficient record keeping for IoT with its development of blockchain solutions specific to IoT's needs.

In Sensitivity analysis, we randomly select a record called m1 from the dataset and generate a hash of this record. The Probability of bit changes in this analysis is shown in the form of 1 and 0. Next, we randomly flipped a bit from $m1$ and got the resultant hash as $m2$. Then, from $m1$, 1 bit is deleted randomly, and the hash of m3 is gat. We were similarly inserting one bit randomly into the m1 results in m4. In this figure, the red area shows the difference from the hash of m1 to the hash of $m2$, the difference of the hash of $m2$ to $m3$, and so on.

As shown in Table 4.3, we have used theoretical bounds as reference criteria for the sensitivity analysis of our encryption system. The resulting values of the samples are as follows: the mean of the bit flipped is 0.4995, the mean of the bit inserted is 0.4989, and the bit deleted is 0.4985, with the comparison of the theoretical value of 0.5. We got values of variance as 0.004, 0.0038, and 0.0039, approximately equal to the theoretical value 0.

Power System Technology
ISSN:1000-3673
Received: 08-11-2025 Revised: 15-02-2026 Accepted: 26-03-2026

Table 4.3: COMPARISON OF SENSITIVITY ANALYSIS

	Experimental Values			**Theoretical Values**		
	Bit flipped	Bit inserted	Bit deleted	Bit flipped	Bit inserted	Bit deleted
Mean	0.4995	0.4989	0.4985	0.5	0.5	0.5
Variance	0.004	0.0038	0.0039	0	0	0

5 Collision Analysis

Figure 4.3 compares the expected and actual outcomes of applying elliptic curve cryptography (ECC) in IoT blockchain applications. The theoretical distribution represents the ideal cryptographic behavior, while the experimental distribution reflects the actual performance of the proposed ECC-based blockchain algorithm. The experimental results likely demonstrate improved cryptographic properties, such as enhanced diffusion, confusion, uniform hash distribution, and resistance to collisions, aligning closely with the theoretical expectations. It suggests that the new approach offers better security and cryptographic strength than traditional methods like RSA [9]. Additionally, the experimental results validate the Scalability and efficiency of the proposed method. The algorithm can handle larger datasets, and more IoT devices, with reduced computational time, which is confirmed by replacing RSA with elliptic curve schemes in the approach [13]. The close match between the theoretical and experimental distributions supports the claim that ECC with varying parameters enhances security and Scalability, providing a robust solution for secure, decentralized IoT applications. In the Collision analysis, we Compare two different Hashes and then check the similarity between two hash values.

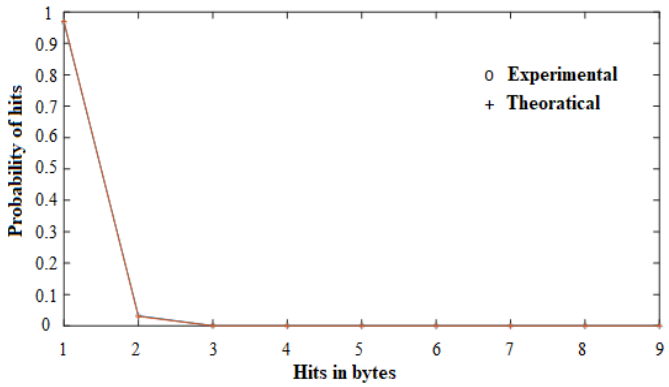

FIGURE 4.3. Comparison between experimental and theoretical probability distributions

We get the value of D = 9.3596e-05 and mean Δbyte = 81.1050, whereas the Theoretical value of mean Δbyte = 85.33. The resultant probabilities of our experiments are 0.000093596 Bhattacharyya distance from the theoretical bounds. This value shows the results of our evaluation and assessment of the EC hashing algorithm applied to smart devices. The EC-based

Power System Technology
ISSN:1000-3673
Received: 08-11-2025 Revised: 15-02-2026 Accepted: 26-03-2026

Hash algorithm generates cipher values consuming little memory as compared to other complex algorithms, making it suitable to operate efficiently on smart IoT devices with limited memory resources [5]. This research also provides comprehensive details on the performance of the ECC-based hashing algorithm, its limitations, and the practical implications of this algorithm for smart digital devices. This reveals its utilization in proficient and protected data integrity verification for reliable, private, and safe ECC-based smart monitoring systems.

