

# Enhancing internet of things security and efficiency through advanced elliptic curve cryptography-based strategies in fog computing

Krishnapura Srinivasa Ravindra<sup>1,2</sup>, Malode Vishwanatha Panduranga Rao<sup>3</sup>

<sup>1</sup>Department of Electronics Engineering, Faculty of Engineering and Technology, JAIN (Deemed-to-be University), Bengaluru, India

<sup>2</sup>Department of Electronics and Communication Engineering, Nitte Mahalinga Adyanthaya Memorial Institute of Technology (Deemed to be University), Karkala, India

<sup>3</sup>Department of Computer Science and Engineering, Faculty of Engineering and Technology, JAIN (Deemed-to-be University), Bengaluru, India

## Article Info

### Article history:

Received Oct 21, 2023

Revised Jan 24, 2024

Accepted Feb 10, 2024

### Keywords:

Coefficient of correlation

Computational cost

Elliptic curve cryptography

Fog computing

Internet of things

## ABSTRACT

Fog computing (FC) has evolved as a significant paradigm within the internet of things (IoT) ecosystem, serving as a crucial link between edge devices and centralised cloud computing resources. This research paper investigates advanced methodologies for improving the security and efficiency of FC in the IoT domain. The primary emphasis is placed on the utilisation of elliptic curve cryptography (ECC) to accomplish these goals. This study examines the difficulties encountered in ensuring the security of IoT deployments based on FC. It also presents novel solutions based on ECC to mitigate these obstacles. Moreover, this study investigates techniques for enhancing the efficiency and allocation of resources in IoT applications within a FC environment. This study seeks to offer significant insights into the application of ECC-based techniques for enhancing the security and efficiency of FC in the context of the IoTs. These insights are derived through a combination of theoretical analysis and practical implementations. To evaluate the effectiveness of the proposed system, an analysis is conducted to examine the encryption time, decryption time, and correlation coefficients. These metrics are then compared to those of existing state-of-the-art approaches.

*This is an open access article under the [CC BY-SA](#) license.*



## Corresponding Author:

Krishnapura Srinivasa Ravindra

Department of Electronics and Communication Engineering

Nitte Mahalinga Adyanthaya Memorial Institute of Technology (Deemed to be University)

Nitte, Karnataka 574110, India

Email: ravindraks@gmail.com

## 1. INTRODUCTION

Fog computing (FC) is a game-changing paradigm in IoTs, offering a novel way to overcome the constraints and issues of traditional cloud-centric architectures [1]. FC uses a decentralised network of edge devices and intermediary processing nodes near the data source, unlike cloud computing, which sends data to distant data centres. This network's strategic placement enables real-time edge data processing, analysis, and decision-making [2]. This reduces delay and bandwidth and improves system response time. FC fits the diverse and ever-changing characteristics of internet of things (IoT) installations. IoT devices consistently generate large amounts of data. Sensors in smart cities, wearable health monitors, and industrial applications generate this data [3]. The proximity of FC to these devices allows data filtration, consolidation, and preprocessing before transferring only relevant data to the cloud. This optimises network resources and reduces data transfer costs. FC also improves IoT ecosystem security and privacy by reducing data exposure to threats during

transmission to remote cloud servers [4]. It improves critical application response time and IoT system performance in intermittent connections by enabling local processing and decentralised decision-making. Security and efficiency are significant in the context of FC, as they play a critical role in guaranteeing the dependability, feasibility, and triumph of IoTs implementations. The computing paradigm, which expands the possibilities of cloud computing to the periphery of the network, introduces distinct obstacles and prospects within various domains.

The inherent dispersed configuration and close alignment with the actual environment of a FC contribute to the emergence of a diverse set of security challenges. The imperative to uphold the confidentiality, integrity, and availability of data within the FC environment assumes heightened importance for a multitude of compelling reasons. The intricate interplay of these factors underscores the critical need for robust security measures to safeguard the sensitive information, ensuring that it remains protected against potential threats and vulnerabilities that may arise in the dynamic and decentralized landscape of a field area controller.

Data privacy, fog nodes (FNs) play a pivotal role in the intricate process of handling and analyzing sensitive data sourced from IoT sensors. This encompassing responsibility involves the processing not only of personal health information but also extends to industrial sensor data. It is imperative to underscore that any untoward incident, such as a data breach within this intricate network, possesses the inherent risk of compromising individual privacy. Such breaches not only have the potential to infringe upon the confidentiality of personal and industrial data but may also give rise to legal ramifications and consequences [5]. Cyberattacks, the heightened proximity of nodes to the network's periphery significantly amplifies the potential attack surface, thereby exposing the FNs to a diverse array of cyber threats [6]. Given this expanded vulnerability, it becomes imperative to prioritize the implementation of robust measures aimed at fortifying these nodes against malicious entities. The paramount objective is to secure and safeguard these foundational nodes, a critical imperative to uphold and maintain the overall integrity of the system. Real-time threat mitigation, the expeditious detection and mitigation of security hazards arising from FC environments is imperative, as any delay in responsive actions may precipitate substantial financial ramifications or the compromise of critical information assets. It is paramount for computing systems to possess the capability to promptly identify and counteract potential threats within the realm of fog security, ensuring the safeguarding of valuable data and the prevention of costly adversities [7].

