International Journal of Electrical and Computer Engineering (IJECE)
Vol. 14, No. 6, December 2024, pp. 7224~7235
ISSN: 2088-8708, DOI: 10.11591/ijece.v14i6.pp7224-7235 ❐ 7224

A novel secured open standard framework for internet of things applications integrating elliptic curve cryptography and fog computing

Krishnapura Srinivasa Ravindra[1,2], Malode Vishwanatha Panduranga Rao[3]
[1]Department of Electronics Engineering, Faculty of Engineering and Technology, JAIN (Deemed to be University), Bengaluru, India
[2]Department of Electronics and Communication Engineering, NMAM Institute of Technology, NITTE (Deemed to be University), Nitte, India
[3]Department of Computer Science and Engineering, Faculty of Engineering and Technology, JAIN (Deemed to be University), Bengaluru, India

Article Info

Article history:

Received May 20, 2024
Revised Aug 4, 2024
Accepted Aug 14, 2024

Keywords:

Elliptic curve cryptography
Fog computing
Internet of things
Lightweight cryptography
Man-in-the-middle-attack
network scalability

ABSTRACT

The internet of things (IoT) has revolutionized various fields by enabling seamless connectivity and data exchange among numerous devices. However, this interconnectivity introduces significant security challenges, particularly in ensuring data confidentiality, integrity, and authenticity. This study proposes a novel secure open standard framework for IoT applications, addressing these challenges through the integration of elliptic curve cryptography (ECC) and fog computing. The framework consists of three core components: secure device registration, data encryption within the fog gateway, and a robust mechanism for detecting man-in-the-middle (MITM) attacks. The unique aspect of the proposed method lies in its comprehensive approach to IoT security. Utilizing ECC, the framework ensures secure communication among resource constrained IoT devices, balancing encryption strength and efficiency. The integration of fog computing reduces latency and enhances processing efficiency by offloading intensive tasks from IoT devices to the fog layer. The MITM attack detection mechanism continuously monitors cryptographic keys and communication patterns, providing an additional layer of security against advanced cyber threats. The system was implemented and evaluated using the NS-3.26 network simulator and Python for data visualization. The experimental setup included 100 IoT devices, 25 users, a fog gateway, a datacenter, and a cloud server. Results demonstrate the framework's scalability and efficiency, with consistent throughput increases and balanced power consumption across varying IoT device numbers.

Corresponding Author:

Krishnapura Srinivasa Ravindra
Department of Electronics and Communication Engineering, NMAM Institute of Technology, NITTE (Deemed to be University)
Nitte 574110, Karnataka, India
Email: ravindraks@gmail.com

1. INTRODUCTION

The internet of things (IoT) has emerged as a transformative force, promising to revolutionize how we interact with the world around us. Smart homes and cities, industrial automation, and healthcare are just a few of the many industries where IoT technologies offer smooth communication, automation, and data-driven decision-making by linking a multitude of devices, sensors, and systems [1], [2]. But as IoTs devices proliferate, so do hitherto unseen security issues that seriously jeopardize system dependability, integrity, and data privacy [3]. Given the circumstances, it is crucial to provide a secure and universally accepted architecture for IoT applications to reduce the risk of security breaches and build confidence in IoT ecosystems. An effective framework must prioritize critical security considerations, such as device authentication, data confidentiality, integrity protection, and resistance to malicious assaults. By offering a uniform method for implementing security, ensuring compatibility, and meeting regulatory requirements, it can promote wider acceptance and unlock the complete capabilities of IoT technology. Cloud computing has been a huge success, relieving clients of computationally intensive activities. However, in situations where reducing latency and limiting communications are critical, alternative paradigms have emerged by moving cloud capabilities to the network edge. One such paradigm, fog computing, extends cloud computing by relocating a portion of the cloud's computational and communication capabilities near sensor nodes. Figure 1 indicates a generalized IoT fog computing architecture with several considerations. Three independent IoT networks and a fog layer, which facilitates communication between nodes across the networks and with the cloud, comprise the described setup. The bidirectional arrows represent data flow between several elements. The design consists of three layers of gateways, with the top layer serving as the principal access point to the fog. Like how computers design cache memory levels, this hierarchical method aims to reduce latency when accessing processor memory. Here, the layer closest to the IoT nodes responds quickly but has fewer computing and memory resources.

In the context of IoT fog computing, transport layer security (TLS) is a very suitable choice for guaranteeing safe communications. However, it faces challenges because the initial design of several commonly used standard cipher suites did not account for the constraints of devices with limited resources and battery power. The main goal of this research is to improve the security of IoT fog computing gateways that have limited resources and are energy efficient.

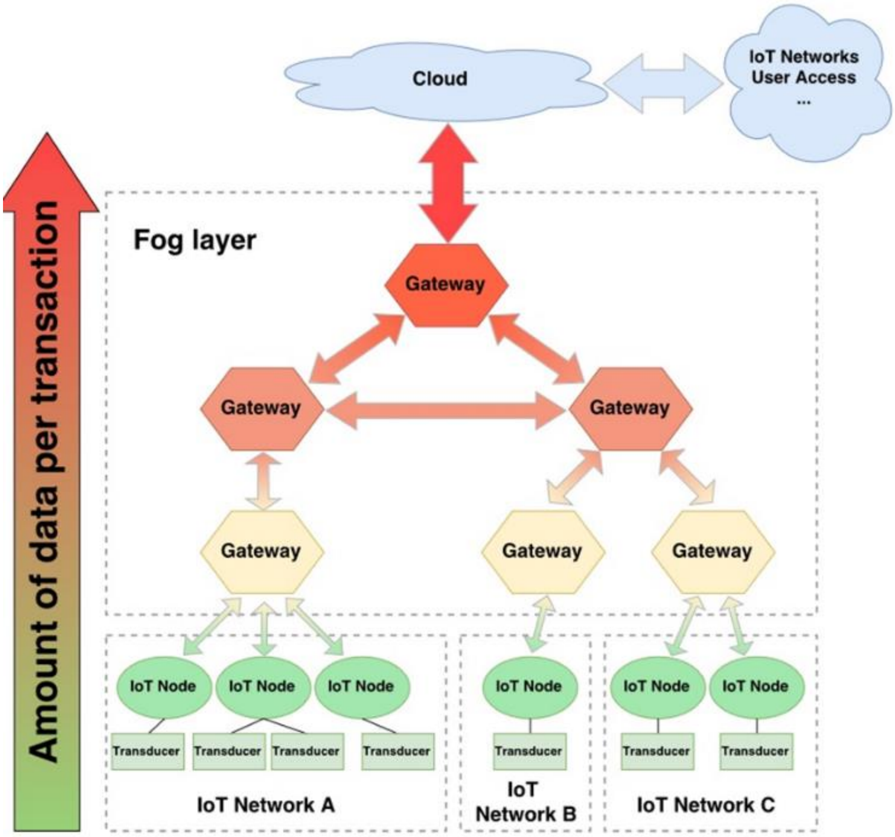


Figure 1. IoT fog computing architecture

The objective of this study is to recommend and evaluate an extensive security architecture specifically designed for IoT fog computing applications, utilizing advanced cryptographic algorithms and architectural concepts. Researchers have specifically designed the architecture to support a wide range of deployment scenarios, encompassing various types of IoT devices, fog gateways, micro-datacenters, and cloud servers that constitute a diversified ecosystem [4]. Our goal is to implement sophisticated security measures at every level of the IoT infrastructure to create a strong defense-in-depth approach. This strategy will protect valuable data and system assets from emerging threats. Our suggested system relies on the implementation of ECC to ensure the security of IoT device connections [5]. ECC has various benefits compared to conventional cryptographic techniques, such as reduced key sizes, accelerated computation, and improved resilience against quantum assaults [6]. By utilizing ECC to produce cryptographic keys, encryption, and authentication, one may strike a harmonious equilibrium between security and the efficient utilization of resources. This makes ECC particularly suitable for IoT situations that have limited resources [7]. In proposed architecture, initially enroll IoT devices by assigning them distinct IDs and producing public and private keys using ECC. The registration procedure creates a trust connection between the devices and the central administration infrastructure, allowing for secure communication and the exchange of data. Additionally, the fog gateway encrypts all collected data using ECC before sending it to the cloud server. This guarantees that the data remains secret and protected from any tampering throughout the whole transmission process.

