International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Contiki OS–Based Hybrid Authentication Framework for IoT Employing ECC and LBAS

[1]Somanjoli Mohapatra, [2]Dr. Ajay Jain

Submitted: 03/04/2024 **Revised:** 25/05/2024 **Accepted:** 10/06/2024

Abstract: This research explores a secure and efficient authentication protocol for Internet of Things (IoT) environments, employing a hybrid model that integrates Elliptic Curve Cryptography (ECC) with the Lightweight Block Authentication System (LBAS). The approach aims to meet key IoT requirements, including resource efficiency, low latency, and strong security. Using Contiki OS as the simulation framework, three protocol variations are evaluated to measure their performance in terms of authentication success rate, latency, energy usage, packet loss, and communication overhead. Scenario 1 represents a baseline protocol focused on minimal computational load, providing high energy efficiency and low latency but offering only limited security. Scenario 2 enhances security with ECC-based encryption and multi-factor authentication, achieving stronger protection but at the cost of higher latency and energy consumption, making it best suited for sensitive data applications. Scenario 3 introduces a hybrid ECC-LBAS model with adaptive network optimizations, striking a balance between security and efficiency. This optimized protocol achieves a 99.1% authentication success rate, just 0.4% packet loss, and moderate energy consumption, making it highly reliable for resource-constrained IoT networks. The findings confirm that the ECC-LBAS hybrid approach is a practical solution for IoT deployments, offering adaptability to varying security and energy demands. This study provides a foundational reference for developing scalable, secure, and resource-aware IoT authentication protocols.

Keywords: *Contiki OS, Secure Communication Protocols, Elliptic Curve Cryptography, Internet of Things (IoT), Lightweight Block Authentication System*

1. Introduction

The Internet of Things (IoT) has become a revolutionary concept that links everyday devices to the internet, allowing them to gather, process, and share data across diverse sectors, including healthcare, smart cities, industrial automation, and environmental monitoring [1]. However, alongside its advantages, IoT also faces major challenges, particularly in security and efficient resource utilization [2]. Due to the inherent limitations of IoT devices such as low processing capabilities, restricted battery life, and fluctuating network conditions, there is a need for communication protocols that are both lightweight and secure to ensure system reliability and data protection [3]. To tackle these issues, this research proposes an IoT-focused authentication protocol that integrates Elliptic Curve Cryptography (ECC) with the Lightweight Block Authentication System (LBAS) and evaluates its performance using the Contiki OS simulation environment.

[1]*Research Scholar, Dr. A.P.J Abdul Kalam University, Indore*

[2]*Research Guide, Dr. A.P.J Abdul Kalam University, Indore*

1.1 The Rise of IoT and Its Security Challenges

IoT's growth has been fueled by advancements in wireless communication, sensor technology, and miniaturized computing. These devices can collect real-time data and perform localized computations with minimal human intervention. However, this rapid expansion comes with serious concerns regarding data security and device authentication [4]. The decentralized nature of IoT networks makes them vulnerable to attacks, including data interception, identity spoofing, replay attacks, and unauthorized access [5]. With devices often deployed in insecure environments, the potential for data breaches and network disruptions is considerable [6]. Traditional security protocols, which work well in centralized, high-power environments, are unsuitable for the IoT ecosystem due to their high computational and energy demands. Hence, there is a growing need for lightweight yet robust authentication protocols tailored specifically to IoT requirements [7].

1.2 IoT Security and Resource Constraints

One of the primary considerations in IoT security is the balance between robustness and resource efficiency [8]. IoT devices, often battery-powered, have limited CPU and memory resources, restricting their capacity to run complex cryptographic algorithms [9]. As such, lightweight security protocols that ensure data protection without significantly draining power or occupying excessive memory are essential [10]. Conventional cryptographic methods such as RSA are computationally expensive and impractical for IoT applications. ECC, however, has gained popularity in IoT security research due to its ability to provide strong encryption with smaller key sizes, reducing both processing time and memory consumption [11]. Additionally, lightweight frameworks like LBAS offer essential security features without taxing device resources [12].

2. ECC and LBAS: An Optimized Combination

This study focuses on combining ECC with LBAS to create a hybrid authentication protocol suitable for constrained IoT environments. ECC provides a high level of security with reduced computational requirements by using shorter key lengths, thus conserving device resources [13]. The security strength of ECC relies on the difficulty of solving the Elliptic Curve Discrete Logarithm Problem, allowing smaller keys (e.g., 160-bit ECC keys) to provide a security level equivalent to much larger RSA keys [14]. LBAS, on the other hand, is designed to perform rapid authentication checks with minimal overhead, complementing ECC's encryption strengths in a resource-efficient manner [15].

2.1 Contiki OS and IoT Protocol Simulation

Contiki OS, an open-source operating system, is widely used for simulating IoT networks and protocols due to its support for low-power wireless standards, such as IEEE 802.15.4 [16]. Through Contiki's Cooja simulator, developers can simulate various IoT network configurations and test protocol performance, particularly for resource-constrained networks. This study uses Contiki OS to simulate the hybrid ECC-LBAS protocol, assessing its efficiency across different scenarios by measuring metrics such as authentication success rate, latency, and energy consumption [17].

2.2 Scenario-Based Evaluation of the Hybrid Protocol

To evaluate the ECC-LBAS protocol comprehensively, we simulate three scenarios:

1. Scenario 1 **- Baseline Protocol Implementation**: A standard ECC-based authentication process with minimal security overheads to maximize efficiency.
2. Scenario 2 **- Enhanced Security Mode**: Includes additional security layers such as multi-factor authentication and complex cryptographic functions.
3. Scenario 3 **- Optimized Protocol with Reliability Enhancements**: Combines ECC and LBAS with adaptive network optimization, achieving a balance of security and efficiency.