Efficiency is essential in FC for several reasons: i) Latency reduction, the primary and crucial goal of FC revolves around the reduction of latency through the localized processing of data near its source. This essential objective is intricately tied to the proficient handling and decision-making processes at the edge, particularly in scenarios where swift responses are imperative. This is particularly evident in applications with stringent real-time requirements, such as autonomous vehicles and industrial automation, where the expeditious execution of computations at the edge plays a pivotal role in ensuring prompt reactions to dynamic environmental conditions and operational needs. Therefore, the efficacy of FC is contingent upon its ability to optimize data manipulation and decision-making at the edge, thereby minimizing latency and enhancing overall system responsiveness [8]; ii) resource utilization, IoT devices often come with limitations in terms of computing power and energy resources. The optimization of resource utilization in FC ensures the effective functioning of these devices, thereby reducing the strain on their limited capabilities. This optimization strategy plays a crucial role in enhancing the overall efficiency of IoT devices by carefully managing and maximizing the use of their constrained computing and energy resources, ultimately leading to improved performance, and minimized operational burdens [9]; and iii) cost optimization, the effective deployment of FC holds the promise of generating cost efficiencies by mitigating the need for extensive high-bandwidth data transfers to centralized cloud infrastructure [10]. This optimization in data transmission not only stands to yield economic benefits but may also result in a consequential reduction in associated expenses linked to cloud services. The relationship between security and efficiency in FC is highly interconnected. Achieving an appropriate equilibrium between these two variables is crucial to establish a robust, adaptable, and economically efficient IoTs ecosystem. Advanced methodologies, such as elliptic curve cryptography (ECC), play a crucial role in attaining this equilibrium by augmenting security measures while simultaneously reducing computing burdens [11].

The use of elliptic curve (EC) equation ( $y^2 = x^3 + ax + b$ ) inside finite fields is a fundamental aspect of ECC. The inherent algebraic features of these curves facilitate the implementation of secure encryption, digital signatures, and key exchange protocols. ECC is distinguished by several significant advantages, the ECC algorithm uses shorter key lengths than other cryptographic methods to increase security. This method reduces computational and memory needs, making it ideal for IoT sensors with limited resources. The broad application of ECC in numerous sectors, such as secure communication protocols (e.g., TLS and HTTPS), digital signatures, and safeguarding data in IoT ecosystems, may be attributed to its flexibility and security [12].

The relevance of this work lies in its exploration of sophisticated ECC-based strategies for enhancing the security and efficiency of FC in the context of the IoTs. This research contributes to the wider domain of secure and efficient implementations of IoT. The study's authors collaborated to conduct a thorough investigation of advanced strategies based on ECC for enhancing the security and optimisation of FC in the context of the IoTs.

## 2. BACKGROUND

This section aims to comprehensively examine the existing literature, offering a historical contextualization of developments and crucial background insights essential for a nuanced understanding of the forthcoming challenges and opportunities. The selected papers within this review span topics such as IoT security, FC, cryptography, and optimization, contributing valuable perspectives to the evolving landscape. Particularly in FC-based IoT systems, the nexus of security and efficiency emerges as increasingly pivotal. This literature review not only lays the groundwork for comprehending the current state of affairs but also serves as a precursor to the innovative insights and solutions that this research study endeavors to contribute.

### 2.1. Related works

Confidentiality, integrity, and availability (CIA) are the three pillars of information security [13]. Cryptography schemes guarantee the privacy and authenticity of transmitted data. Asymmetric cryptography is one such method; it employs both public and private keys [14]. The sender utilizes the receiver's public key to encrypt the plaintext before sending it. Anyone can use this key because it's been made public. The private key, on the other hand, is only known by the receiver and is used to decrypt the cypher text that has been sent to them. When using short keys, ECC is just as secure as the Rivest–Shamir–Adleman (RSA) algorithm [15]. Therefore, ECC has become the method of choice for dealing with crucial size issues and keeping performance steady in confined settings [16]. In 1987, Koblitz [17] presented the first curve for use in ECC. After the asymmetric approach generated the shared key with ECC, the symmetric approach encrypted plain text with advanced encryption standard (AES) [18]. However, many of these systems did not explain the ECC ciphering procedure, including converting encoding values to numbers, and using them in the mapping stage. Many methods have been proposed to improve key ECC encryption processes; however, the literature is still lacking. The schemes in [19] use ECC, although it is unclear how the raw text was encoded and transferred to the curve. Most improvements to such methods prioritise speed above security. ECC has efficient and quick scalar multiplication algorithms [20]. The schemes hide the original text in numerous ways. For each character, the American standard code for information interchange (ASCII) table can derive its decimal value [21]. This "Hello" would be unencoded as "72" "101" "108" "108" "111". Mapping these values onto the EC creates a cypher text. DeoxyriboNucleic Acid (DNA)-based ECC inspired [22]'s IoT encryption.

### 2.2. Preliminaries on elliptic curve cryptography for fog computing based internet of things

There are several IoT-based intelligent applications, including smart water management, healthcare systems, and grid technology. Due to IoTs, massive amounts of data have been generated, causing data explosions [23]. When using cloud computing for data processing and storage, real-time access, latency, and network bandwidth limits must be addressed. FC is a new computing paradigm that addresses this issue [24]. FC extends cloud services to the network edge, improving low-latency, mobility, network capacity, security, and privacy. Figure 1 depicts FC architecture. Three layers make up the architecture: end device, fog, and cloud computing. Smart sensors are strategically placed in the end device layer (EDL) to monitor and detect a variety of attributes based on application parameters. EDLs include low-resource devices. Due to resource restrictions, device layer security research is growing. FNs form fog. The fog layer's core is the FN [25]. Intelligent end devices are linked to FNs.

