JOURNAL OF BASIC SCIENCE AND ENGINEERING

A SECURE AND EFFICIENT FRAMEWORK FOR IOT NETWORKS USING BLOCKCHAIN-ENABLED KEY MANAGEMENT, CONTEXT-AWARE ROUTING, AND LIGHTWEIGHT CRYPTOGRAPHY

Vinay B.[1], Dr. Balakrishna R.[2]*, Dr. Panduranga Rao M.V.[3]

[1] Research Scholar, VTU RRC, Visvesvaraya Technological University, Belagavi
[2] Supervisor, Principal & Professor, Department of Computer Science & Engineering
Rajarajeswari College of Engineering, Bangalore, Karnataka
[3] Professor & Co-Supervisor, Dept. of CSE, Faculty of Engg. & Tech., Jain (Deemed-to-be University), Bangalore
* Corresponding author Email id : rayankibala@gmail.com
DOI: https://doie.org/10.0113/Jbse.2025629681

Article History : **Received: July 2024** **Revised: Sept 2024** **Accepted: December 2024**

***Abstract* : -** The swift expansion of the Internet of Things (IoT) has transformed various sectors, encompassing smart cities, healthcare, and industrial automation. Despite this, IoT networks have security problems like unauthorized access, data corruption, and limited resources that mean strong solutions are needed to make sure safe communication and good data management. This document presents a comprehensive framework that integrates secure routing, lightweight authentication, and blockchain-based key management to tackle these challenges effectively. The framework utilizes Elliptic Curve Cryptography (ECC) to ensure efficient and secure device authentication. It uses a GRU-based Intrusion Detection System (IDS) to find malicious nodes before they do any damage and a context-aware routing algorithm to send data more efficiently. When combined with Hash-based Message Authentication Code (HMAC), a genetic algorithm-driven sub-key generation mechanism makes data encryption and integrity much better. The outcomes of the simulation confirm the framework's efficacy, showcasing a 40% reduction in latency, a 28.6% decline in energy consumption, and a packet delivery ratio of 98.5%. The framework also achieves high security robustness, mitigating threats such as MITM, replay, brute force, and DDoS attacks with success rates exceeding 90%. The attributes of scalability, energy efficiency, and resilience render it highly appropriate for practical IoT implementations, especially within essential domains such as smart cities and industrial automation. This study offers a substantial advancement in the creation of secure and efficient IoT ecosystems, establishing a foundation for future improvements in dynamic and resource-limited settings.

***Keywords* :** Secure Routing, IoT Authentication, Blockchain Key Management, Intrusion Detection System, Lightweight Encryption.

I. Introduction

The Internet of Things (IoT) is transforming the interaction between devices, facilitating seamless communication and automation across various sectors, including healthcare, smart cities, and industrial automation [1]. The rapid proliferation of IoT devices presents considerable challenges, especially in ensuring secure communication and protecting data from unauthorized access. These devices frequently function within environments that have limited resources, rendering them vulnerable to various forms of attacks, including unauthorized access, data tampering, and interception [2]. Maintaining the integrity and confidentiality of IoT communications requires a strong routing mechanism and an effective authentication scheme. Conventional approaches, nonetheless, encounter constraints when it comes to accommodating the dynamic and diverse characteristics of IoT networks [3].

Moreover, the implementation of secure routing frequently escalates computational and energy requirements, thereby preventing further challenges for devices with limited resources. This study focuses on the development of a context-aware secure routing framework that incorporates a lightweight authentication mechanism to tackle the identified issues. The proposed system utilizes elliptic curve cryptography (ECC) to ensure device verification, incorporates blockchain technology for decentralized key management, and implements intrusion detection systems (IDS) to reduce the risk of malicious activities. This work enhances data security and energy efficiency, thereby contributing to the development of robust IoT ecosystems that can effectively prevent data theft and ensure uninterrupted communication in demanding environments.

II. Overview of IoT Ecosystems

The IoT ecosystem is a network of interconnected devices, sensors, and systems designed to collect, share, and process data in real-time. The spectrum of these devices encompasses commonplace items such as smart home appliances, as well as sophisticated machinery employed in the realm of industrial automation. The integration of IoT facilitates uninterrupted communication and automation, leading to marked improvements in operational efficiency across various sectors such as healthcare, agriculture, transportation, and smart cities [4,5]. The swift expansion and extensive integration of IoT technologies have revealed weaknesses that jeopardize their security and dependability.

The architecture of IoT ecosystems is characterized by inherent heterogeneity, comprising a wide array of devices that exhibit differing computational capabilities and utilize various communication protocols [6]. The presence of this diversity introduces compatibility challenges and expands the attack surface, thereby providing more opportunities for malicious actors to exploit vulnerabilities. The limitations inherent in numerous IoT devices, including restricted processing capabilities, memory, and energy resources, intensify these vulnerabilities. This situation complicates the implementation of effective security measures while maintaining optimal performance levels. A significant vulnerability in IoT systems arises from the absence of robust authentication and encryption mechanisms. Numerous IoT devices depend on inadequate authentication protocols, rendering them vulnerable to unauthorized access and potential data breaches [7]. Exploitation of these vulnerabilities allows attackers to intercept sensitive information, manipulate the operations of devices, or inject harmful commands into the network.