To improve the security of proposed framework, in this method implemented measures to identify and counteract man-in-the-middle (MITM) attacks [8] that may occur during the transfer of data. Our technology may detect illegal interception or tampering attempts by monitoring the integrity of cryptographic keys and analyzing communication patterns for anomalies. MITM attacks can be stopped quickly by taking steps like changing encryption keys or isolating the affected network [9]. This stops people from getting to your data without your permission and keeps service interruptions to a minimum. Aside from security concerns, our article also examines the performance ramifications of using the suggested architecture in actual IoT settings. Assessed important measures such as power consumption, resource usage, energy efficiency, end-to-end delay, and throughput across different sizes of IoT deployments. Our goal is to estimate the additional costs incurred by security measures to provide a better understanding of the balance between security and system performance. This will help decision-makers make well-informed choices when implementing security measures.

The rapid expansion of the IoT has resulted in an unparalleled increase in the number of interconnected devices in diverse fields, including smart homes, cities, industrial automation, and healthcare. While the interconnection of systems presents significant advantages in terms of effectiveness, convenience, and creativity, it also presents numerous security obstacles that demand attention. Therefore, urgently need a safe and standardized architecture specifically for IoT applications. The primary source of security vulnerabilities in IoT ecosystems arises from the extensive number and diverse nature of interconnected devices [10]. Given the projected number of IoT devices in use, it is critical to understand that individuals with malevolent intent may target each device, aiming to exploit weaknesses and compromise the system's overall security. Originally designed for traditional computing systems, conventional security approaches typically fail to adequately meet the specific needs and limitations of IoT implementations. Consequently, there is a pressing requirement for uniform security standards [11], procedures, and optimal strategies to reduce risks and guarantee the reliability of IoT systems. Moreover, the absence of consistency in security measures among various IoT platforms and manufacturers intensifies the difficulties in achieving interoperability and obstructs the smooth integration of IoT solutions. Without established security frameworks, developers and system integrators have problems with interoperability, fragmentation, and vendor lock-in, which impede the scalability and acceptance of IoT technology [12]. An open standard framework facilitates the exchange of security specifications and interfaces among various IoT components, promoting interoperability and encouraging collaboration within the ecosystem. Furthermore, the ever-changing nature of IoT environments, which are defined by occasional connectivity, limited resources, and scattered data processing, presents distinct security concerns that require customized solutions [13]. Dispersed and resource limited IoT deployments may not suit conventional security methods such as perimeter protection and centralized authentication. Hence, it is imperative for a standardized framework to incorporate decentralized trust models, lightweight cryptographic algorithms, and adaptive security rules to cater to the varied requirements of IoT applications.

Another crucial aspect driving the need for a secured open standard framework is the increasing regulatory scrutiny and privacy concerns surrounding IoT data collection, processing, and sharing practices [14]. With the accumulation of substantial quantities of sensitive data from various sources, such as personal devices, sensors, and actuators, it becomes crucial to prioritize compliance with privacy legislation and the protection of user data. Implementing a standardized framework may offer clear direction on safeguarding data, managing permission, and employing approaches that preserve privacy. This, in turn, improves transparency, accountability, and user confidence in the implementation of IoT systems. Furthermore, the rise of new attack methods and complex dangers that specifically target IoT devices highlights the need for immediate implementation of security measures and the sharing of intelligence on potential threats. IoT devices are becoming more and more attractive to hackers who aim to disrupt operations, steal sensitive information, or undermine vital infrastructure. They target these devices using methods such as ransomware [15], botnets [16], supply chain attacks [17], and zero-day [18] vulnerabilities. By embracing a transparent and widely accepted framework that is backed by a cooperative security network, all parties involved may work together to tackle new risks, exchange information about potential attacks, and utilize security improvements pushed by the community to outpace their opponents.

This study attempts to tackle important issues related to IoT security, performance, and standardization. Firstly, proposed a thoroughly secured open standard framework specifically for IoT applications. This approach addresses the urgent security issues inherent in IoT ecosystems, including device authentication, data confidentiality, integrity protection, and resistance to malicious attacks. Through the creation of a uniform methodology for security implementation, interoperability, and compliance, expecting to reduce any hazards and vulnerabilities related to the spread of IoT devices, interoperability, and compliance, thus promoting confidence among interested parties. Second, the work attempts to demonstrate, by thorough testing and analysis, the practical viability and effectiveness of the suggested framework. Aimed to give empirical proof that the framework is effective in protecting IoT applications while reducing performance overhead by deploying it in real-world IoT environments and assessing important performance metrics including power consumption, resource utilization, energy efficiency, end-to-end delay, and throughput. Additionally, the work looks at new methods for reducing MITM threats during data transfer to add to the larger conversation on IoT security. The goal of this approach is to improve the resistance of IoT systems against efforts at manipulation and illegal interception by including techniques for identifying and preventing MITM attacks inside the suggested architecture. To assess the efficiency of these mitigation strategies in preventing different MITM attack scenarios and maintaining the integrity and confidentiality of IoT data by empirical analysis and simulation. The main aim of this work is to advance the state-of-the-art in IoT security, performance, and standardization. Aim of this research is to support the creation of reliable, interoperable, and trustworthy IoT ecosystems by creating and assessing a safe open standard framework, as well as the empirical examination of important security methods and performance indicators. By promoting cooperation, standardization, and knowledge exchange, the aim is to stimulate creativity and encourage the widespread use of safe and dependable IoT technology.

2. RELATED WORKS

The literature has developed numerous security standards, assessment frameworks, and special publications on security techniques to address various aspects of cybersecurity across different environments. These materials provide recommendations, ideal practices, and approaches for putting into place efficient security measures to safeguard digital assets, reduce risks, and guarantee adherence to legal obligations. Therefore, it's crucial to keep in mind that these security standards and evaluation frameworks, tailored to specific application domains or industrial sectors, often mirror the unique security and regulatory challenges inherent in each environment.

According to research by Hinduja and Pandey [19], the exponential expansion of IoT-based systems has intensified security apprehensions, underscoring the critical need for a security assessment framework tailored specifically for IoT systems. The authors introduced an evaluation paradigm that closely examines the security features of IoT-based devices. This proposed approach allows for a thorough assessment of security factors using a hybrid multi-criteria decision-making (MCDM) methodology. Then, using their developed methodology, the researchers carried out an empirical investigation to evaluate the security of IoT-based healthcare devices. Researchers emphasize the real-time tracking of products, information management, and status monitoring capabilities of IoT technology for inventory automation [20]. Nevertheless, a strong security framework is essential to guarantee authentication, authorization, integrity, and confidentiality of the sent data because of the data flow among linked devices inside such networks. To overcome this issue, the authors propose a lightweight security evaluation framework specifically for inventory automation using wireless sensor networks. Recently, Ebadinezhad and Mobolade [21] presented a novel cloud-based remote patient monitoring system for internet of things health detection. The results revealed significant improvements in patient happiness, data transmission security, and general healthcare outcomes. Especially at decision time, the study showed that the suggested framework was more efficient than other methods. More precisely, authors achieved a phenomenal accuracy rate of 100% with a decision time of 16.3 seconds for processing 46 features [22]. These findings demonstrate notable progress in the field of remote patient monitoring and show how IoT-enabled technologies may improve patient care and healthcare delivery.