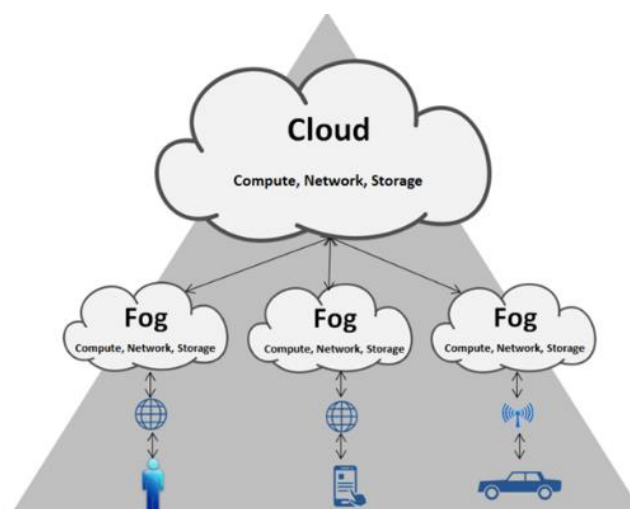


Figure 1. Architecture of FC

Examining data security from the EDL to the FNs is a critical area of study. When it comes to the transmission of data between smart end devices and FNs, several pivotal security considerations come to the forefront, including confidentiality, integrity, data freshness, and authentication. Maintaining the secrecy of sensor data is imperative, as it restricts access to the intended recipient [26]. In the event of communication exchanges being intercepted and monitored by unauthorized individuals, it becomes imperative to implement robust measures to safeguard the data, ensuring its confidentiality and preventing decipherment. The implementation of encryption and decryption mechanisms plays a vital role in upholding and enforcing the confidentiality of the transmitted data during its journey from the EDL to the FNs.

### 2.3. Significance of lightweight cybersecurity for fog based internet of things

For IoTs deployments, lightweight cybersecurity is crucial. As IoT devices proliferate across industries and fields, so does the need for strong security protocols. To overcome IoT challenges and constraints, lightweight cybersecurity techniques have many benefits. Insufficient funding is an early and persistent IoT deployment issue. Many IoT devices lack power, storage, and processing. Traditional cybersecurity methods work well in robust systems but may be too expensive on resource-constrained devices, resulting in lower performance, higher power consumption, or operational failures. In contrast, lightweight methods provide safety with low effort and computation [27]. ECC and other lightweight cryptographic methods provide strong security for IoT devices without sacrificing performance or resources.

Second, in large IoT deployments, lightweight cybersecurity systems can efficiently distribute keys. Cryptographic keys for secure communication and authentication become harder to manage as connected devices grow exponentially. Little keys mean less resource-intensive key storage and transmission in lightweight schemes. Key management for IoT networks becomes more scalable and viable due to lower key distribution overhead. Lightweight cybersecurity solves IoT scalability and interoperability. IoT deployments with multiple manufacturers and communication protocols require flexible and standardised security. Lightweight methods secure and interoperate many devices and platforms [28]. IoT device security is improved by lightweight cryptography standardisation.

## 3. PROPOSED METHOD

A proposed solution for establishing secure communication between individuals involves the implementation of a layer that encompasses the end users who consume and produce data, as well as a cloud layer that incorporates an authentication and encryption technique. The authentication and encryption technique presented for IoT-based medical sensor data consists of three stages: authentication, encryption, and decryption. The initial phase of the proposed system involves authentication. The proposed scheme consists of nine steps. The primary contribution of this research was the introduction of ECC, an encryption technique that is both secure and efficient. The generation of a shared key facilitates secure communication between parties by enabling them to encrypt their messages. The establishment of a shared key for the encryption of shared messages has been overlooked by several recent research, despite being an essential first step. Given the importance of the ECC in facilitating secure group communication, our analysis primarily focuses on the earliest three stages of the ECC. The suggested approach is illustrated in Figure 2, which outlines the nine steps.

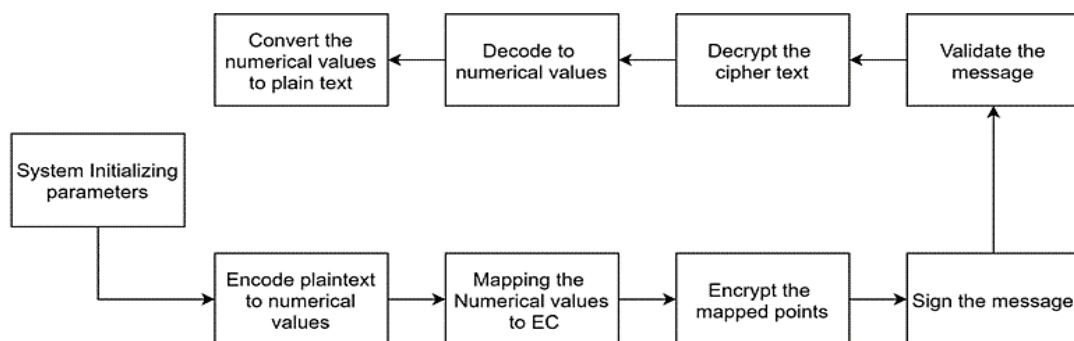


Figure 2. Nine stages of the proposed method

### 3.1. Establishing system parameters

In this phase, the generation of public and private keys will provide secure communication among all involved entities. This phase, proceeded with the generation of the  $G_{pkey}$ , which will serve as the encryption

mechanism for the internal communications within the group. The edge is responsible for creating and protecting the group's shared key (also known as  $G_{keysh}$ ). This allows for efficient decryption of encrypted text between the parties concerned. Hence, the Edge platform utilises its unique identifier ( $id_{edge}$ ) and a private random key (PRK) to construct the initial  $G_{keysh}$ . The first group shared key  $G_{keysh}$  is created using an edge algorithm.