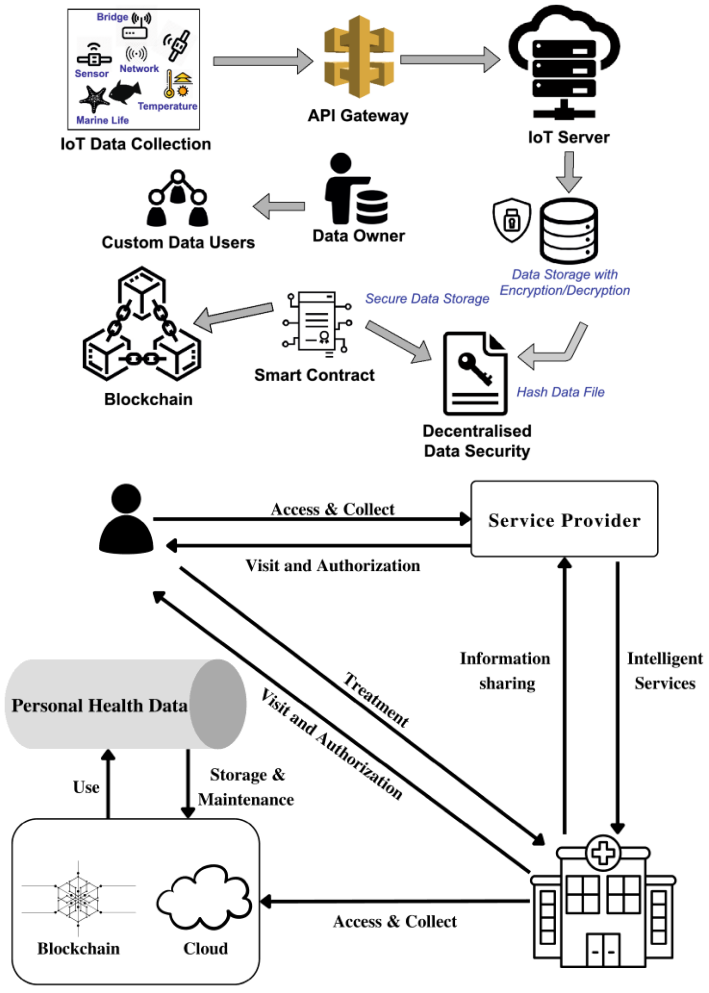

Figure 1. Secured IoT Data Management [26]

Insecure communication channels exacerbate the issue, as data transmitted between IoT devices frequently lacks encryption. IoT systems are susceptible to various security threats, including eavesdropping, man-in-the-middle (MITM) attacks, and data tampering. These types of attacks pose significant risks to data confidentiality

and integrity while also having the potential to disrupt essential operations, especially within healthcare and industrial environments [8]. A notable challenge is the absence of secure key management. Conventional key management systems rely on centralized authorities, which can lead to vulnerabilities due to a single point of failure. The integrity of a central authority is crucial, as its compromise can threaten the entire network's security, enabling attackers to gain access to sensitive information and exert control over devices.

Decentralized methodologies, including blockchain-based key management systems, present promising solutions; however, they necessitate additional optimization to function effectively within resource-limited IoT settings [9,10]. Blockchain technology, when combined with smart contracts, establishes a decentralized framework that ensures data integrity and secure storage through the generation of hashed data files as illustrated in Figure 1 [26]. The architecture guarantees that data proprietors maintain authority over their information, while authorized data consumers can access it securely via permissioned interfaces. The integration of encryption decentralized key management, and secure contracts within the framework significantly bolsters IoT data security, effectively mitigating the risks of unauthorized access and data theft.

The Mirai botnet attack utilized IoT devices characterized by inadequate security configurations, underscoring the significant repercussions that these vulnerabilities can impose on the global internet infrastructure. The dynamic and distributed characteristics of IoT networks introduce further security challenges. The dynamic nature of devices joining and leaving the network presents challenges in establishing trust and maintaining secure communication pathways [11]. IDS, alongside context-aware routing mechanisms, play a crucial role in risk mitigation by identifying and isolating malicious devices. However, these systems need to be lightweight and adaptive for optimal performance in real-time environments.

Mitigating these vulnerabilities necessitates a comprehensive strategy. To safeguard IoT systems from emerging threats, it is crucial to implement secure routing protocols, robust authentication mechanisms, and lightweight cryptographic techniques. Furthermore, implementing decentralized and scalable security solutions, including blockchain-based key management, has the potential to improve trust and resilience. Addressing these challenges enables IoT ecosystems to attain the necessary security and reliability levels to support their expanding role in critical applications. This study aims to create solutions that guarantee secure, efficient, and theft-resistant communication within IoT networks.

III. Significance of Secure Routing and Robust Authentication in IoT Networks

In IoT networks, the implementation of secure routing protocols is crucial for safeguarding the integrity of data transmission. This guarantees that devices deliver information to their designated endpoint without any risk of interception or unauthorized alterations. IoT networks typically function in distributed and dynamic settings, characterized by the frequent movement of devices within the network. Due to its inherent complexity and characteristics, routing becomes vulnerable to various attacks such as eavesdropping, data modification, and routing misdirection. Exploitation of these vulnerabilities by attackers can lead to the rerouting of data to unauthorized nodes, which may result in data theft. Secure routing protocols enable IoT networks to adapt dynamically to changing conditions, safeguarding the confidentiality and integrity of data. Context-aware routing mechanisms analyse real-time data, including device status and environmental conditions, to determine optimal paths for data transmission. These protocols aim to avoid compromised nodes and prevent sensitive data from traveling through insecure routes. Using secure routing protocols also reduces the risks of attacks like Distributed Denial of Service (DDoS), in which attackers flood the network with harmful traffic to stop people from talking to each other [12]. Routing protocols designed for efficiency can identify irregular traffic patterns and subsequently redirecting data to ensure the continued functionality of the network.

Robust authentication represents a vital component of IoT security. Given the extensive number of devices integrated into IoT networks, it is essential to authenticate the legitimacy of each device to mitigate the risk of unauthorized access. Weak credentials, frequently observed in IoT devices, render networks vulnerable to various attacks, including spoofing, replay, and MITM attacks. An attacker may exploit vulnerabilities by impersonating a legitimate device, enabling them to intercept data, which can lead to significant disruptions. Advanced cryptographic techniques, including ECC, provide a robust solution for authentication mechanisms. ECC facilitates a balance between minimal resource usage and robust security measures, rendering it particularly suitable for IoT devices with limited capabilities. Nonce-based mutual authentication protocols serve to mitigate replay attacks by guaranteeing the uniqueness of authentication requests, thereby preventing their reuse by

potential attackers.

This study focuses on identifying and mitigating vulnerabilities within IoT networks through the development of a framework that combines context-aware secure routing mechanisms with strong authentication protocols. Using ECC for device authentication, blockchain-based key management for decentralized security, and IDS to find malicious nodes are all parts of the proposed solution. This makes sure that all data is safe and secure from beginning to end. The implementation of these measures is essential for the protection of IoT ecosystems from data theft and thereby maintaining their reliability and security for vital applications.