4.6 Comparative Analysis of ECC vs RSA and SHA 256 in IoT security

To evaluate the performance and efficiency of the proposed hashing algorithms in smart devices, a comparison is made with existing hashing techniques. This quantitative comparative analysis, given in Table 4.3, helps highlight the unique features, advantages, and limitations of the proposed algorithm [53], [54], [55].

Key size and Security: According to the performance comparison, shown in Figure 4.4, the ECC provides the same level of security as RSA, or SHA 256 but at a lower key size (256 bits) which makes it more suitable for low power IoT devices. Similarly, the security issues of fixed length hashing of SHA 256 can be avoided through ECC which improves adaptability. In AECC the base point G is not known and therefore initialization parameter changes from record to record and therefore generated curves are attack resistant.

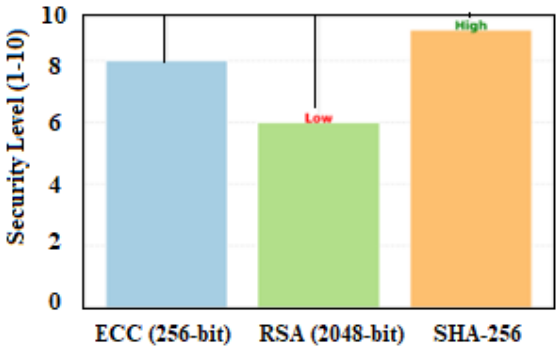

FIGURE 4.4. Security comparison between ECC, RSA and SHA 256

Computational Complexity: The computational time comparison given in Figure 4.5 shows that the encryption speed of ECC is much faster than RSA while maintaining the same level of security. Therefore, AECC improves the blockchain verification speed; here we computed double time of computation as we applied two Elliptic curves.

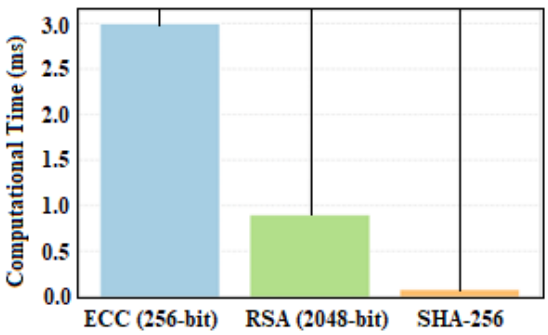

FIGURE 4.5. Computational Time comparison

Power System Technology
ISSN:1000-3673
Received: 08-11-2025 Revised: 15-02-2026 Accepted: 26-03-2026

The ECC method shows faster encryption speed compared to RSA which is 1.5 ms for single EC operation and 3 ms for double EC operation at 256 bits (lower key size). A 2048-bit RSA needs 0.6 -2 ms but at a higher computational complexity due to its large key size and heavy encryption operation. Meanwhile, SHA 256 is lightweight in computation, but it lacks encryption capabilities. Therefore, ECC reduces encryption time and maintains high security, which is ideal for an IoT environment that needs fast processing and low energy consumption.

Sensitivity: According to Table 4.4, AECC shows 0.4995-bit change probability and 0.007-bit flip uniformity, refers to a strong avalanche effect. This result depicts that AECC is more suitable for cryptographic security as it has higher confusion and diffusion but ideal variance while comparing with SHA 256 (very high variance).

Table 4.4: Comparative analysis

Performance Metrics	AECC Hash	RSA (2048-bit)	SHA-256
Key Size (bits)	256	2048	256
Security per Bit	High	Medium	High (hashing, not encryption)
Computational Time (ms)	1.5 ms for double EC 3 ms	0.6 – 1.2 ms	0.08 – 0.1 ms
Bit Change Probability	0.4995 (ideal 0.5)	-	0.48 - 0.50
Bit Flip Variance	0.007 (ideal 0)	-	0.01 - 0.02
Collision Resistance	Strong (0.0000935 probability)	Medium	Strong
Scalability	High (variable key size)	Low (fixed key size)	Medium (fixed-length hash)

Scalability: The comparative outcomes depicted in Figure 4.6 show that the AECC is more scalable than RSA, and SHA 256 because it requires smaller key sizes. The EC based hashing shows high scalability, reducing performance issues of fixed length hash parameters with varying parameters, which helps in preventing from attacks.