Input:  $id_{edge}$ ; PRK  
 Output:  $G_{keysh}$   
 $G_{keysh} = id_{edge} \oplus \text{PRK};$   
 Initial shared group key  $\leftarrow G_{keysh}$

The preservation of forward and backward secrecy can be achieved using  $G_{keysh}$ , a cryptographic technique, to execute encryption and decryption of messages exchanged across nodes inside a network. Similarly, in the context of network communication, nodes that get disconnected from the network are unable to access and decipher encrypted messages that are transmitted after their disconnection. The suggested method achieves this objective by assigning specific tasks related to  $G_{keysh}$  maintenance to each individual node. The edge broadcasts the newly added node's hashed identifier ( $id_{ni}$ ) to each of the other nodes in the network. Subsequently, every node modifies the value of  $G_{keysh}$  and concurrently appends the hashed identification to its respective list.

### 3.2. Encoding/mapping the plaintext

The hypothesised encoding and mapping phases were expanded by this experiment. The encoding method used in this experiment has a security vulnerability, according to relevant research. Two implementations of the same encryption algorithm producing identical ciphertext during ECC encoding and mapping is the main vulnerability. Thus, the adversary can learn about the plaintext from the ciphertext. The study suggests dividing the original text into  $B$  blocks to overcome the limitation. According to the (1),  $M$  is the total number of characters in a plaintext and  $B$  is the required number of blocks.

$$B = \left\lceil \frac{M}{N} \right\rceil \quad (1)$$

The requirement for this length arises from the need to allocate each block  $B$  to the 192-bit ECC, which in turn necessitates the partition of the plaintext. During the mapping phase, the determination of mapping points involves the utilisation of the reserved 8 bits within each block as padding bits. This is done to guarantee the required number of repeats. The procedure of converting a plaintext " $M$ " into a blockset is shown in Figure 3. In the preliminary stage of the process, the decimal representations of each secured block are systematically conveyed to the EC. This specialized center has been established with the explicit purpose of ascertaining the individual values of  $y_i$  associated with each block. The method employed for the allocation and transmission of these encrypted blocks to the EC is elucidated in detail in Figure 4, meticulously outlining the sequential steps integral to this pivotal phase of the overall operation.

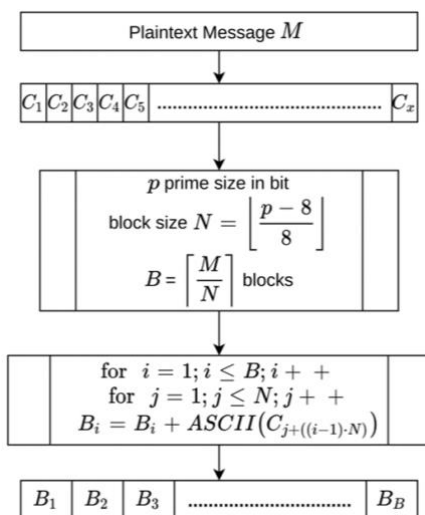


Figure 3. The action of transforming plain text into blocks

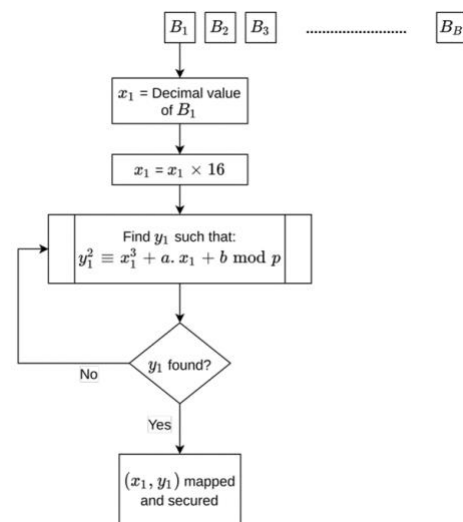


Figure 4. Secure block mapping onto an EC

### 3.3. Encrypting and decrypting the mapped points

In numerous techniques, it is commonly assumed that the mapping step in isolation suffices for the encryption of the plaintext. However, the mapping procedure to the EC proves that these points are essential to the final EC, allowing the elliptic curve discrete logarithm problem (ECDLP) to be exploited. In this suggested solution, the encryption of these data pieces is achieved by appending them to  $G_{key}$ . The process for encrypting the plotted data points is illustrated in Figure 5.

The subsequent stages exhibit a reversal of the preceding ones. As a result, the recipient employs the  $G_{key}$  to decode the encrypted data points and performs subtraction on them, seen in Figure 6. As seen earlier, the process of encrypting and decrypting messages involves the utilisation of a shared group point (referred to as  $G_{key}$ ) that is common to all individuals involved. The provided example in Figure 6 illustrates the process of decoding secured endpoints.