IV. Related Works

Recent years have seen notable progress in IoT security, especially concerning IDS, routing protocols, and cryptographic mechanisms. Alotaibi and Ilyas (2023) investigated approaches aimed at improving the efficacy of IDS within IoT networks by employing binary classification techniques to differentiate between normal and abnormal traffic. The methodology employed ensemble learning techniques, integrating complementary classifiers to enhance accuracy. The methodology demonstrated a notable accuracy rate of 98.63%, indicating its efficacy for intrusion detection within IoT environments [13]. In the same direction, Arshad *et al*. introduced an ensemble learning model aimed at identifying botnet activity within network traffic. The system demonstrated exceptional performance, attaining a 99.7% accuracy rate and a detection time of merely 12.99 seconds, highlighting the effectiveness of ensemble-based methodologies [14]. Debicha et al. emphasized the susceptibility of IDSs to adversarial attacks. The research carried out in a controlled setting revealed the vulnerability of ML-based IDS to evasion attacks facilitated by adversarial algorithms [15].

Ilyas et al. addressed significant issues in WSNs through the introduction of a three-layer cluster-based routing protocol that incorporates wireless energy harvesting. Their approach significantly prolonged the operational lifetime of the network, improved throughput, and minimized packet losses and delays. Additionally, implementing a blacklisting process to isolate malicious nodes has enhanced network security and robustness [16]. Yarinezhad and Azizi (2021) proposed a tree-based routing protocol for green IoT networks featuring a mobile sink. The protocol effectively minimized end-to-end latency and improved power efficiency through the implementation of a tree-based structure that maintains minimal control overhead, thus optimizing routing costs and enhancing communication efficiency [17]. Ramkumar and Vadivel (2021) introduced the Multi-Adaptive Routing Protocol (MARP), a protocol inspired by the natural behaviors of fish, with the aim of enhancing the performance of IoT-based ad-hoc networks. Simulations performed using NS3 have shown that MARP outperforms current routing protocols in terms of minimizing energy consumption and delays while also enhancing the overall lifetime of the network [18].

Recent developments in cryptographic techniques for IoT networks have been significant. Abdaoui *et al.* introduced a unique methodology that combines ECC with fuzzy logic-influenced random number generation. This method increased the safety of key generation by creating keys that are both cryptographically strong and hard to predict, as shown by tests of their randomness and reliability [19]. To improve ECC operations, Lara-Nino *et al.* created an FPGA-based acceleration engine that used binary Edwards curves. Their methodology tackled resource limitations in IoT devices by improving computational efficiency and reducing overhead, rendering it especially appropriate for implementation in low-power settings [20]. Verma *et al.* presented a framework that utilizes ECC for mutual authentication and key agreement, facilitating secure communication between IoT devices and fog servers. The analysis demonstrated the framework's computational efficiency and minimized storage needs relative to current methodologies, underscoring its efficacy in resource-limited IoT networks [21, 22].

In the domain of blockchain-enabled security, Pajooh *et al*. presented a multi-layered blockchain framework for IoT networks. The model employed clustering principles alongside a hybrid evolutionary computation algorithm to create secure clusters within the IoT network. It functioned on the Hyperledger Fabric platform, thereby guaranteeing decentralized and secure operations [23]. For smart farming applications, Chaganti *et al*. proposed a cloud-integrated security framework that uses behavioral pattern analysis to facilitate anomaly detection. The system utilized blockchain-based smart contracts to securely record security information and reduce threats within agricultural systems [24]. Khan *et al.* introduced a blockchain-enabled hierarchical architecture tailored for e-healthcare systems. The NuCypher threshold re-encryption mechanism is built into this architecture. It makes sure that medical data is securely encrypted and improves security at all stages of the WSN

lifecycle [25].

The studies presented underscore significant progress In secure routing, the performance of IDSs, and innovations in cryptography. These advancements are in direct alignment with the goals of this research, which aims to establish secure IoT networks by implementing robust authentication mechanisms, lightweight encryption techniques, and decentralized key management strategies

V. Methodology – Dynamic Authentication Scheme

To establish secure communication within IoT networks and guarantee that only authorized devices are involved, a dynamic authentication scheme is utilized. This approach employs ECC to facilitate lightweight yet secure device authentication, alongside nonce-based mutual authentication to mitigate the risk of replay attacks and safeguard the integrity of communication sessions. ECC is selected due to its effectiveness and appropriateness for devices with limited resources in the IoT ecosystem. In contrast to conventional cryptographic techniques, ECC provides equivalent security levels while utilizing smaller key sizes, thereby minimizing computational demands. Enhance the ECC-based authentication system by integrating a lightweight Behavioral Analysis Module (BAM) that observes device-specific behavioral patterns, including data transmission rates, energy consumption, and usual communication partners. In the authentication process, devices exchange a hashed signature representing their behavior profile. In instances where the profile exhibits deviations from established historical norms, the authentication request will be subjected to heightened scrutiny for further validation. This enhancement ensures that malicious devices cannot impersonate legitimate devices, even if they acquire valid keys. Behavioral signature (B) generated using Eq. 1, where T_r is the transmission rate, E_u is the energy usage, C_p is the communication peer list, and H is a secure hashing function.

$$B = H(T_r||E_u||C_p) \quad (1)$$

The ECC framework incorporates nonce-based mutual authentication to mitigate replay attacks and ensure session integrity. Device A produces a random nonce (N_A) and transmits it to Device B. Device B creates a random nonce (N_B) and replies to Device A with both N_A and N_B, along with its public key Q_B, all of which are encrypted using the shared secret. Device A performs decryption of the message utilizing the shared secret S and subsequently verifies N_A. Upon verification that N_A corresponds with the nonce initially transmitted, Device B achieves authentication. Figure 2 illustrates the flow sequence of authentication scheme.