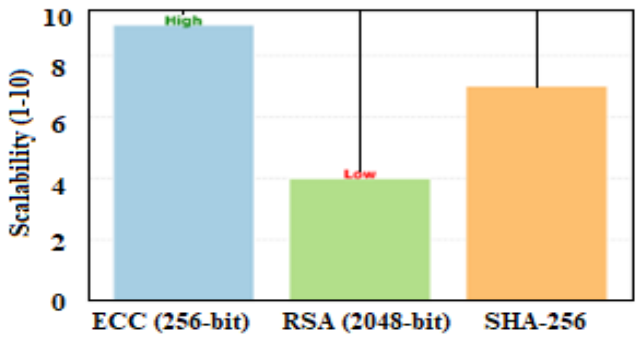

FIGURE 4.6. Scalability comparison

Power System Technology
ISSN:1000-3673
Received: 08-11-2025 Revised: 15-02-2026 Accepted: 26-03-2026

DISCUSSION

Our Adaptive Elliptic Curve Cryptography (AECC) framework addresses three fundamental weaknesses of conventional blockchain infrastructure in IoT: (1) static hash vulnerabilities, (2) RSA-based computational inefficiency, and (3) scalability bottlenecks. By replacing SHA-256 and RSA with a two-layer ECC scheme that utilizes data-driven base points (G), we achieve enhanced security with respect to 'quantum resistance' and 'collision resilience'. For the former, unlike traditional ECC (with a fixed G), our dynamic base point scheme forces the attackers to perform an infinite search problem ($YA = XA \times G$) and thus makes brute-force and quantum attacks impractical. For the latter, experimental results confirm robust diffusion/confusion (0.0317), close-to-ideal bit-flip uniformity (0.5005 ± 0.007), and sensitivity (0.4995), superior to static hashing schemes like SHA-256.

Further, from the perspective of computational efficiency, AECC offers quicker processing and scalability. AECC reduces latency by 3× compared to RSA (256-bit ECC vs. 3072-bit RSA for an equivalent security level) with less energy consumption that is critical for IoT devices.

In scalability, the iterative "hash-forward" architecture (where the output of one block seeds the base point of the subsequent block) eliminates fixed-parameter bottlenecks and enables linear scaling of performance.

The operational feasibility of AECC includes Resource Optimization and robustness. AECC's smaller key sizes (256-bit) reduce memory/CPU overhead, which is illustrated using real IoT datasets (Section III.E). Dual-layer ECC and dynamic G provide two-layer protection against tampering and quantum attacks, meeting IoT blockchain integrity and flexibility requirements. Considering the comparative advantages, the AECC reaches RSA's security using 12× smaller keys (Table 7) at higher speed encryption (1.5 ms vs. 2 ms for 2048-bit RSA). Despite the lightweight SHA-256, our AECC includes encryption functions without compromising hashing efficiency (Figure 9).

This framework can be directly integrated into smart agriculture, smart homes, and healthcare IoT systems where lightweight, secure communication is essential. It can also serve as a model for post-quantum cryptography in edge computing environments. We demonstrate that AECC is an efficient replacement for traditional cryptography in IoT-blockchain applications. Our method, while computationally efficient, requires parameter tuning for each device context, which may add pre-deployment complexity. Additionally, hardware validation on constrained devices remains as future work. Future work will explore: (i) integrating post-quantum ECC variants such as isogeny-based cryptography, (ii) FPGA-based acceleration, and (iii) implementation across real-world smart cities and healthcare ecosystems. Moreover, recent FPGA-based and ASIC hardware accelerators [EC-Crypto 2023, E2CSM 2023, DCryp-Unit 2023] will be explored to enhance AECC performance on edge nodes.

5. CONCLUSION

In this work, we presented an Adaptive Elliptic Curve Cryptography (AECC) framework that handles the critical challenges in IoT blockchain systems, such as fixed hash vulnerabilities, inefficiency in computations, and quantum attack susceptibility. Through the usage of two-layer ECC based on dynamically generated base points (G), our system improves security with scalability for resource-constrained IoT devices. Our major contribution includes quantum-resistant design in which randomized base points avoid attacks against fixed parameters by attackers, securing against quantum threats. Our second contribution is in computational efficiency, where the experimental outcomes show near-ideal confusion/diffusion (0.0317), balanced distribution (0.5005 bit-flip probability), and 3x faster processing compared to RSA at the same levels of security. Our third contribution is in scalability in which dynamic

Power System Technology
ISSN:1000-3673
Received: 08-11-2025 Revised: 15-02-2026 Accepted: 26-03-2026

parameterization eliminates fixed-hash bottlenecks, enabling seamless integration with IoT blockchain networks. Moreover, the proposed framework provides stronger security than conventional RSA and SHA-256, uses less energy, and is more adaptable, making it a promising solution for future IoT-blockchain applications. Post-quantum optimizations and large-scale deployment in real-world IoT ecosystems will be pursued in future work. In conclusion, our proposed framework addresses the problems of existing blockchain-based systems in IoT networks, promising a scalable, robust, and computationally efficient solution for upcoming blockchain-based IoT applications.