In their work, Chatterjee *et al.* [23] designed a new lightweight remote user authentication and key management system based on ECC specifically for IoT communication within the fog computing framework.

The work addresses the flaws in authentication technique to enhance the effectiveness and security of authentication systems in fog-centric IoT environments. The authors try to remove the several security flaws and restrictions present in the current framework using the suggested approach. An automated validation of internet security protocols and applications (AVISPA) simulation and thorough mathematical security analysis demonstrate the effectiveness of the suggested approach. The results of these analyses demonstrate convincingly that the suggested approach successfully reduces all relevant security risks, thereby improving the security posture of fog centric IoT communication. Kapoor *et al.* [24] described a new method called RF-DECC, which combines the RedFox optimization algorithm for clustering with DNA-based ECC. Its goal is to make data more secure in fog computing environments. The study demonstrates the effectiveness of ECC, a lightweight cryptographic solution, in resource-constrained internet of things settings such as fog computing. Comparing ECC to conventional public key cryptography techniques, the former has benefits in terms of computing performance and smaller key sizes. However, adding a higher level of encryption complexity to ECC by incorporating DNA-based encoding improves the system's security. This novel method strengthens the encryption process and enhances data security in fog computing situations by taking advantage of the special qualities of DNA encoding. Narayana and Patibandla [25] presented a fog-based model, highlighting its functional importance and critical role in the IoT environment. The suggested method gets around IoT devices' communication problems by combining fog computing with resource management, validation procedures, and the configuration of IoT devices to create a strong programming environment. This fog computing architecture enables smooth connections between IoT devices while also guaranteeing data security throughout the communication process.

3. PROPOSED METHOD

The main contribution of this study is the introduction of a very efficient and secure encryption technique that is based on elliptic curve cryptography (ECC). This method facilitates the generation of a shared key among participants, which allows them to safeguard their shared messages and thus enable secure communication. The current investigation of shared message encryption frequently neglects the critical initial stage of establishing this shared key. In addition to strengthening the security of the communication process, this study introduces a resilient and enhanced method for encoding and mapping plaintext to an elliptic curve (EC). The study primarily focuses on providing a detailed explanation of the three processes involved in initiating ECC, which is a crucial element in securing group communication systems, especially in IoT environments. Furthermore, this strategy integrates the notion of IoT fog nodes, which serve as mediators to enable and safeguard communication between IoT devices and the cloud. The fog nodes carry out essential functions like encryption and key management, utilizing ECC to ensure the security and effectiveness of the entire communication process within the IoT ecosystem. Figure 2 shows the representation of the suggested strategy.

The first stage of the implementation plan entails establishing a comprehensive network infrastructure that includes 100 IoT devices, 25 users, 1 fog gateway, 1 micro datacenter, and 1 cloud server. This broad and wide configuration enables the establishment of a realistic IoT ecosystem where different devices engage and exchange information. The innovation in this configuration lies in the incorporation of a fog gateway and a tiny datacenter, which allows computing and storage capabilities to be close to the network's edge. The next step focuses on the secure registration of IoT devices. Every device is enrolled with a distinct identity (ID), a public key, and a private key, all created using ECC. The innovation in this stage is employing ECC for the generation of the initial key. This not only improves security but also guarantees that the system remains lightweight and efficient, which is essential for extensive IoT implementations.

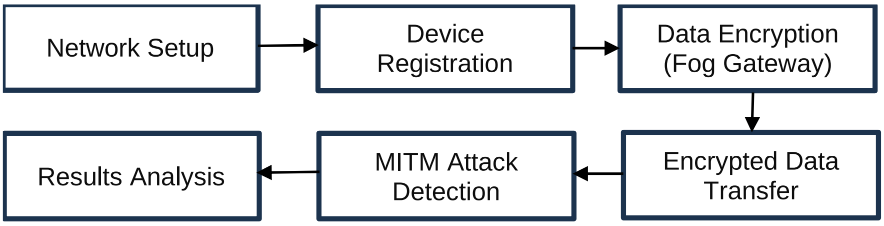


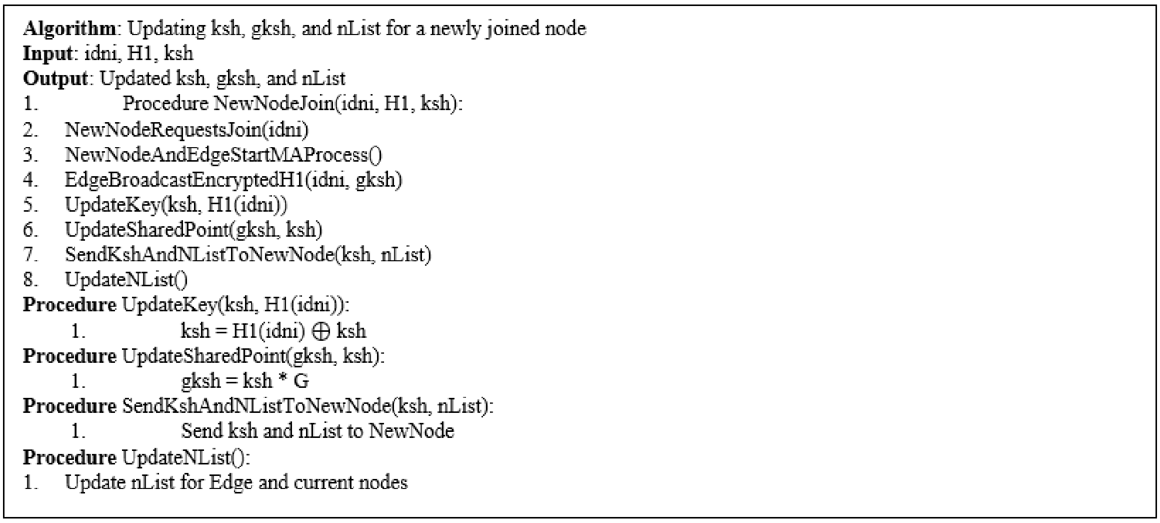
Figure 2. Proposed methodology block diagram

The fog gateway uses ECC to encrypt the data collected from IoT devices during the subsequent stage. The fog gateway acts as an intermediary, offering enhanced security and computing capabilities near

IoT devices. By encrypting data at this specific level, the system ensures the protection of confidential information before it reaches the cloud server. This approach utilizes the processing power of the fog gateway to transfer encryption tasks from IoT devices that have limited resources. The IoT devices transmit the data to the cloud server after encryption. This measure guarantees the security of all data sent across the network, reducing the possibility of data breaches while in transit. While transmitting encrypted data, the system consistently monitors for possible MITM attacks. The system accomplishes this by analyzing cryptographic keys and communication patterns. The system has the capability to identify anomalies that suggest unlawful interception or tampering efforts. This two-tiered security method ensures instant identification and resolution of any attempt to breach the communication, providing robust protection for the IoT ecosystem.