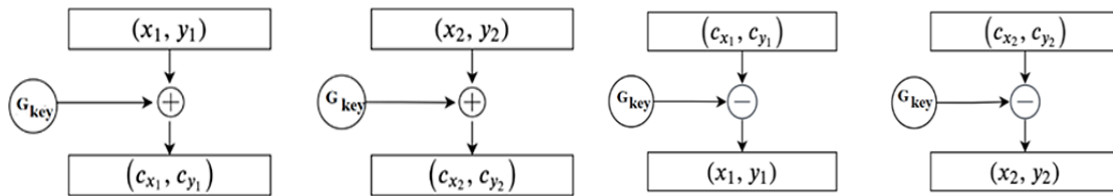


Figure 5. Encryption of mapped points

Figure 6. Decryption of secured points

### 3.4. Verification of encrypted messages

The encrypt-then-sign methods employed in our research endeavour to guarantee the confidentiality, integrity, and non-repudiation of communicated messages among entities. The suggested methodology guarantees privacy by implementing a series of preliminary measures. The data being transferred includes an encrypted coordinate, the current time ( $t_o$ ), and a signature integer created at random. Figure 7 illustrates the procedures involved in the signature process. By using the public key of the sender, the recipient can verify the genuineness of a signed communication.

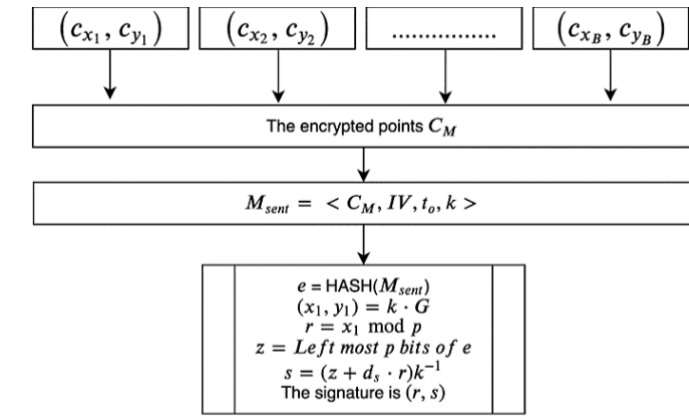


Figure 7. Signing process by sender

## 4. PERFORMANCE EVALUATION

### 4.1. Simulation environment

In this research, a network is constructed using NS3 simulation software. The network configuration includes 100 IoT devices, 25 users, one fog gateway, one micro datacentre, and one cloud server. The first step involves the registration of IoT devices through the utilisation of identification (ID), public key, and private key. To key creation, ECC is employed. Subsequently, the data obtained via sensing is subjected to encryption through the utilisation of ECC within the fog gateway. Subsequently, the IoTs devices transmit the encrypted data to the Cloud Server. Subsequently, during encrypted data transfer, the identification of a man in the middle (MITM) attack can be accomplished by analysing the keys involved. The findings were analysed for the

relationship between the number of IoT devices and resource utilisation, as well as the encryption and decryption time. Additionally, a correlation coefficient analysis was conducted.

#### 4.1.1. Encryption time

The temporal duration utilized by the encryption algorithm to transform a plaintext into ciphertext is denoted by the term "difference." This term specifically characterizes the time span between the initiation and completion phases of the encryption process. This temporal discrepancy is formally expressed through mathematical representation in the form of (2). In essence, the (2) delineates the mathematical relationship governing the time interval between the commencement and conclusion of encryption, elucidating the temporal intricacies involved in the encryption algorithm's operation.

$$i_{(t)} = i_{end(t)} - i_{start(t)} \quad (2)$$

#### 4.1.2. Decryption time

The evaluation of this metric involves the calculation of the temporal difference between the conclusion and initiation phases of the decryption process. This temporal disparity is precisely quantified through the application of a mathematical representation, specifically referred to as (3), which serves as a formalized expression encapsulating the quantitative aspects of the temporal relationship between the phases within the decryption process.

$$O_{(t)} = O_{end(t)} - O_{start(t)} \quad (3)$$

#### 4.1.3. Correlation coefficient analysis

The relationship between plaintext and ciphertext parameters is often determined using statistical analysis, specifically correlation coefficients. The coefficient indicates how well the encryption algorithm prevents statistical attacks. An effective encryption algorithm should produce ciphertext that is completely different from plaintext. Calculate correlation coefficient using (4).

$$\text{Corr Coef}(x, y) = \frac{\sum_{i=1}^n (x_i - \mu(x))(y_i - \mu(y))}{\sigma(x)\sigma(y)} \quad (4)$$

When the correlation coefficient attains a value of 1, it serves as an indication that the plaintext and ciphertext under consideration are entirely identical. Conversely, when the correlation coefficient reaches 0, it signifies that there exists a complete dissimilarity between the ciphertext and plaintext. Consequently, the effectiveness of the encryption technique can be assessed by scrutinizing the correlation coefficient, with a lower numerical value suggesting a higher degree of efficacy in the encryption process.

#### 4.2. Performance analysis

The term "computation cost" refers to the measure of computing resources required for the execution of a specific operation within a designated system or algorithm. These computing resources encompass processing power, time, and memory. In Table 1, a comprehensive comparison of the computational costs associated with various operations is provided. This table serves to illustrate the varying resource demands and efficiency considerations across different computational tasks within the specified system or algorithm.