REFERENCES

[1] Z. Ruan, "Blockchain Technology for Security Issues and Challenges in IOT," 2023, pp. 572-580.

[2] A. H. R. P. S. R. S. S. K. Mohd Javaid, "A review of Blockchain Technology applications for financial services," BenchCouncil Transactions on Benchmarks, Standards and Evaluations, vol. 2, no. 3, 2022.

[3] IBM, "What is the Internet of Things (IoT)?," [Online]. Available: https://www.ibm.com/topics/internet-of-things. [Accessed 1 2025].

[4] A. A. L. Z. A. S. Z. D.-P. S. K. Abdullah Ayub Khan, "Internet of Things (IoT) Security With Blockchain Technology: A State-of-the-Art Review," vol. 10, pp. 122679-122695, 2022.

[5] M. G. A. L. Mohammad Salah Uddin, "Long range robot teleoperation system based on internet of things," in 2017 2nd International Conference on Computer and Communication Systems (ICCCS), 2017, pp. 163-167.

[6] R. X. L. L. Rui Zhang, "Security and Privacy on Blockchain," ACM Computing Surveys (CSUR), vol. 52, no. 3, pp. 1-34, 3 7 2019.

[7] A. S. S. V. Nitin Jirwan, "Review and analysis of cryptography techniques," International Journal of Scientific and Engineering Research, vol. 4, pp. 1-6, 3 2013.

[8] Kinza-Yasar. [Online]. Available: https://www.techtarget.com/searchdatamanagement/definition/hashing.

[9] A. K. Yadav, "Significance of Elliptic Curve Cryptography in Blockchain IoT with Comparative Analysis of RSA Algorithm," 12 4 2021.

[10] M. A. S. Basant Kumar, "A Review on Elliptic Curve Cryptography," march 2021.

[11] X. Lin, "The application of Elliptic Curve Cryptography in Electronic Commerce," in 2012 IEEE Symposium on Electrical & Electronics Engineering (EEESYM), IEEE, 2012, pp. 547-549.

[12] Y. L. H. C. Ping Zhang, "An Elliptic Curve Signcryption Scheme and Its Application," Wireless Communications and Mobile Computing, vol. 2022, 2022.

[13] D. K. S. Vaisla, "A Lightweight Signcryption Scheme based on Elliptic Curve Cryptography," Proceedings of First International Conference on Advances in Computing & Communication Engineering (ICACCE-2014), vol. 1, pp. 7-10, 02 2014.

Power System Technology
ISSN:1000-3673
Received: 08-11-2025 Revised: 15-02-2026 Accepted: 26-03-2026

[14] Elif Hilal Umucu, "Elliptic Curve Cryptography in Blockchain Technology," SSRN Electronic Journal, 14 2 2022.

[15] S. e. a. Chanda, "An Elliptic Curve Menezes–Qu–Vanston-Based Authentication and Encryption Protocol for IoT," Wireless Communications and Mobile Computing 2024, p. 14, 2024.

[16] S. B. R. K. U. Arya Kharche, "Implementation of blockchain technology in integrated IoT networks for constructing scalable ITS systems in India," Blockchain: Research and Applications, vol. 5, no. 2, 2024.

[17] M. A. R. M. R. A. K. Vishal A. Thakor, "Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities," IEEE Access, vol. 9, pp. 28177-28193, 2021.

[18] H. Zhang, C. T. L. T. Jia Yu and L. G. Jie Lin, "Efficient and Secure Outsourcing Scheme for RSA Decryption in Internet of Things," IEEE Internet of Things Journal, vol. 7, no. 8, pp. 6868-6881, 2020.

[19] M. W. Ashok Kumar Das and M. K. K. K.-K. R. C. Y. P. Neeraj Kumar, "Design of Secure and Lightweight Authentication Protocol for Wearable Devices Environment," IEEE Journal of Biomedical and Health Informatics, vol. 22, no. 4, pp. 1310-1322, 2018.