3.1. Updating newly added node

To maintain both forward and backward secrecy, it is imperative to ensure that any newly joined nodes cannot interpret the ciphertext delivered before their inclusion in the group using the shared key k_{sh}. Similarly, nodes departing from the group should not be able to decipher the ciphertext they send. The suggested method gives each node the ability to carry out tasks to maintain k_{sh}. When a new node wants to join the group, the edge sends the hashed ID $H_1(id_{ni})$ of the joining node to all current nodes. Afterwards, each node includes this hashed ID in its node list nList while simultaneously updating k_{sh} as described in Figure 3.



```
Algorithm: Updating ksh, gksh, and nList for a newly joined node
Input: idni, H1, ksh
Output: Updated ksh, gksh, and nList
        Procedure NewNodeJoin(idni, H1, ksh):
    NewNodeRequestsJoin(idni)
    NewNodeAndEdgeStartMAProcess()
    EdgeBroadcastEncryptedH1(idni, gksh)
    UpdateKey(ksh, H1(idni))
    UpdateSharedPoint(gksh, ksh)
    SendKshAndNListToNewNode(ksh, nList)
    UpdateNList()
Procedure UpdateKey(ksh, H1(idni)):
        ksh = H1(idni) ⊕ ksh
Procedure UpdateSharedPoint(gksh, ksh):
        gksh = ksh * G
Procedure SendKshAndNListToNewNode(ksh, nList):
        Send ksh and nList to NewNode
Procedure UpdateNList():
    Update nList for Edge and current nodes
```

Figure 3. Updating newly added node

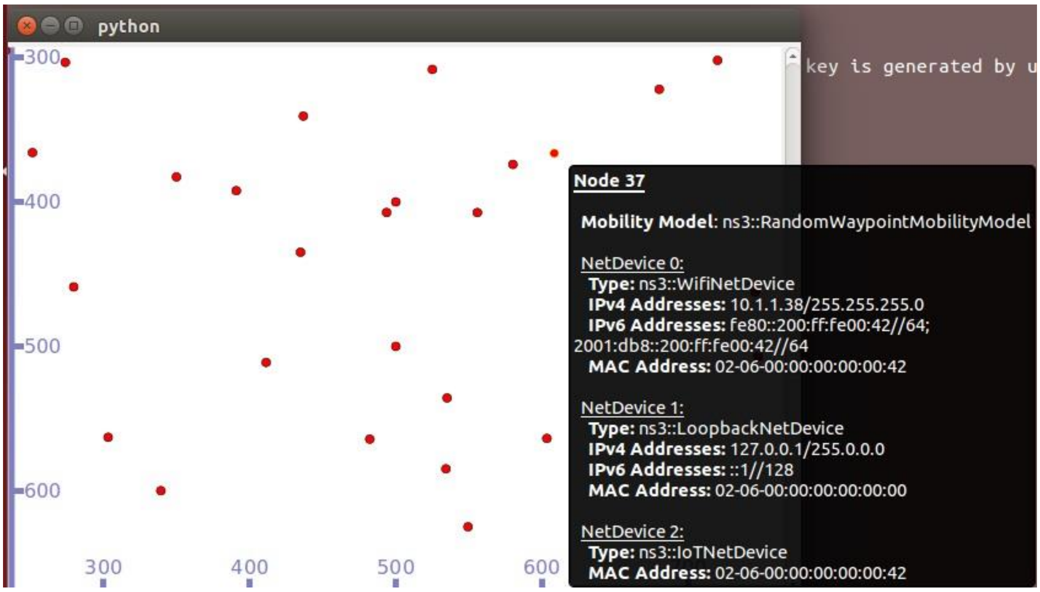
3.2. Securing against encryption attacks

Utilized the cipher block chaining (CBC) mode of operation to protect the blocks from encryption attacks like the chosen plaintext attack (CPA) and the chosen ciphertext attack (CCA). This mode improves the blocks' resistance to such assaults by incorporating a feedback mechanism that combines each plaintext block with the ciphertext of the previous block before encryption. This interdependence between succeeding blocks ensures that any changes or manipulations in one block propagate unpredictably through the subsequent blocks, foiling attempts to derive information about the plaintext or influence the ciphertext. Figure 4 depicts the process of block chaining in CBC mode, demonstrating how this approach helps to improve the security of encrypted data.

3.3. MITM attack detection

The MITM attack detection method aims to improve the security of IoT communications by utilizing a multi-layered strategy to detect potential MITM attacks. This algorithm integrates multiple cutting-edge algorithms to enable reliable detection while preserving optimal efficiency for IoT scenarios. Initially, the method validates the integrity of the session key. The process entails generating a session key using both the sender and recipient's public keys. Then compare this derived key with the encryption session key. This phase guarantees that any inconsistencies in key derivation, which may suggest a MITM attack, are immediately identified. Additionally, the method verifies the data transmission's integrity by performing a hash function on the current encrypted data and comparing it to the hash of the previous successful transmission. To detect any unwanted repeats or adjustments in the data stream, which are common indicators of MITM attacks, the technique ensures that these hashes are different. The third phase entails observing and analyzing patterns of communication. The program predicts a communication pattern using the sender and recipient's public keys and then compares it to the observed communication pattern. This novel method utilizes the reliability of anticipated contacts to detect any irregularities in the communication process that could indicate the existence of an unauthorized individual.

Finally, the algorithm examines irregularities in the transfer of data. The process analyses different attributes of the encrypted data to identify any abnormalities that surpass a predetermined threshold. This thorough examination guarantees the detection of even minor indications of intervention or manipulation, thereby enhancing the level of security. The algorithm innovates by incorporating numerous detection methods, each targeting distinct vulnerabilities, to provide a robust and reliable protection mechanism specifically tailored for IoT contexts with limited resources.



```
Node 37

Mobility Model: ns3::RandomWaypointMobilityModel

NetDevice 0:
  Type: ns3::WifiNetDevice
  IPv4 Addresses: 10.1.1.38/255.255.255.0
  IPv6 Addresses: fe80::200:ff:fe00:42//64;
2001:db8::200:ff:fe00:42//64
  MAC Address: 02-06-00:00:00:00:00:42

NetDevice 1:
  Type: ns3::LoopbackNetDevice
  IPv4 Addresses: 127.0.0.1/255.0.0.0
  IPv6 Addresses: ::1//128
  MAC Address: 02-06-00:00:00:00:00:00

NetDevice 2:
  Type: ns3::IoTNetDevice
  MAC Address: 02-06-00:00:00:00:00:42
```