Table 1. Computational costs comparative analysis

Method	Computational costs (μs)		$i_{(t)}$ (μs)	$O_{(t)}$ (μs)
	Gateway	IoT device		
[29]	0.26	0.19	1.41	1.43
[30]	0.55	0.19	1.68	1.7
Ours	0.12	0.12	1.032	1.006

All authentication techniques in the simulation, such as time stamps, random numbers, one-way hash functions, wireless access, and a sensor node, are given a 128-bit size. Computational costs were estimated to be in the ranges of 0.0004, 0.055, and 0.062 microseconds for a one-way hash function, symmetric encryption/decryption, and EC point multiplication, respectively. The overall computational cost can be determined by considering the hashing cost during the user's registration phase, which amounts to  $2H$ . On the other hand, at the sensor level, the computational cost can be calculated by combining the hashing and



encryption costs, denoted as  $(1H + Ec)$ . Adding together the costs of verification and decryption yields the cost at the gateway, which is represented by  $(1H + Dc)$ .

The results of the simulations show that the proposed method has a shorter running time for both encryption and decryption than the other approaches. The graphical representation of this analysis can be seen in Figures 8 and 9. Table 2 presents the correlation coefficient that has been calculated using various types of message sets. The findings indicate that the coefficient of correlation for the suggested model is approximately 0.051, indicating a proximity to zero.

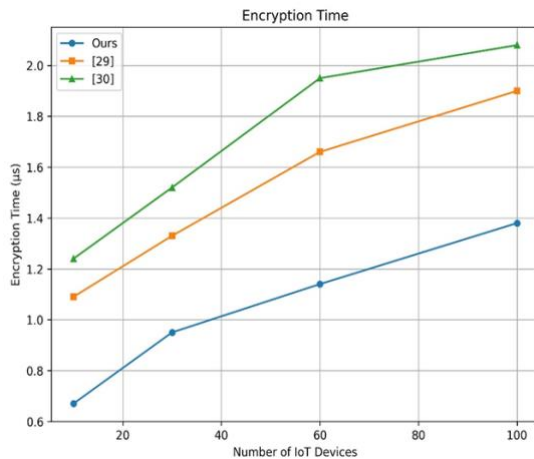


Figure 8. Encryption time analysis

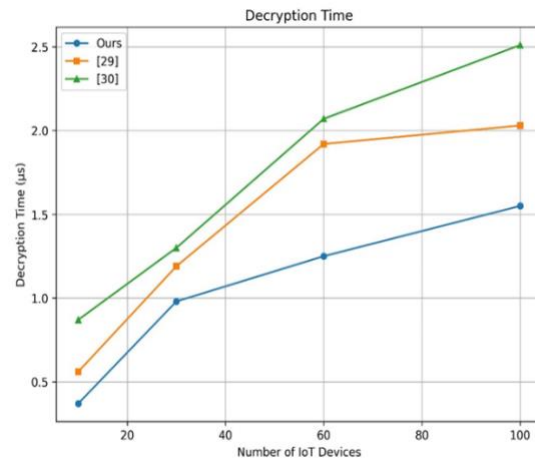


Figure 9. Decryption time analysis

Table 2. Correlation coefficient values

Message description	Correlation value
Registration data	0.015
Login data	0.065
Control data	0.073
Average	0.051

The examination of the correlation between resource utilisation and the number of IoT devices within a network is of paramount importance in comprehending the scalability and efficacy of IoT implementations. The escalation in the quantity of IoT devices necessitates a thorough consideration of resource utilisation, as it plays a crucial role in determining system performance, reliability, and cost-effectiveness. Figure 10 gives the chart of resource utilization vs number of IoT devices.