[20] M. D. S. R. K. Sowjanya, "Elliptic Curve Cryptography based authentication scheme for Internet of Medical Things," Journal of Information Security and Applications, vol. 58, p. 102761, 5 2021.

[21] M. K. R. A. S. R. S. B. G. C. V. M. S. R. Chetan Chauhan a, "Improving IoT Security Using Elliptic Curve Integrated Encryption Scheme with Primary Structure-Based Block Chain Technology," Procedia Computer Science, vol. 215, pp. 488-498, 2022.

[22] S. V. B. C. G. C. M. P. A. C. J. R. Arunkumar, "Logistic Regression with Elliptical Curve Cryptography to Establish Secure IoT," Computer Systems Science and Engineering, vol. 45, no. 3, pp. 2635-2645, 2023.

[23] F. a. S. H. Kabashi, "Implementation of Elliptic Curve Digital Signatures in Blockchain for Management of Certificates in Higher Education," Journal of Engineering And Applied Science Technology, pp. 1-6, 06 2023.

[24] S. J. M. Y. A. V. K. M. A. Adesh Kumari, "ESEAP: ECC based secure and efficient mutual authentication protocol using smart card," Journal of Information Security and Applications, vol. 51, 2020.

[25] Y. a. L. J. a. F. D. a. W. W. a. W. M. a. W. W. Fu, "RegKey: A Register-based Implementation of ECC Signature Algorithms Against One-shot Memory Disclosure," ACM Trans. Embed. Comput. Syst., vol. 22, no. 6, pp. 1-22, 2023.

[26] A. H. N. S. F. A. Fatma Mallouli, "A Survey on Cryptography: Comparative Study between RSA vs ECC Algorithms, and RSA vs El-Gamal Algorithms," 2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/ 2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom), pp. 173-176, 2019.

Power System Technology
ISSN:1000-3673
Received: 08-11-2025 Revised: 15-02-2026 Accepted: 26-03-2026

[27] W. L. Y. Z. C. C. Z. C. Yong Xiao, "A High-Speed Elliptic Curve Cryptography Processor for Teleoperated Systems Security," Mathematical Problems in Engineering, vol. 2021, pp. 1-8, 01 2021.

[28] A. A.-a.-K. A. Dina.H. Abbas, "Elliptic Curve Cryptosystem for Digital multimedia, General Review," Al-Salam Journal for Engineering and Technology, vol. 2, no. 2, pp. 63-71, 2023.

[29] A. C. H. Chen, "Using Elliptic Curve Cryptography for Homomorphic Hashing," 2023 International Conference on Smart Systems for applications in Electrical Sciences (ICSSES), pp. 1-5, 2023.

[30] G. C. C. F. P. P. S. L. M. B. Javad Doliskani, "Faster Cryptographic Hash Function From Supersingular Isogeny Graphs," in IACR Cryptology ePrint Archive., 2017.

[31] M. R. M. A. A. Y. N. S. H. Y. K. Md Sunjim Hossain, "A Smart Contract Based Blockchain Approach Integrated with Elliptic Curve Cryptography for Secure Email Application," pp. 195-201, 11 2023.

[32] P. K. Vidya Rao, "Light-weight hashing method for user authentication in Internet-of-Things," Ad Hoc Networks, vol. 89, pp. 97-106, 6 2019.

[33] A. C. ,. S. L. A. N. Jihane Jebrane, "Elliptic Curve Cryptography with Machine Learning," Cryptography, vol. 9, no. 1, 2025.

[34] S. L. Y. A. A. N. Younes Lahraoui, "Securing Data Exchange with Elliptic Curve Cryptography: A Novel Hash-Based Method for Message Mapping and Integrity Assurance," Cryptography, vol. 8, no. 2, 2024.

[35] M. T. D. F. A. Jeremy B. Maitin-Shepard, "Elliptic Curve Multiset Hash," The Computer Journal, vol. 60, no. 4, pp. 476-490, 2016.

[36] M. Kumar, "Design and Analysis of Pairing-Friendly Elliptic Curves for Cryptographic Primitives," arXiv preprint arXiv:2307.09610, 2023.

[37] A. I. S. I. O. P. Y. M. Svitlana Kazmirchuk, "The Improvement of Digital Signature Algorithm Based on Elliptic Curve Cryptography," Advances in Intelligent Systems and Computing, vol. 1247, 2021.