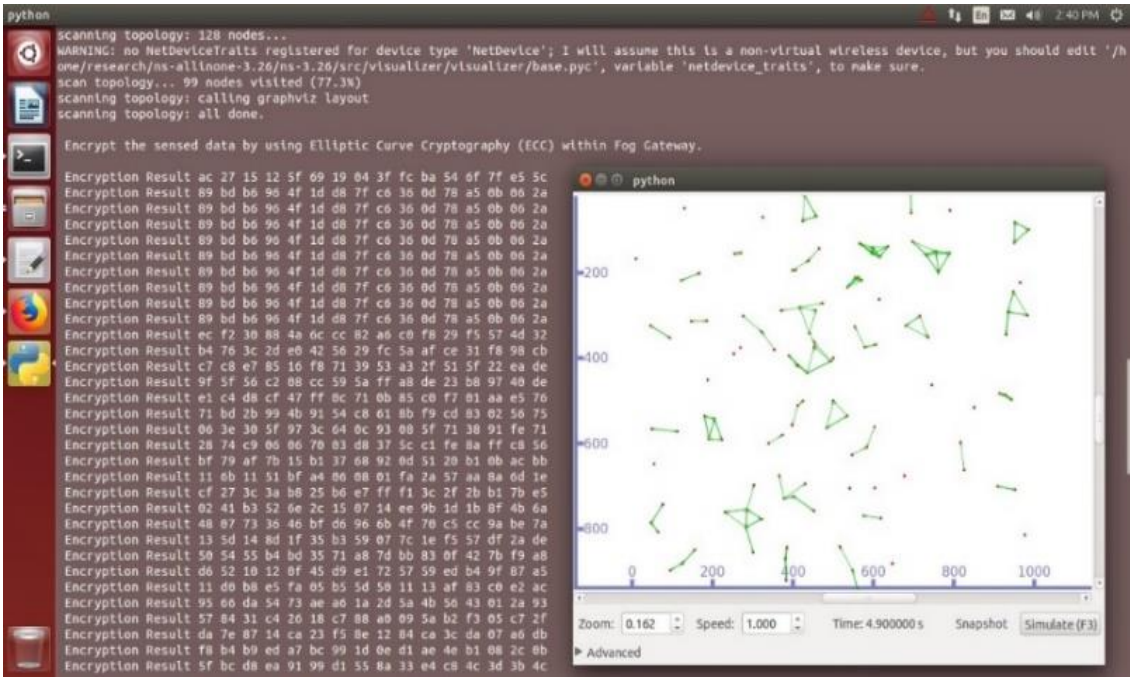
Figure 4. Initial setup screenshot

4. RESULTS AND DISCUSSION

Performed a detailed analysis of the implementation, focusing on key performance metrics across different stages, to evaluate our secured open standard framework for IoT applications. The initial phase of the implementation plan has resulted in the creation of a comprehensive network infrastructure consisting of 100 IoT devices, 25 users, 1 fog gateway, 1 micro datacenter, and 1 cloud server. Figure 4 shows the detail of the network setup of single node. This configuration offers a strong and reliable setting to evaluate the effectiveness of the framework in practical situations. Our investigation encompasses a variety of critical factors, including power consumption, resource usage, average energy consumption, average end-to-end delay, and throughput. Aimed to measure the performance impact of the security mechanisms and evaluate the overall effectiveness of the proposed framework by analyzing these indicators.

Figure 5 shows a setup where a network simulation is running, using the NS-3.26 network simulator. The left terminal displays logs and encryption results for a network structure consisting of 128 nodes. The procedure entails scanning the network architecture, implementing a Graphviz layout, and encrypting sensed data using ECC within a fog gateway. The terminal displays many lines of encrypted data, suggesting effective encryption of information from different nodes. The Python window on the right displays the network topology, illustrating nodes connected by green lines, which indicate communication links, and red dots denoting the nodes themselves.

IoT devices receive and transmit packets to the cloud server during the simulation. Log entries show that the system finds a MITM attack by analyzing the keys, as shown by the "man-in-the-middle (MITM) attack detected" messages as shown in Figure 6. The nodes and links undergo dynamic changes during the simulation, effectively demonstrating the flow of data and interactions within the network.



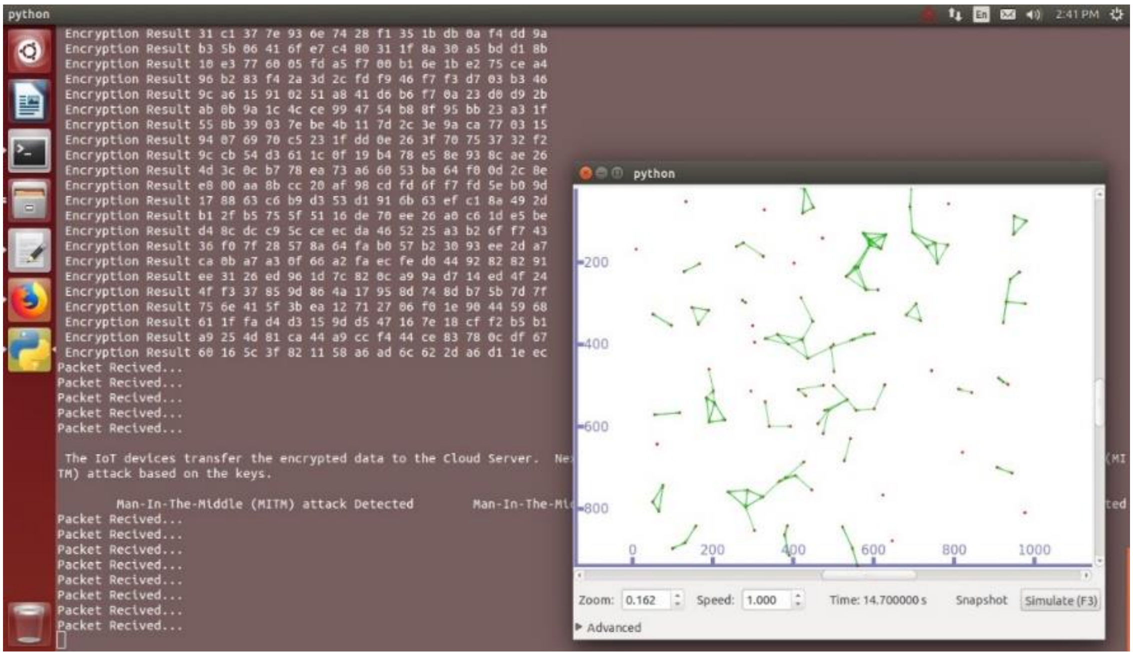
```
scanning topology: 128 nodes...
WARNING: no NetDeviceTraits registered for device type 'NetDevice'; I will assume this is a non-virtual wireless device, but you should edit '/h
one/research/ns-allinone-3.26/ns-3.26/src/visualizer/visualizer/base.pyc', variable 'netdevice_traits', to make sure.
scan topology... 99 nodes visited (77.3%)
scanning topology: calling graphviz layout
scanning topology: all done.

 Encrypt the sensed data by using Elliptic Curve Cryptography (ECC) within Fog Gateway.

 Encryption Result ac 27 15 12 5f 69 19 04 3f fc ba 54 6f 7f e5 5c
 Encryption Result 89 bd b6 96 4f 1d d8 7f c6 36 0d 78 a5 0b 06 2a
 Encryption Result 89 bd b6 96 4f 1d d8 7f c6 36 0d 78 a5 0b 06 2a
 Encryption Result 89 bd b6 96 4f 1d d8 7f c6 36 0d 78 a5 0b 06 2a
 Encryption Result 89 bd b6 96 4f 1d d8 7f c6 36 0d 78 a5 0b 06 2a
 Encryption Result 89 bd b6 96 4f 1d d8 7f c6 36 0d 78 a5 0b 06 2a
 Encryption Result 89 bd b6 96 4f 1d d8 7f c6 36 0d 78 a5 0b 06 2a
 Encryption Result 89 bd b6 96 4f 1d d8 7f c6 36 0d 78 a5 0b 06 2a
 Encryption Result 89 bd b6 96 4f 1d d8 7f c6 36 0d 78 a5 0b 06 2a
 Encryption Result 89 bd b6 96 4f 1d d8 7f c6 36 0d 78 a5 0b 06 2a
 Encryption Result ec f2 30 88 4a 6c cc 82 a6 c0 f8 29 f5 57 4d 32
 Encryption Result b4 76 3c 2d e0 42 56 29 fc 5a af ce 31 f8 98 cb
 Encryption Result c7 c8 e7 85 16 f8 71 39 53 a3 2f 51 5f 22 ea de
 Encryption Result 9f 5f 56 c2 08 cc 59 5a ff a8 de 23 b8 97 40 de
 Encryption Result e1 c4 d8 cf 47 ff 0c 71 0b 85 c0 f7 01 aa e5 76
 Encryption Result 71 bd 2b 99 4b 91 54 c8 61 8b f9 cd 03 02 56 75
 Encryption Result 06 3e 30 5f 97 3c 64 0c 93 08 5f 71 38 91 fe 71
 Encryption Result 28 74 c9 06 06 70 03 d8 37 5c c1 fe 8a ff c8 56
 Encryption Result bf 79 af 7b 15 b1 37 68 92 0d 51 20 b1 0b ac bb
 Encryption Result 11 6b 11 51 bf a4 06 08 01 fa 2a 57 aa 8a 6d 1e
 Encryption Result cf 27 3c 3a b8 25 b6 e7 ff f1 3c 2f 2b b1 7b e5
 Encryption Result 02 41 b3 52 6e 2c 15 07 14 ee 9b 1d 1b 8f 4b 6a
 Encryption Result 48 07 73 36 46 bf d6 96 6b 4f 70 c5 cc 9a be 7a
 Encryption Result 13 5d 14 8d 1f 35 b3 59 07 7c 1e f5 57 df 2a de
 Encryption Result 50 54 55 b4 bd 35 71 a8 7d bb 83 0f 42 7b f9 a8
 Encryption Result d6 52 10 12 0f 45 d9 e1 72 57 59 ed b4 9f 87 a5
 Encryption Result 11 d0 b8 e5 fa 05 b5 5d 50 11 13 af 83 c0 e2 ac
 Encryption Result 95 66 da 54 73 ae a6 1a 2d 5a 4b 56 43 01 2a 93
 Encryption Result 57 84 31 c4 26 18 c7 88 a0 09 5a b2 f3 05 c7 2f
 Encryption Result da 7e 87 14 ca 23 f5 8e 12 84 ca 3c da 07 a6 db
 Encryption Result f8 b4 b9 ed a7 bc 99 1d 0e d1 ae 4e b1 08 2c 0b
 Encryption Result 5f bc d8 ea 91 99 d1 55 8a 33 e4 c8 4c 3d 3b 4c
```