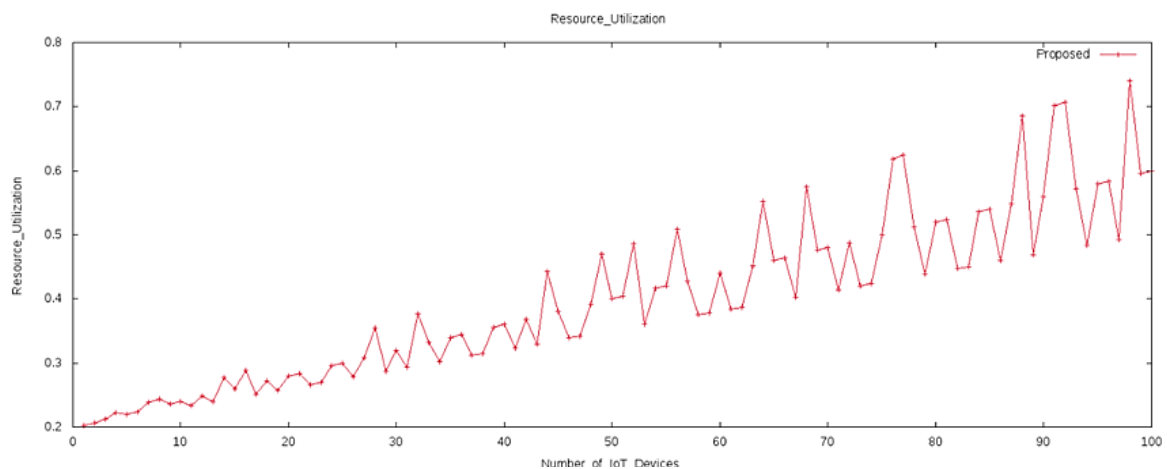


Figure 10. Resource utilization vs number of IoT devices



## 5. CONCLUSION

This comprehensive research underscores the pivotal role of cutting-edge ECC techniques in addressing intricate challenges within the realm of FC-based IoT, a dynamically evolving field. The paramount importance of security and efficiency in FC is acknowledged, with ECC emerging as a key enabler for enhancing data privacy, mitigating cyber risks, and optimizing resource utilization in IoT deployments through a thorough exploration of its multifaceted applications. A meticulous examination of the relevant literature reveals the significant contributions of researchers in shaping security protocols for IoT and FC, providing a nuanced understanding of the current landscape characterized by advancing technologies and evolving threats. The insights gleaned from this study serve as a beacon for the development of adaptive and secure IoT systems, offering valuable guidance to practitioners and decision-makers tasked with leveraging FC while safeguarding sensitive data. As this study peer into the future, the potential for ECC-based approaches and FC platforms to propel IoT security and efficiency to unprecedented heights becomes evident. The amalgamation of ECC and FC represents a noteworthy stride towards cultivating a safer and more effective IoT, especially in an era marked by the convergence of digital and physical realms. This research not only encapsulates the present state of affairs but also lays the foundation for anticipating and embracing forthcoming enhancements, positioning ECC and FC as dynamic forces poised to redefine the landscape of IoT security and efficiency.




## REFERENCES

- [1] G. Peralta, M. I. -Urkia, M. Barcelo, R. Gomez, A. Moran, and J. Bilbao, "Fog computing based efficient IoT scheme for the Industry 4.0," in *2017 IEEE International Workshop of Electronics, Control, Measurement, Signals and their Application to Mechatronics (ECMSM)*, 2017, pp. 1–6, doi: 10.1109/ECMSM.2017.7945879.
- [2] A. Paul, H. Pinjari, W. -H. Hong, H. C. Seo, and S. Rho, "Fog computing-based IoT for health monitoring system," *Journal of Sensors*, vol. 2018, pp. 1–7, Oct. 2018, doi: 10.1155/2018/1386470.
- [3] H. A. Alshambri and F. Alassery, "Securing fog computing for e-learning system using integration of two encryption algorithms," *Journal of Cyber Security*, vol. 3, no. 3, pp. 149–166, 2021, doi: 10.32604/jcs.2021.022112.
- [4] A. K. Das, M. Wazid, A. R. Yannam, J. J. P. C. Rodrigues, and Y. Park, "Provably secure ECC-based device access control and key agreement protocol for IoT environment," *IEEE Access*, vol. 7, pp. 55382–55397, 2019, doi: 10.1109/ACCESS.2019.2912998.
- [5] C. Biswas, U. D. Gupta, and M. M. Haque, "An efficient algorithm for confidentiality, integrity and authentication using hybrid cryptography and steganography," in *2019 International Conference on Electrical, Computer and Communication Engineering (ECCE)*, Feb. 2019, pp. 1–5, doi: 10.1109/ECACE.2019.8679136.
- [6] G. Verma, M. Liao, D. Lu, W. He, X. Peng, and A. Sinha, "An optical asymmetric encryption scheme with biometric keys," *Optics and Lasers in Engineering*, vol. 116, pp. 32–40, 2019, doi: 10.1016/j.optlaseng.2018.12.010.
- [7] A. Rana et al., "The rise of blockchain internet of things (BIoT): secured, device-to-device architecture and simulation scenarios," *Applied Sciences*, vol. 12, no. 15, Jul. 2022, doi: 10.3390/app12157694.
- [8] H. N. Almajed, A. S. Almogren, and A. Altameem, "A resilient smart body sensor network through pyramid interconnection," *IEEE Access*, vol. 7, pp. 51039–51046, 2019, doi: 10.1109/ACCESS.2019.2909557.
- [9] N. Koblit, "Elliptic curve cryptosystems," *Mathematics of Computation*, vol. 48, no. 177, pp. 203–209, 1987, doi: 10.1090/S0025-5718-1987-0866109-5.
- [10] A. Piedra, A. Braeken, and A. Touhafi, "Extending the IEEE 802.15.4 security suite with a compact implementation of the NIST P-192/B-163 elliptic curves," *Sensors*, vol. 13, no. 8, pp. 9704–9728, Jul. 2013, doi: 10.3390/s130809704.
- [11] L. Ferretti, M. Marchetti, and M. Colajanni, "Fog-based secure communications for low-power IoT devices," *ACM Transactions on Internet Technology*, vol. 19, no. 2, pp. 1–21, 2019, doi: 10.1145/3284554.
- [12] Y. Hao et al., "Lightweight architecture for elliptic curve scalar multiplication over prime field," *Electronics*, vol. 11, no. 14, Jul. 2022, doi: 10.3390/electronics11142234.
- [13] K. Gasm, S. Dilek, S. Tosun, and S. Ozdemir, "A survey on computation offloading and service placement in fog computing-based IoT," *The Journal of Supercomputing*, vol. 78, no. 2, pp. 1983–2014, Feb. 2022, doi: 10.1007/s11227-021-03941-y.
- [14] F. A. Alhaidari and E. J. Alqahtani, "Securing communication between fog computing and iot using constrained application protocol (CoAP): a survey," *Journal of Communications*, pp. 14–30, Jan. 2020, doi: 10.12720/jcm.15.1.14-30.
- [15] Y. Liu, J. Zhang, and J. Zhan, "Privacy protection for fog computing and the internet of things data based on blockchain," *Cluster Computing*, vol. 24, no. 2, pp. 1331–1345, Jun. 2021, doi: 10.1007/s10586-020-03190-3.
- [16] L. Zhou, H. Guo, and G. Deng, "A fog computing based approach to DDoS mitigation in IIoT systems," *Computers & Security*, vol. 85, pp. 51–62, Aug. 2019, doi: 10.1016/j.cose.2019.04.017.
- [17] K. F. Hassan and M. E. Manaa, "Detection and mitigation of DDoS attacks in internet of things using a fog computing hybrid approach," *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 11, no. 3, pp. 1604–1613, Jun. 2022, doi: 10.11591/eei.v11i3.3643.
- [18] S. Shukla, M. F. Hassan, L. T. Jung, A. Awang, and M. K. Khan, "A 3-tier architecture for network latency reduction in healthcare internet-of-things using fog computing and machine learning," in *Proceedings of the 2019 8th International Conference on Software and Computer Applications*, Feb. 2019, pp. 522–528, doi: 10.1145/3316615.3318222.
- [19] B. Dezfouli and Y. Liu, "Editorial: special issue 'edge and fog computing for internet of things systems,'" *Sensors*, vol. 22, no. 12, Jun. 2022, doi: 10.3390/s22124387.
- [20] N. Raveendran, H. Zhang, L. Song, L.-C. Wang, C. S. Hong, and Z. Han, "Pricing and resource allocation optimization for IoT fog computing and NFV: an EPEC and matching based perspective," *IEEE Transactions on Mobile Computing*, vol. 21, no. 4, pp. 1349–1361, Apr. 2022, doi: 10.1109/TMC.2020.3025189.
- [21] L. D. Singh and K. M. Singh, "Implementation of text encryption using elliptic curve cryptography," *Procedia Computer Science*, vol. 54, pp. 73–82, 2015, doi: 10.1016/j.procs.2015.06.009.
- [22] H. D. Tiwari and J. H. Kim, "Novel method for DNA-based elliptic curve cryptography for IoT devices," *ETRI Journal*, vol. 40, no. 3, pp. 396–409, Jun. 2018, doi: 10.4218/etrij.2017-0220.