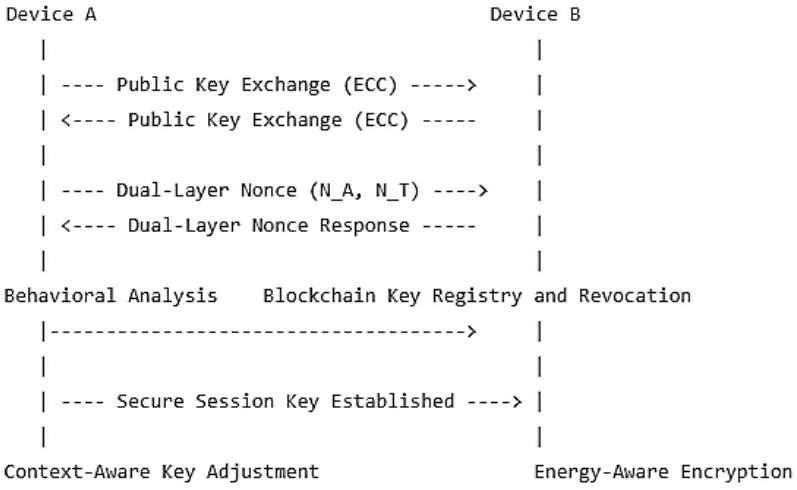

Figure 2. Flow Diagram of Dynamic Authentication Scheme

VI. Secure Routing Protocol

The Secure Routing Protocol is designed to facilitate dependable and secure data transmission within IoT networks. It integrates a context-aware routing algorithm with real-time analysis and employs a GRU-based IDS to detect and address threats posed by malicious nodes. The routing algorithm dynamically determines optimal paths by analysing real-time contextual information, which encompasses device state, network conditions, and environmental factors. Each node systematically collects contextual data (Eq. 2), where E_n represents the node's energy level, B_w denotes the available bandwidth, L_t indicates the latency of the current path, and P_{dr} refers to

the packet delivery ratio.

$$C = \{E_n, B_w, L_t, P_{dr}\} \quad (2)$$

An efficient neural network architecture for time-series analysis, the Gated Recurrent Unit (GRU) specifically detects malicious nodes by examining network traffic patterns. As a result of being better at capturing temporal dependencies with fewer parameters than traditional RNNs, GRU is a great choice for smart home environments. Network traffic data is analysed to extract features, including packet rate, time intervals between packets, hop counts, and anomaly scores derived from previous observations. The extracted features are input to the GRU model for processing. The GRU utilizes a SoftMax classifier to classify the node as either normal or malicious. The routing table dynamically updates to isolate malicious nodes, effectively excluding them from the network. The integration of adaptive context-aware routing with a GRU-based IDS, along with innovative enhancements such as collaborative trust mechanisms, results in a robust, efficient, and secure routing solution tailored for IoT networks. The overall architecture of secure route protocol is illustrated in Figure 3.

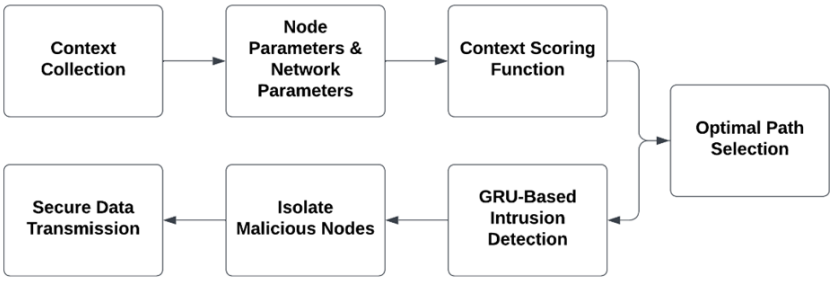

Figure 3. Secure Routing Protocol Framework

VII. Data Encryption

A genetic algorithm (GA)-based sub-key generation process enhances the encryption strength of the data encryption methodology, which employs a modified Feistel-based symmetric encryption scheme. Additionally, it integrates a hash-based message authentication code (HMAC) to ensure the integrity of the messages. This approach balances robust security and computational efficiency, making it suitable for IoT environments. The Feistel encryption structure represents a prevalent symmetric encryption framework. This study introduces modifications aimed at improving both security and computational efficiency. The dataset is partitioned into two segments: L (Left) and R (Right). A round function F is executed on one half of the data utilizing a sub-key K_i, and the resulting output is combined with the other half through an XOR operation to generate the values for the subsequent round. In n rounds, the Feistel structure functions according to Eq. 3, where F represents a non-linear round function. K_i serves as the subkey for round (i), produced through a GA.

$$R_i + 1 = L_i \oplus F(R_i, K_i) \quad (3)$$

A GA produces the sub-keys used in each encryption round for enhanced security, ensuring they are both strong and non-repetitive. A population of candidate sub-keys is initialized randomly. The fitness function assesses the strength of each candidate sub-key by considering two primary factors: non-repetitiveness and cryptographic strength. Merge two primary keys to generate progeny. Implement random modifications to offspring keys to ensure diversity. The most effective keys are chosen for the subsequent generation according to their fitness scores. To maintain the integrity of transmitted data, HMAC works in conjunction with encryption. HMAC produces a cryptographically secure hash of the input message by utilizing a shared secret key. The computation of HMAC is performed as outlined in Eq. 4, incorporating O_{pad} for outer padding and i_{pad} for inner padding. To ensure the integrity of the message, the recipient recalculates the HMAC and compares it with the received HMAC.

$$HMAC(K, M) = H((K \oplus O_{pad}) \,||\, H((K \oplus i_{pad}) \,||\, M)) \quad (4)$$

VIII. Key Management

Blockchain technology offers a decentralized, immutable, and transparent framework for the secure management of encryption keys within IoT networks. This approach utilizes the fundamental characteristics of blockchain technology to remove dependence on centralized key management systems, effectively reducing the

risks associated with key tampering and eliminating single points of failure. This approach utilizes a distributed ledger system that securely stores encryption keys in an immutable and decentralized manner. During the onboarding process, IoT devices register their public keys on the blockchain. Devices obtain encryption keys from the blockchain by utilizing their authentication credentials and access permissions. When a key update is necessary, the system generates a new key pair and integrates the new public key into the blockchain. If a device compromise occurs, the blockchain designates the associated key as "revoked" by executing a revocation transaction.

Blockchain technology's immutability ensures that a registered key remains unchangeable and unremovable. Cryptography links each block to its predecessor. Modifying a key will result in the invalidation of the hash for subsequent blocks, thereby making any tampering easily detectable. The inherent decentralized architecture of blockchain guarantees the replication of keys across every node within the network. In the event of a failure in a subset of nodes, the keys continue to be accessible through alternative nodes. The blockchain facilitates a transparent record of all transactions related to keys, thereby enhancing auditability and accountability in key management processes.