Zoom: 0.162 Speed: 1.000 Time: 4.900000 s

Figure 5. Screenshot showing encryption and nodes communication



```
 Encryption Result 31 c1 37 7e 93 6e 74 28 f1 35 1b db 0a f4 dd 9a
 Encryption Result b3 5b 06 41 6f e7 c4 80 31 1f 8a 30 a5 bd d1 8b
 Encryption Result 10 e3 77 60 05 fd a5 f7 00 b1 6e 1b e2 75 ce a4
 Encryption Result 96 b2 83 f4 2a 3d 2c fd f9 46 f7 f3 d7 03 b3 46
 Encryption Result 9c a6 15 91 02 51 a8 41 d6 b6 f7 0a 23 d0 d9 2b
 Encryption Result ab 0b 9a 1c 4c ce 99 47 54 b8 8f 95 bb 23 a3 1f
 Encryption Result 55 8b 39 03 7e be 4b 11 7d 2c 3e 9a ca 77 03 15
 Encryption Result 94 07 69 70 c5 23 1f dd 0e 26 3f 70 75 37 32 f2
 Encryption Result 9c cb 54 d3 61 1c 0f 19 b4 78 e5 8e 93 8c ae 26
 Encryption Result 4d 3c 0c b7 78 ea 73 a6 60 53 ba 64 f0 0d 2c 8e
 Encryption Result e8 00 aa 8b cc 20 af 98 cd fd 6f f7 fd 5e b0 9d
 Encryption Result 17 88 63 c6 b9 d3 53 d1 91 6b 63 ef c1 8a 49 2d
 Encryption Result b1 2f b5 75 5f 51 16 de 70 ee 26 a0 c6 1d e5 be
 Encryption Result d4 8c dc c9 5c ce ec da 46 52 25 a3 b2 6f f7 43
 Encryption Result 36 f0 7f 28 57 8a 64 fa b0 57 b2 30 93 ee 2d a7
 Encryption Result ca 0b a7 a3 0f 66 a2 fa ec fe d0 44 92 82 82 91
 Encryption Result ee 31 26 ed 96 1d 7c 82 8c a9 9a d7 14 ed 4f 24
 Encryption Result 4f f3 37 85 9d 86 4a 17 95 8d 74 8d b7 5b 7d 7f
 Encryption Result 75 6e 41 5f 3b ea 12 71 27 06 f0 1e 90 44 59 68
 Encryption Result 61 1f fa d4 d3 15 9d d5 47 16 7e 18 cf f2 b5 b1
 Encryption Result a9 25 4d 81 ca 44 a9 cc f4 44 ce 83 78 0c df 67
 Encryption Result 60 16 5c 3f 82 11 58 a6 ad 6c 62 2d a6 d1 1e ec
Packet Recived...
Packet Recived...
Packet Recived...
Packet Recived...
Packet Recived...

 The IoT devices transfer the encrypted data to the Cloud Server.  Ne                                                                  (MI
TM) attack based on the keys.

        Man-In-The-Middle (MITM) attack Detected        Man-In-The-Mi                                                                 ted
Packet Recived...
Packet Recived...
Packet Recived...
Packet Recived...
Packet Recived...
Packet Recived...
Packet Recived...
Packet Recived...
```

Zoom: 0.162 Speed: 1.000 Time: 14.700000 s

Figure 6. Screenshot indicating MITM detection

As depicted in Figure 7, the analysis of energy consumption across various IoT nodes provides valuable insights into the network's operating dynamics and effectiveness. Every IoT node exhibits a steady rise in energy usage as time progresses. This trend suggests that as the simulation advances, the nodes consistently consume energy, possibly because of continual communication, processing workloads, and encryption activities. The consistent linear trend indicates a balanced allocation of workload among the nodes, with no notable surges or declines in energy consumption. The variations in energy usage among the nodes suggest that some nodes are operating more intensively or performing more demanding functions within the network.

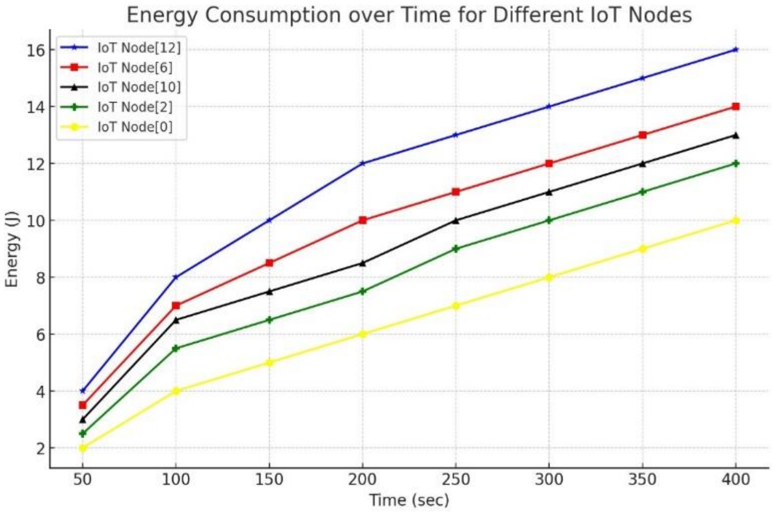


Figure 7. Cumulative energy consumption plot for some IoT nodes

Figure 8 illustrates the processing usage percentage over time for three distinct schemes: From [26], [27], and the proposed scheme. All three systems show significant variations in processor usage over time. This implies that the tasks under processing display variability, leading to sporadic increases and decreases in utilization. The significant fluctuation in [26] indicates that the Scheme can effectively manage demanding processing demands. However, it may also encounter periods of underutilization. The proposed method demonstrates fluctuations, but overall, it maintains a steadier performance in comparison to the other two schemes. The observed stability indicates that the suggested system distributes the processing burden in a more balanced manner over time, potentially enhancing overall efficiency. The consistency of the proposed scheme's processor utilization suggests that it has the potential to be more scalable. When there is an increase in the number of jobs or IoT devices, a more stable scheme can effectively manage the additional load without experiencing severe performance degradation. Therefore, the suggested approach becomes a feasible choice for larger and more intricate IoT networks.