- [23] C. Patel, A. K. Bashir, A. A. AlZubi, and R. Jhaveri, "EBAKE-SE: A novel ECC-based authenticated key exchange between industrial IoT devices using secure element," *Digital Communications and Networks*, vol. 9, no. 2, pp. 358–366, Apr. 2023, doi: 10.1016/j.dcan.2022.11.001.
- [24] V. K. Quy, N. V. Hau, D. V. Anh, and L. A. Ngoc, "Smart healthcare IoT applications based on fog computing: architecture, applications and challenges," *Complex & Intelligent Systems*, vol. 8, no. 5, pp. 3805–3815, Oct. 2022, doi: 10.1007/s40747-021-00582-9.
- [25] A. Ilyas *et al.*, "Software architecture for pervasive critical health monitoring system using fog computing," *Journal of Cloud Computing*, vol. 11, no. 1, Nov. 2022, doi: 10.1186/s13677-022-00371-w.
- [26] T. A. Ahanger, U. Tariq, A. Ibrahim, I. Ullah, Y. Bouteraa, and F. Gebali, "Securing IoT-empowered fog computing systems: machine learning perspective," *Mathematics*, vol. 10, no. 8, Apr. 2022, doi: 10.3390/math10081298.
- [27] B. Hammi, A. Fayad, R. Khatoun, S. Zeadally, and Y. Begriche, "A lightweight ECC-based authentication scheme for internet of things (IoT)," *IEEE Systems Journal*, vol. 14, no. 3, pp. 3440–3450, Sep. 2020, doi: 10.1109/JSYST.2020.2970167.
- [28] K. Sowjanya, M. Dasgupta, and S. Ray, "Elliptic curve cryptography based authentication scheme for internet of medical things," *Journal of Information Security and Applications*, vol. 58, 2021, doi: 10.1016/j.jisa.2021.102761.
- [29] S. Kumari and H. Om, "Authentication protocol for wireless sensor networks applications like safety monitoring in coal mines," *Computer Networks*, vol. 104, pp. 137–154, Jul. 2016, doi: 10.1016/j.comnet.2016.05.007.
- [30] F. Wu *et al.*, "A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks," *Future Generation Computer Systems*, vol. 82, pp. 727–737, 2018, doi: 10.1016/j.future.2017.08.042.

## BIOGRAPHIES OF AUTHORS



**Krishnapura Srinivasa Ravindra**    completed his bachelor's degree in Electronics & Communication Engineering from NMAM Institute of Technology, Nitte and master's degree in digital Electronics and Communication from NMAM Institute of Technology, Nitte, Karkala, Udupi. Currently he is pursuing his Ph.D. from JAIN (deemed to be University), Bengaluru. He has 18 years of academic experience. His areas of interest include IoT, computer networks, cyber security, and real-time systems. At present he is working as Assistant Professor at NMAM Institute of Technology, Nitte (deemed to be University). He can be contacted at email: ravindraks@gmail.com.



**Dr. Malode Vishwanatha Panduranga Rao**    obtained his Ph.D. degree in computer science from National Institute of Technology Karnataka, Mangalore, India. He has completed a Master of Technology in computer science and Bachelor of Engineering in Electronics and communication Engineering. He is currently working as Professor in Jain (Deemed to be University) Bengaluru, India. His research interests are in the field of real-time and embedded systems-internet of things. He has published various research papers in journal and conferences across India, also in the IEEE international conference in Okinawa, Japan (visited) 2008. He has authored two reference books on Linux internals. He is the life member of Indian Society for Technical Education and IAENG. Now from past three years, he has published 12 indian patents and three patents are stepping towards grant status. One research scholar under his guidance was awarded a Ph.D. degree. He can be contacted at email: r.panduranga@jainuniversity.ac.in.