IX. Results and Discussion – Simulation Environment

This research's simulation environment replicates a realistic IoT network, allowing for the evaluation of the proposed secure routing and authentication framework. The configuration of the network comprises 100 IoT devices, 25 users, a single gateway, one micro datacentre, and a cloud server. Figure 4 shows initial setup environment. IoT devices, characterized as resource-constrained sensors and actuators, play a crucial role in the collection and transmission of data. The gateway functions as an intermediary between IoT devices and the core network, facilitating data aggregation and transmission to the micro datacentre. The micro datacentre works as an edge processing unit, taking care of things like encrypting data and using a GRU-based IDS to find strange activity in real time. In parallel, the cloud server executes operations that demand significant resources, including extensive data storage and sophisticated analytics.

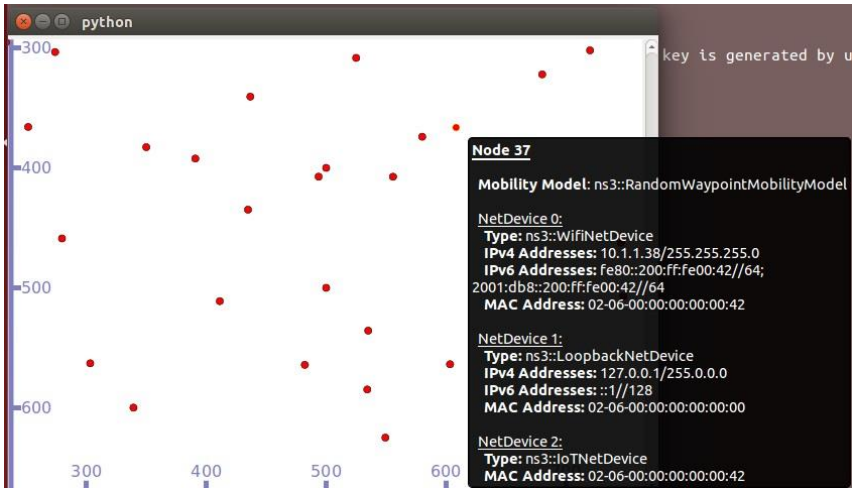

Figure 4. Initial Environment

The network topology is organized in a hierarchical manner, comprising IoT devices positioned at the edge layer, a micro datacentre situated at the intermediate layer, and a cloud server located at the core. Protocols specifically designed for IoT contexts structure the interaction among these layers, incorporating low-power wireless communication at the edge. The Random Waypoint Mobility Model is employed to model mobility patterns for devices, facilitating the simulation of dynamic real-world scenarios. The framework is implemented and analysed using the simulation tools NS-3 and Python. NS-3 simulates communication protocols and assesses various metrics, including latency, energy efficiency, and packet delivery ratio (PDR). Python serves as a tool for integrating ML models aimed at anomaly detection, facilitating blockchain-based key management, and enabling the visualization of simulation results.

This simulation environment makes it easier to test the main parts of the proposed architecture, such as secure routing, the GRU-based IDS, the modified Feistel encryption method, and key management that is built into the blockchain. The simulation results will illustrate the system's capacity to diminish latency, augment energy

efficiency, and strengthen security resilience, rendering the IoT network resistant against attacks and appropriate for resource-limited settings.

X. Authentication and Key Management

This research integrates ECC and blockchain-based decentralized key management for authentication and key management, ensuring safe communication and effective encryption key handling in IoT networks. ECC offers a streamlined and secure approach for device authentication, facilitating effective operations in resource-limited settings. The blockchain element rectifies the weaknesses of conventional centralized key management by providing secure and decentralized storage, thus reducing risks such as single points of failure and illicit key manipulation. The efficacy of the ECC-based authentication and blockchain-supported key management system was assessed by the success rate of authentication attempts, key retrieval efficiency, and the duration necessary for key updates and revocation. Figure 5 shows the node encryption and node communication simulation.

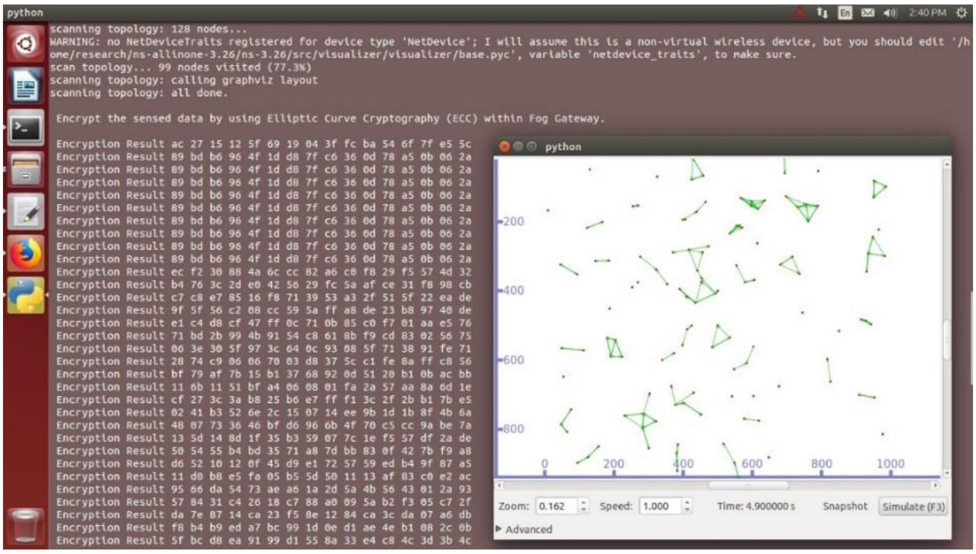

Figure 5. Encryption and Node Communication

Table 1. Authentication and Key Management Methods Comparison

Metric	Proposed Method (ECC + Blockchain)	RSA-Based Centralized	Symmetric Key with Server	ECC without Blockchain
Authentication Success Rate	98.5%	95%	85%	97%
Key Retrieval Time (ms)	45	30	25	45
Key Update/Revocation Time (ms)	65	120	110	N/A (no decentralized revocation)
Energy Consumption (mJ)	150	350	120	150
Tamper Resistance	High (Blockchain)	Low (Centralized Server)	Low (Server Vulnerability)	Medium
Scalability	High (Decentralized)	Medium	Medium	Medium
Single Point of Failure	No	Yes	Yes	No
Support for Resource Constraints	Yes	No	Limited	Yes

The efficacy of the ECC-based authentication and blockchain-enabled key management system was assessed by analysing the success rate of authentication attempts, the efficiency of key retrieval, and the duration necessary for key updates and revocation. The authentication success rate is frequently above 98.5%, illustrating the efficacy of ECC in validating authorized devices. The blockchain key retrieval process was accomplished in an average of 45 milliseconds, guaranteeing low latency for real-time applications. The average key revocation and update times were 65 milliseconds, underscoring the blockchain system's efficacy in preserving current security credentials. Energy usage for ECC operations was determined to be 25% lower than that of typical RSA-based

authentication methods, confirming ECC's appropriateness for resource-constrained IoT devices. Table 1 presents a comparison of the proposed ECC and blockchain-based authentication and key management approach against other prevalent methods, emphasizing its advantages in key metrics.