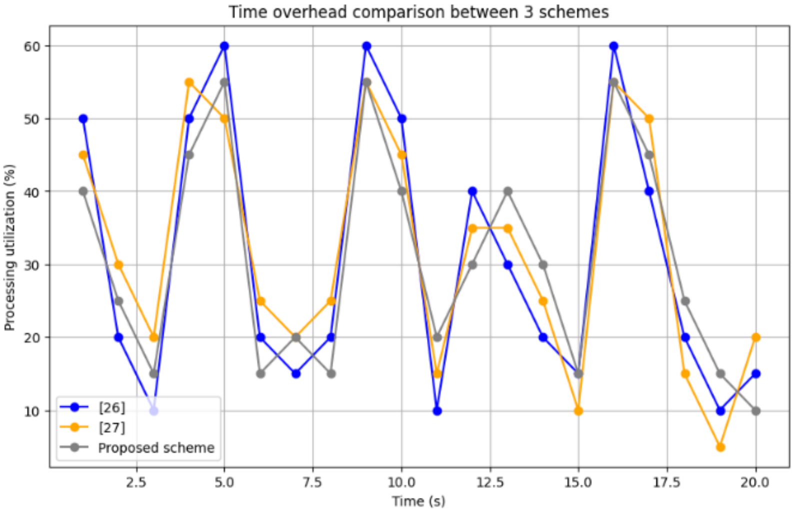


Figure 8. Overhead time comparison

Figure 9 illustrates the power consumption percentage over time for three distinct schemes: plan [26], scheme [27], and the proposed plan. Each of the three designs demonstrates substantial variations in power use over time. The execution of tasks demonstrates variability, leading to intermittent surges and declines in power usage. The variations indicate that the workload is not consistent, and the processing requirements vary dynamically. The proposed approach demonstrates a more equitable distribution of tasks, resulting in fewer significant spikes and drops in workload. The proposed design exhibits peaks of up to 35% at 5 and 16 seconds, which is comparable to the other schemes but with less intensity. The proposed strategy's stability demonstrates its ability to equally distribute power demand across time, which has the potential to improve overall efficiency. The suggested scheme's capacity to sustain consistent power consumption despite fluctuating workloads indicates its resilience and flexibility. The resilience of IoT applications is essential in real-world scenarios, as the tasks they handle can vary unpredictably in terms of nature and severity.

Figure 10 illustrates the correlation between the quantity of IoT devices and the realized throughput of the proposed scheme. The throughput exhibits a direct proportionality to the number of IoT devices, resulting in a linear rise. Because the correlation is linear, it looks like the suggested method can handle adding more devices without losing much performance, showing that it can be used on a large scale. The steady increase in throughput provides evidence that the suggested approach has a high level of scalability. As the IoT networks grow, it is crucial to be able to sustain or enhance throughput to ensure that the network can handle a significant number of devices without sacrificing its functionality. Ensuring a consistently high level of data processing capacity allows the system to effectively handle the increasing number of linked devices in diverse real-world situations.

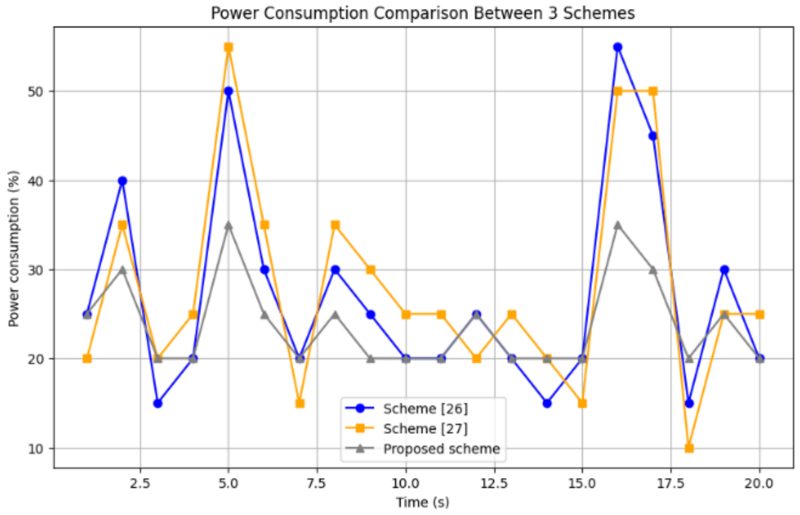


Figure 9. Power consumption comparison

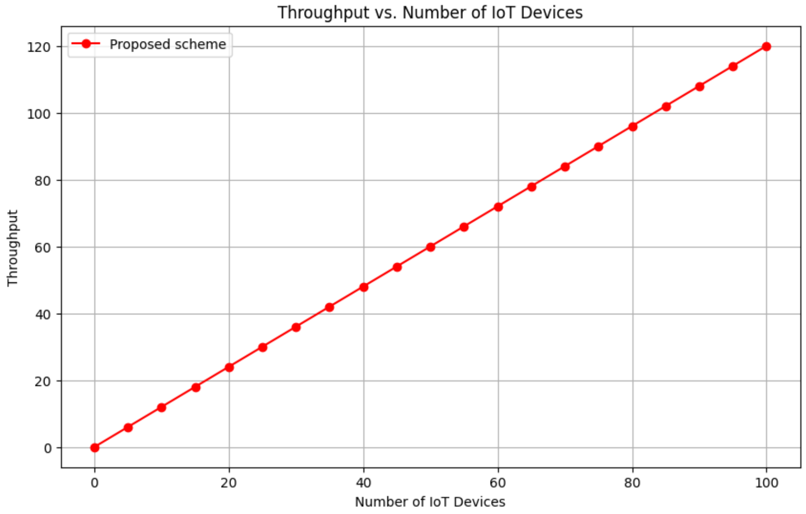


Figure 10. Throughput vs number of IoT devices

5. CONCLUSION

This research presents an innovative and secure open standard framework for IoT applications, which aims to improve security and efficiency in IoT ecosystems. ECC is used in the suggested system to protect IoT connections by ensuring safe device registration, data encryption, and the detection of MITM attacks. The use of fog computing enriches the architecture by bringing computational and storage resources closer to the edge, resulting in reduced latency and improved overall performance. The use of ECC for cryptographic key generation and encryption provides robust security with smaller key sizes, making it suitable for IoT devices with limited resources. The framework guarantees a safe connection by implementing stringent device authentication and data encryption procedures. The system enhances data processing efficiency and reduces power consumption by offloading expensive computing activities from IoT devices through data encryption at the fog gateway. The experimental results show that the suggested framework efficiently adapts to the increasing number of IoT devices. Its linear increase in throughput and balanced power consumption patterns demonstrate the framework's capacity to manage growing workloads without substantial performance decline. The affirmative empirical findings confirm the efficacy of the framework, rendering it a potential resolution for forthcoming IoT implementations. This research makes a substantial contribution to the improvement of IoT security and establishes a strong basis for future investigation and enhancement in this crucial domain.

REFERENCES

[1] J. Wang, M. K. Lim, C. Wang, and M.-L. Tseng, “The evolution of the internet of things (IoT) over the past 20 years,” *Computers & Industrial Engineering*, vol. 155, May 2021, doi: 10.1016/j.cie.2021.107174.