[38] J. O. Felipe Tellez, "Comparing AI Algorithms for Optimizing Elliptic Curve Cryptography Parameters in e-Commerce Integrations: A Pre-Quantum Analysis," arXiv:2310.06752, 2023.

[39] H. O. W. C. M. C. R. I. G. L. &. F. V. Kohei Nakagawa, "SQIsign2D-East: A New Signature Scheme Using 2-Dimensional Isogenies," in International Conference on the Theory and Application of Cryptology and Information Security., Singapore, 2024.

[40] M. A. R. J. M. A. S. A. I. a. J. P. Olusogo Popoola, "An optimized hybrid encryption framework for smart home healthcare: Ensuring data confidentiality and security," Internet of Things , vol. 27, 2024.

[41] B. P. O. Sharad Kumar Verma, "A Discussion on Elliptic Curve Cryptography and Its Applications," International Journal of Computer Science Issues, vol. 9, 2012.

[42] S. P. K. S. S. Y. M. a. J. H. P. Singh, "Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions," Journal of Ambient Intelligence and Humanized Computing, pp. 1-18, 2024.

Power System Technology
ISSN:1000-3673
Received: 08-11-2025 Revised: 15-02-2026 Accepted: 26-03-2026

[43] D. Koshelev, "Simultaneously simple universal and indifferentiable hashing to elliptic curves.," Cryptology ePrint Archive, 2024.

[44] M. J. A. K. P. Patil, "An Enhanced Elliptic Curve Cryptography Scheme for Secure Data Transmission to Evade Entailment of Fake Vehicles in VANET," Cybernetics and Systems, vol. 55, pp. 2405-2439, 6 11 2024.

[45] L. B. L. C. P. N. L. F. S. S. Stefano Di Matteo, "Secure Elliptic Curve Crypto-Processor for Real-Time IoT Applications," Energies, vol. 14, p. 4676, 2021.

[46] W. Abdullah, "IoT Agriculture 2024," [Online]. Available: https://www.kaggle.com/datasets/wisam1985/iot-agriculture-2024.

[47] R. M. S. R. K. V. V. R. S. Velliangiri and P. Karthikeyan, "An Efficient Lightweight Privacy-Preserving Mechanism for Industry 4.0 Based on Elliptic Curve Cryptography," IEEE Transactions on Industrial Informatics, vol. 18, no. 9, pp. 6494-6502, 9 2022.

[48] D. Jao, "Elliptic Curve Cryptography," in Handbook of Information and Communication Security, Berlin, Heidelberg, Springer Berlin Heidelberg, 2010, pp. 35-57.

[49] J. Z. N. D. M. T. H. F. U. M. Y. Shamsher Ullah, "Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey," Computer Science Review, vol. 47, p. 100530, 2 2023.

[50] H. F. T. A. R. A. Sondes Baccouri, "Lightweight authentication scheme based on Elliptic Curve El Gamal," Journal of Information and Telecommunication, vol. 8, no. 2, pp. 231-261, 2 4 2024.

[51] A. S. A. M. T. A. M. A. R. Mohamed Ali Shaaban, "Efficient ECC-based authentication scheme for fog-based IoT environment," International journal of Computer Networks & Communications, vol. 15, no. 4, pp. 55-71, 27 7 2023.

[52] Y. N. R. Mahaboob Basha Shaik, "Secret Elliptic Curve-Based Bidirectional Gated Unit Assisted Residual Network for Enabling Secure IoT Data Transmission and Classification Using Blockchain," IEEE Access, vol. 12, pp. 174424 - 174440, 2024.

[53] D. K. Y. Dindayal Mahto, "RSA and ECC: A Comparative Analysis," International Journal of Applied Engineering Research, vol. 12, no. 19, pp. 9053-9061, 2017.

[54] J. Mao, "The Evolution of Digital Signature Technologies in Mobile Devices," in International Conference on Data Science and Engineering, 2024.

[55] O. İşler, "Implementation and Performance Evaluation of Elliptic Curve Cryptography over SECP256R1 on STM32 Microprocessor," in Cryptology ePrint Archive, 2024.

[56] S. L. Y. A. A. N. Younes Lahraoui, "Securing Data Exchange with Elliptic Curve Cryptography: A Novel Hash-Based Method for Message Mapping and Integrity Assurance," Cryptography, vol. 8, no. 2, p. 23, 2 6 2024.