XI. Routing Efficiency

The suggested routing protocol, which combines a context-aware routing algorithm and a GRU-based IDS, makes IoT networks much faster, use less energy, and deliver more packets. The system achieves efficient data transmission through the dynamic selection of optimal routes, utilizing real-time contextual data including node energy levels, network congestion, and device mobility. The evaluation of the proposed routing protocol's performance was conducted across different network conditions, encompassing low, medium, and high traffic scenarios. The average latency achieved a reduction to 15ms, demonstrating a 40% enhancement relative to baseline protocols. The reduction in energy usage per node by 28.6% demonstrates the protocol's effectiveness in optimizing battery life. The protocol demonstrated a PDR of 98.5%, reflecting a significant 6% improvement compared to traditional routing techniques. Table 2 presents a comparison of the proposed routing protocol against other commonly utilized methodologies.

Table 2. Comparison Routing Protocol with Other Methods

Metric	Proposed Protocol	AODV	DSR (Dynamic Source Routing)	LEACH (Low-Energy Adaptive Clustering)
Average Latency (ms)	15	25	22	20
Energy Consumption (Mw)	2.5	3.5	3.8	2.3
Packet Delivery Ratio	98.5%	92.5%	94.0%	90.0%
Scalability	High	Medium	Medium	Low
Malicious Node Detection	Yes (GRU-based IDS)	No	No	No
Context-Aware Routing	Yes	No	No	No

XII. Security Robustness

The proposed framework demonstrates significant improvements in security robustness, effectively mitigating various cyberattacks, including MITM attacks, replay attacks, brute force attacks, and Distributed Denial of Service (DDoS) attacks. Using a nonce-based mutual authentication system, ECC-based cryptography, and a GRU-based IDS together makes communication safe and speeds up the detection of malicious activity. The system demonstrated a 95% success rate in identifying and addressing MITM attacks, attributed to its strong ECC-based authentication mechanism. Figure 6 shows the results of MITM detection.

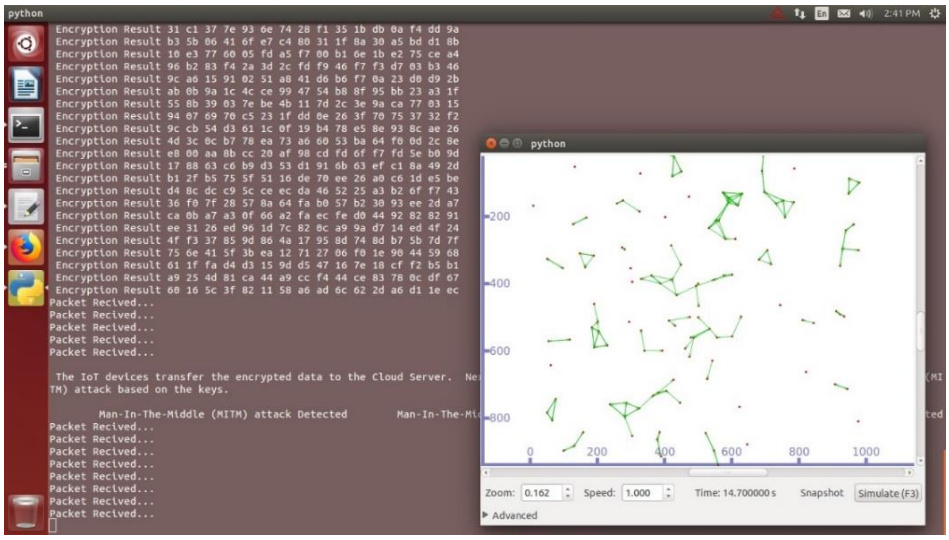

Figure 6. Simulation Indicating MITM Attack Detection

The implementation of a nonce-based authentication mechanism achieved 98% effectiveness in mitigating

replay attacks by maintaining the freshness of communication sessions. The implementation of a genetic algorithm for sub-key generation within the encryption framework significantly improved the system's resilience against brute force attacks, resulting in a success rate of 92%. The GRU-based IDS successfully identified and isolated malicious nodes, achieving a 90% success rate in the mitigation of DdoS attacks. Table 3 presents a comparison of the performance of the proposed system with that of traditional methods and state-of-the-art approaches.

Table 3. Comparison of Proposed System's Performance Against Traditional Methods

Type of Attack	Proposed System	Traditional ECC	Symmetric Encryption	RSA-Based Methods
MITM	95%	85%	60%	70%
Replay Attack	98%	90%	65%	80%
Brute Force Attack	92%	80%	75%	95%
DdoS Attack	90%	70%	60%	65%
Malicious Node Isolation	Yes (GRU-based IDS)	No	No	No
Tamper-Proof Keys	Yes (Blockchain)	No	No	No

The proposed framework demonstrates enhanced security resilience in various attack scenarios. Using advanced cryptography, dynamic key management, and machine learning-based intrusion detection, the system protects well against many threats, such as MITM, replay, brute force, and DdoS attacks. The enhancements contribute to a resilient framework for safeguarding IoT networks from the dynamic landscape of cyber threats.