[2] M. Beale, H. Uchiyama, and J. C. Clifton, “IoT Evolution: what’s Next?,” *IEEE Wireless Communications*, vol. 28, no. 5, pp. 5–7, Oct. 2021, doi: 10.1109/MWC.2021.9615126.

[3] K. Abdul Sattar and A. Al-Omary, “A survey: security issues in IoT environment and IoT architecture,” in *3rd Smart Cities Symposium (SCS 2020)*, 2021, pp. 96–102, doi: 10.1049/icp.2021.0894.

[4] S. Javanmardi, M. Shojafar, R. Mohammadi, M. Alazab, and A. M. Caruso, “An SDN perspective IoT-Fog security: a survey,” *Computer Networks*, vol. 229, Jun. 2023, doi: 10.1016/j.comnet.2023.109732.

[5] 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.

[6] A. Srivastava and A. Kumar, “A review on authentication protocol and ECC in IoT,” in *2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, Mar. 2021, pp. 312–319, doi: 10.1109/ICACITE51222.2021.9404766.

[7] H. AlMajed and A. AlMogren, “A secure and efficient ECC-based scheme for edge computing and internet of things,” *Sensors*, vol. 20, no. 21, pp. 1–31, Oct. 2020, doi: 10.3390/s20216158.

[8] V. Rao and K. V. Prema, “A review on lightweight cryptography for internet-of-things based applications,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 9, pp. 8835–8857, Sep. 2021, doi: 10.1007/s12652-020-02672-x.

[9] R. Badhwar, “Man-in-the-middle attack prevention,” in *The CISO’s Next Frontier*, Cham: Springer International Publishing, 2021, pp. 223–229.

[10] J. Mohanty, S. Mishra, S. Patra, B. Pati, and C. R. Panigrahi, “IoT security, challenges, and solutions: a review,” *Progress in Advanced Computing and Intelligent Engineering*, 2021, pp. 493–504, doi: 10.1007/978-981-15-6353-9_46.

[11] J. Tournier, F. Lesueur, F. Le Mouël, L. Guyon, and H. Ben-Hassine, “A survey of IoT protocols and their security issues through the lens of a generic IoT stack,” *Internet of Things*, vol. 16, Dec. 2021, doi: 10.1016/j.iot.2020.100264.

[12] H. HaddadPajouh, A. Dehghantanha, R. M. Parizi, M. Aledhari, and H. Karimipour, “A survey on internet of things security: requirements, challenges, and solutions,” *Internet of Things*, vol. 14, Jun. 2021, doi: 10.1016/j.iot.2019.100129.

[13] T. Mansouri, M. R. S. Moghadam, F. Monshizadeh, and A. Zareravasan, “Corrigendum to: IoT data quality issues and potential solutions: a literature review,” *The Computer Journal*, vol. 66, no. 6, pp. 1563–1563, Jun. 2023, doi: 10.1093/comjnl/bxac014.

[14] P. G. Chiara, “The IoT and the new EU cybersecurity regulatory landscape,” *International Review of Law, Computers and Technology*, vol. 36, no. 2, pp. 118–137, May 2022, doi: 10.1080/13600869.2022.2060468.

[15] S. Saeed, N. Z. Jhanjhi, M. Naqvi, M. Humayun, and S. Ahmed, “Ransomware: a framework for security challenges in Internet of Things,” in *2020 2nd International Conference on Computer and Information Sciences (ICCIS)*, Oct. 2020, pp. 1–6, doi: 10.1109/ICCIS49240.2020.9257660.

[16] A. Nazir *et al.*, “Advancing IoT security: A systematic review of machine learning approaches for the detection of IoT botnets,” *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 10, 2023, doi: 10.1016/j.jksuci.2023.101820.

[17] T. Sobb, B. Turnbull, and N. Moustafa, “Supply chain 4.0: a survey of cyber security challenges, solutions and future directions,” *Electronics*, vol. 9, no. 11, Nov. 2020, doi: 10.3390/electronics9111864.

[18] R. Ahmad, I. Alsmadi, W. Alhamdani, and L. Tawalbeh, “Zero-day attack detection: a systematic literature review,” *Artificial Intelligence Review*, vol. 56, no. 10, pp. 10733–10811, Oct. 2023, doi: 10.1007/s10462-023-10437-z.

[19] A. Hinduja and M. Pandey, “An ANP-GRA-based evaluation model for security features of IoT systems,” in *Advances in Intelligent Systems and Computing*, 2020, pp. 243–253.

[20] I. Batra, S. Verma, Kavita, and M. Alazab, “A lightweight IoT-based security framework for inventory automation using wireless sensor network,” *International Journal of Communication Systems*, vol. 33, no. 4, Mar. 2020, doi: 10.1002/dac.4228.

[21] S. Ebadinezhad and T. E. Mobolade, “A novel cloud-based IoT framework for secure health monitoring,” *Sustainability*, vol. 16, no. 3, Feb. 2024, doi: 10.3390/su16031349.

[22] S. Rostampour, M. Safkhani, Y. Bendavid, and N. Bagheri, “ECCbAP: a secure ECC-based authentication protocol for IoT edge devices,” *Pervasive and Mobile Computing*, vol. 67, Sep. 2020, doi: 10.1016/j.pmcj.2020.101194.

[23] U. Chatterjee, S. Ray, M. K. Khan, M. Dasgupta, and C.-M. Chen, “An ECC-based lightweight remote user authentication and key management scheme for IoT communication in context of fog computing,” *Computing*, vol. 104, no. 6, pp. 1359–1395, Jun. 2022, doi: 10.1007/s00607-022-01055-8.

[24] K. Raja, “Detection and prevention of ransomware attacks using AES and RSA algorithms,” *DS Journal of Digital Science and Technology*, vol. 1, no. 1, pp. 1–9, Jul. 2022, doi: 10.59232/DST-V1I1P101.

[25] V. L. Narayana and R. S. M. L. Patibandla, “An efficient fog-based model for secured data communication,” in *Integration of Cloud Computing with Internet of Things*, Wiley, 2021, pp. 41–55.

[26] A. G. Reddy, A. K. Das, V. Odelu, A. Ahmad, and J. S. Shin, “A privacy-preserving three-factor authenticated key agreement protocol for client–server environment,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 2, pp. 661–680, 2019, doi: 10.1007/s12652-018-0716-4.

[27] E. T. Oladipupo *et al.*, “An efficient authenticated elliptic curve cryptography scheme for multicore wireless sensor networks,” *IEEE Access*, vol. 11, pp. 1306–1323, 2023, doi: 10.1109/ACCESS.2022.3233632.

BIOGRAPHIES OF AUTHORS

Krishnapura Srinivasa Ravindra completed his bachelor's degree in Electronics and 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 18yrs 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.

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 from Jawaharlal Nehru National College of Engineering Shimoga. He is currently working as professor in Jain University Bengaluru, India. His research interests are in the field of real-time and embedded systems, machine learning-internet of things. He has published various Patents, research papers in journal and conferences across India, also in the IEEE international conference in Okinawa, Japan (visited) 2008. Under his leadership the ISE Department was accredited twice by NBA. Under his leadership the ISE Department of Jain University was accredited National Board of Accreditation for the duration 2022 to 2025. Also, during 2008 to 2011, ISE Department of Don Bosco Institute of Technology, Bangalore is accredited. As HOD of ISE actively participated and contributed in the accreditation of the institution by NAAC with A++ Grade for the duration 2022 – 2028 for ISE Department of Jain University. 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 one patent GRANTED for 20 Years, three patents are stepping towards grant status. One research scholar under his guidance was awarded a Ph.D. degree. Two more research scholars submitted thesis. He can be contacted at email: r.panduranga@jainuniversity.ac.in.