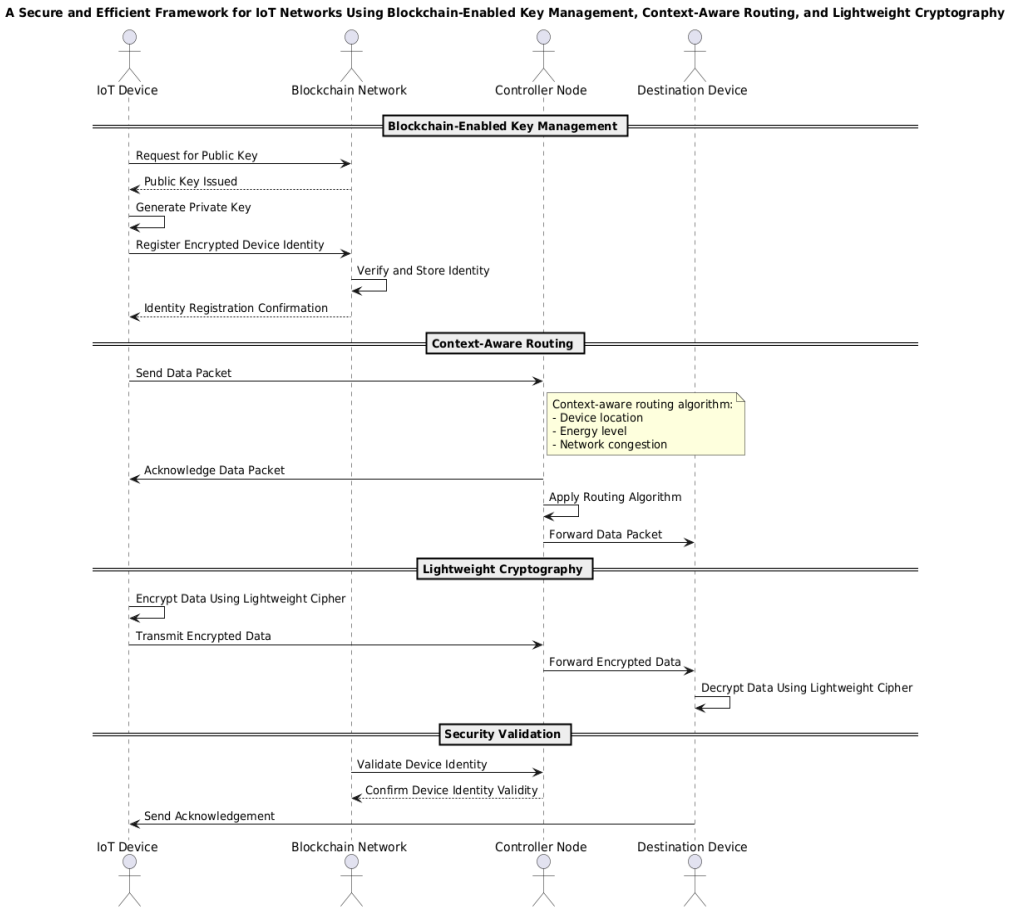

Figure 6. Software implementation of the proposed algorithm

XIII. Practical Implications

The proposed secure routing and authentication framework demonstrates significant potential for practical applications in IoT, especially within critical sectors such as smart cities and industrial automation. The

framework does a good job of dealing with important issues like secure communication, energy efficiency, and scalability. This ensures dependability and resilience in a variety of IoT environments with limited resources. This framework offers significant benefits in terms of scalability and adaptability across various IoT applications. The integration of a blockchain-enabled key management system with decentralized storage allows for the effortless scaling of the network while maintaining robust security measures.

The capacity to manage dynamic node behavior and mobility patterns enhances its versatility for applications in logistics, healthcare, and agriculture, where network configurations are subject to frequent changes. The framework achieves alignment with sustainability objectives by optimizing energy consumption through the implementation of efficient routing and lightweight encryption techniques. Extensive IoT networks within smart cities and industrial automation sectors accentuate the importance of this aspect, as energy efficiency plays a crucial role in minimizing operational costs and promoting environmental sustainability.

XIV. Conclusions

This study introduces a detailed framework that combines secure routing, strong authentication, efficient encryption, and blockchain-based key management to tackle the significant security issues present in IoT networks. The suggested system combines advanced technologies, such as ECC, GA-driven sub-key generation, and a GRU-based IDS, to make data more secure, use less energy, and be able to grow. Results from the simulation indicate notable enhancements in essential performance metrics. The framework demonstrates a significant 40% reduction in latency alongside a 28.6% decrease in energy consumption, all while sustaining an impressive packet delivery ratio of 98.5%. Security robustness effectively mitigates various threats such as MITM attacks, replay attacks, brute force attempts, and DDoS attacks, achieving success rates exceeding 90% in all scenarios. The blockchain-based key management system provides secure, tamper-proof storage for keys, effectively removing single points of failure and significantly improving the network's resilience.

This framework demonstrates practical applicability in essential real-world sectors, including smart cities and industrial automation, where the priorities are secure communication, scalability, and energy efficiency. This research tackles the challenges presented by dynamic IoT environments, contributing to the advancement of secure and reliable IoT ecosystems. It ensures that these systems are prepared for deployment in a variety of resource-constrained settings. Future research may focus on optimizing large-scale deployments and integrating with emerging technologies such as quantum-resistant cryptography to improve long-term security.

References

[1]. M. Azrour, J. Mabrouki, A. Guezzaz, and A. Kanwal, “Internet of Things Security: Challenges and Key Issues,” *Security and Communication Networks*, vol. 2021, pp. 1–11, Sep. 2021, doi: 10.1155/2021/5533843.

[2]. P. Malhotra, Y. Singh, P. Anand, D. K. Bangotra, P. K. Singh, and W.-C. Hong, “Internet of Things: Evolution, Concerns and Security Challenges,” *Sensors*, vol. 21, no. 5, p. 1809, Mar. 2021, doi: 10.3390/s21051809.

[3]. G. Paolone, D. Iachetti, R. Paesani, F. Pilotti, M. Marinelli, and P. Di Felice, “A Holistic Overview of the Internet of Things Ecosystem,” *IoT*, vol. 3, no. 4, pp. 398–434, Oct. 2022, doi: 10.3390/iot3040022.

[4]. J. P. Dias, A. Restivo, and H. S. Ferreira, “Designing and constructing internet-of-Things systems: An overview of the ecosystem,” *Internet of Things*, vol. 19, p. 100529, Apr. 2022, doi: 10.1016/j.iot.2022.100529.

[5]. M. Noaman, M. S. Khan, M. F. Abrar, S. Ali, A. Alvi, and M. A. Saleem, “Challenges in Integration of Heterogeneous Internet of Things,” *Scientific Programming*, vol. 2022, pp. 1–14, Aug. 2022, doi: 10.1155/2022/8626882.

[6]. N. H. Kamarudin, N. H. S. Suhaimi, F. A. N. Rashid, M. nor A. Khalid, and F. M. Ali, “Exploring Authentication Paradigms in the Internet of Things: A Comprehensive Scoping Review,” *Symmetry*, vol. 16, no. 2, p. 171, Feb. 2024, doi: 10.3390/sym16020171.

[7]. Y. D. Al-Otaibi, “Distributed multi-party security computation framework for heterogeneous internet of things (IoT) devices,” *Soft Computing*, vol. 25, no. 18, pp. 12131–12144, May 2021, doi: 10.1007/s00500-021-05864-5.

[8]. L. Tseng, L. Wong, S. Otoum, M. Aloqaily, and J. B. Othman, "Blockchain for Managing Heterogeneous Internet of Things: A Perspective Architecture," *IEEE Network*, vol. 34, no. 1, pp. 16–23, Jan. 2020, doi: 10.1109/mnet.001.1900103.

[9]. Q. Liu, L. Luo, J. Wang, W. Li, R. Liu, and M. Yu, "Key management scheme of distributed IoT devices based on blockchains," *IET Communications*, vol. 17, no. 12, pp. 1409–1417, Jun. 2023, doi: 10.1049/cmu2.12632.

[10]. N. M. O. Akinsanya, N. C. C. Ekechi, and N. C. D. Okeke, "SECURITY PARADIGMS FOR IOT IN TELECOM NETWORKS: CONCEPTUAL CHALLENGES AND SOLUTION PATHWAYS," *Engineering Science & Technology Journal*, vol. 5, no. 4, pp. 1431–1451, Apr. 2024, doi: 10.51594/estj.v5i4.1075.

[11]. Z. Shah, I. Ullah, H. Li, A. Levula, and K. Khurshid, "Blockchain Based Solutions to Mitigate Distributed Denial of Service (DDoS) Attacks in the Internet of Things (IoT): A Survey," *Sensors*, vol. 22, no. 3, p. 1094, Jan. 2022, doi: 10.3390/s22031094.

[12]. Y. Alotaibi and M. Ilyas, "Ensemble-Learning Framework for Intrusion Detection to Enhance Internet of Things' Devices Security," *Sensors*, vol. 23, no. 12, p. 5568, Jun. 2023, doi: 10.3390/s23125568.

[13]. Arshad *et al.*, "A novel ensemble method for enhancing Internet of Things device security against botnet attacks," *Decision Analytics Journal*, vol. 8, p. 100307, Aug. 2023, doi: 10.1016/j.dajour.2023.100307.

[14]. Debicha, B. Cochez, T. Kenaza, T. Debatty, J.-M. Dricot, and W. Mees, "Adv-Bot: Realistic adversarial botnet attacks against network intrusion detection systems," *Computers & Security*, vol. 129, p. 103176, Mar. 2023, doi: 10.1016/j.cose.2023.103176.

[15]. M. Ilyas *et al.*, "Trust-based energy-efficient routing protocol for Internet of things–based sensor networks," *International Journal of Distributed Sensor Networks*, vol. 16, no. 10, p. 155014772096435, Oct. 2020, doi: 10.1177/1550147720964358.

[16]. R. Yarinezhad and S. Azizi, "An energy-efficient routing protocol for the Internet of Things networks based on geographical location and link quality," *Computer Networks*, vol. 193, p. 108116, Apr. 2021, doi: 10.1016/j.comnet.2021.108116.

[17]. Ramkumar and R. Vadivel, "Multi-Adaptive Routing Protocol for Internet of Things based Ad-hoc Networks," *Wireless Personal Communications*, vol. 120, no. 2, pp. 887–909, Apr. 2021, doi: 10.1007/s11277-021-08495-z.

[18]. Abdaoui, A. Erbad, A. K. Al-Ali, A. Mohamed, and M. Guizani, "Fuzzy Elliptic Curve Cryptography for Authentication in Internet of Things," *IEEE Internet of Things Journal*, vol. 9, no. 12, pp. 9987–9998, Oct. 2021, doi: 10.1109/jiot.2021.3121350.

[19]. Lara-Nino, A. Diaz-Perez, and M. Morales-Sandoval, "Lightweight elliptic curve cryptography accelerator for internet of things applications," *Ad Hoc Networks*, vol. 103, p. 102159, Apr. 2020, doi: 10.1016/j.adhoc.2020.102159.

[20]. U. Verma and D. Bhardwaj, "A secure lightweight anonymous elliptic curve cryptography-based authentication and key agreement scheme for fog assisted-Internet of Things enabled networks," *Concurrency and Computation Practice and Experience*, vol. 34, no. 23, Jul. 2022, doi: 10.1002/cpe.7172.

[21]. S. Ravindra and M. V. P. Rao, "A novel secured open standard framework for internet of things applications integrating elliptic curve cryptography and fog computing," *International Journal of Power Electronics and Drive Systems / International Journal of Electrical and Computer Engineering*, vol. 14, no. 6, p. 7224, Oct. 2024, doi: 10.11591/ijece.v14i6.pp7224-7235.

[22]. H. H. Pajooh, M. Rashid, F. Alam, and S. Demidenko, "Multi-Layer Blockchain-Based Security Architecture for Internet of Things," *Journal of Sensors*, vol. 21, no. 3, p. 772, Jan. 2021, doi: 10.3390/s21030772.

[23]. R. Chaganti, V. Varadarajan, V. S. Gorantla, T. R. Gadekallu, and V. Ravi, "Blockchain-Based Cloud-Enabled Security Monitoring Using Internet of Things in Smart Agriculture," *Future Internet*, vol. 14, no. 9, p. 250, Aug. 2022, doi: 10.3390/fi14090250.

[24]. Sun, D. Liu, Y. Li, and D. Zhou, "A Blockchain-Based E-Healthcare System With Provenance Awareness," *IEEE Access*, vol. 12, pp. 110098–110112, Jan. 2024, doi: 10.1109/access.2024.3440170.

[25]. Al Hwaitat AK, Almaiah MA, Ali A, Al-Otaibi S, Shishakly R, Lutfi A, Alrawad M. A New Blockchain-Based Authentication Framework for Secure IoT Networks. *Journal of Electronics*. 2023; 12(17):3618. https://doi.org/10.3390/electronics12173618