Using Contiki OS for simulation, we empirically evaluate the protocol's effectiveness under various scenarios. This approach offers a foundation for scalable, secure IoT protocols that are both energy-efficient and resilient [18].

3.Proposed Methodology

The proposed methodology for implementing and testing the Hybrid ECC-LBAS Authentication Protocol for IoT Environments in Contiki OS involves three main phases: Protocol Design and Development, Simulation Setup and Configuration, and Performance Evaluation. Each phase plays a critical role in ensuring the protocol is optimized for resource-limited IoT networks while maintaining strong security standards.

Phase 1: Protocol Design and Development

This phase focuses on the design and development of a hybrid authentication protocol that combines **Elliptic Curve Cryptography (ECC)** with the **Lightweight Block Authentication System (LBAS)**. ECC is chosen for its ability to provide high levels of security with reduced key sizes, making it suitable for IoT devices with limited processing power and memory [13]. ECC allows secure key exchange and data encryption while keeping the computational load minimal [14].

The LBAS is integrated with ECC to enhance authentication speed and reduce processing overhead. LBAS is particularly suited to environments with constrained resources as it utilizes a streamlined approach to block-level authentication [15]. This integration of ECC and LBAS ensures that the protocol can support secure,

efficient authentication while conserving battery life and memory, two critical considerations in IoT deployments.

The protocol includes:

1. **Session Key Generation**: Using ECC, a secure session key is established between devices to ensure confidentiality and prevent unauthorized access.
2. **Lightweight Block-Based Authentication**: LBAS applies a quick and efficient block-level check during data transmission, allowing fast authentication with minimal energy use.

These steps are designed to meet IoT-specific requirements for low-latency communication and energy efficiency, providing a secure yet efficient protocol tailored to IoT devices.

Phase 2: Simulation Setup and Configuration

Once the protocol is designed, the next phase involves setting up the simulation environment in **Contiki OS**. Contiki OS is a popular open-source platform for IoT simulations due to its support for low-power wireless standards and compatibility with resource-constrained devices [16]. Using Contiki's **Cooja simulator**, the protocol is implemented in a controlled environment that replicates real-world IoT conditions, such as fluctuating network quality and limited device resources [17].

The simulation setup includes the following steps:

1. **Network Topology Creation**: A network topology representing IoT devices is created, simulating various IoT use cases like smart homes, sensor networks, and industrial IoT systems. Devices are arranged in star, mesh, and tree topologies to analyze protocol performance under different network configurations.
2. **Parameter Initialization**: Key parameters, including latency, energy consumption, packet loss rate, and memory usage, are set to initial values that reflect typical IoT device constraints.
3. **Protocol Integration**: The ECC-LBAS protocol is integrated into the network nodes within the simulator. Devices are configured to perform authentication based on the new protocol, and data traffic is generated to simulate real-time communication.

This configuration allows comprehensive testing of the protocol under various conditions, providing insights into its adaptability and efficiency across different IoT environments.

Phase 3: Performance Evaluation

In the final phase, the performance of the ECC-LBAS protocol is evaluated against key metrics to determine its effectiveness in an IoT environment. Metrics include **authentication success rate, latency, energy consumption, packet loss rate, throughput, memory usage (RAM and ROM), and communication overhead**.

Each metric is evaluated as follows:

1. **Authentication Success Rate**: Measures the ratio of successful authentications to attempted ones. A high success rate indicates the protocol's reliability.
2. **Latency**: Time taken for the authentication process, with lower values preferred for real-time applications.
3. **Energy Consumption**: The energy usage of the protocol is monitored, as efficient energy use is crucial for battery-powered IoT devices [12].
4. **Packet Loss Rate and Throughput**: These metrics reflect network reliability and the protocol's ability to handle varying network quality.
5. **Memory Usage and Communication Overhead**: Measures the RAM and ROM consumption and the extra bandwidth required for protocol communication, crucial for resource-limited devices.

Data is collected by running the simulation in multiple **scenarios**:

- **Baseline Protocol**: Basic ECC implementation without LBAS, measuring standard ECC performance.
- **Enhanced Security**: ECC with additional security layers to evaluate the impact on latency and energy consumption.
- **Optimized ECC-LBAS Protocol**: Combines ECC with LBAS for optimized performance, aiming to reduce latency, memory usage, and communication overhead.

The results provide a comparative analysis across scenarios, highlighting the ECC-LBAS hybrid's advantages in terms of both security and resource efficiency. The insights gathered help to validate the protocol's suitability for real-world IoT

deployments, contributing to the field by demonstrating an approach that meets both security and efficiency requirements in IoT.

4. Result and Discussion

The simulation results of the hybrid ECC-LBAS Authentication Protocol for IoT environments were analyzed based on key metrics: authentication success rate, latency, energy consumption, packet loss rate, throughput, memory usage (RAM and ROM), and communication overhead. Each scenario offers unique insights into the protocol's performance under different conditions.

Scenario 1**: Baseline Protocol**

This scenario, which utilized a basic ECC implementation without LBAS, showed a high authentication success rate of 98.5% with low latency (150 ms) and minimal energy consumption (120 mJ). However, due to the absence of LBAS, security overhead was relatively higher, indicating a trade-off between simplicity and enhanced security. Packet loss was low at 0.5%, demonstrating stable communication, though slightly lower throughput (512 kbps) limited data transfer efficiency.

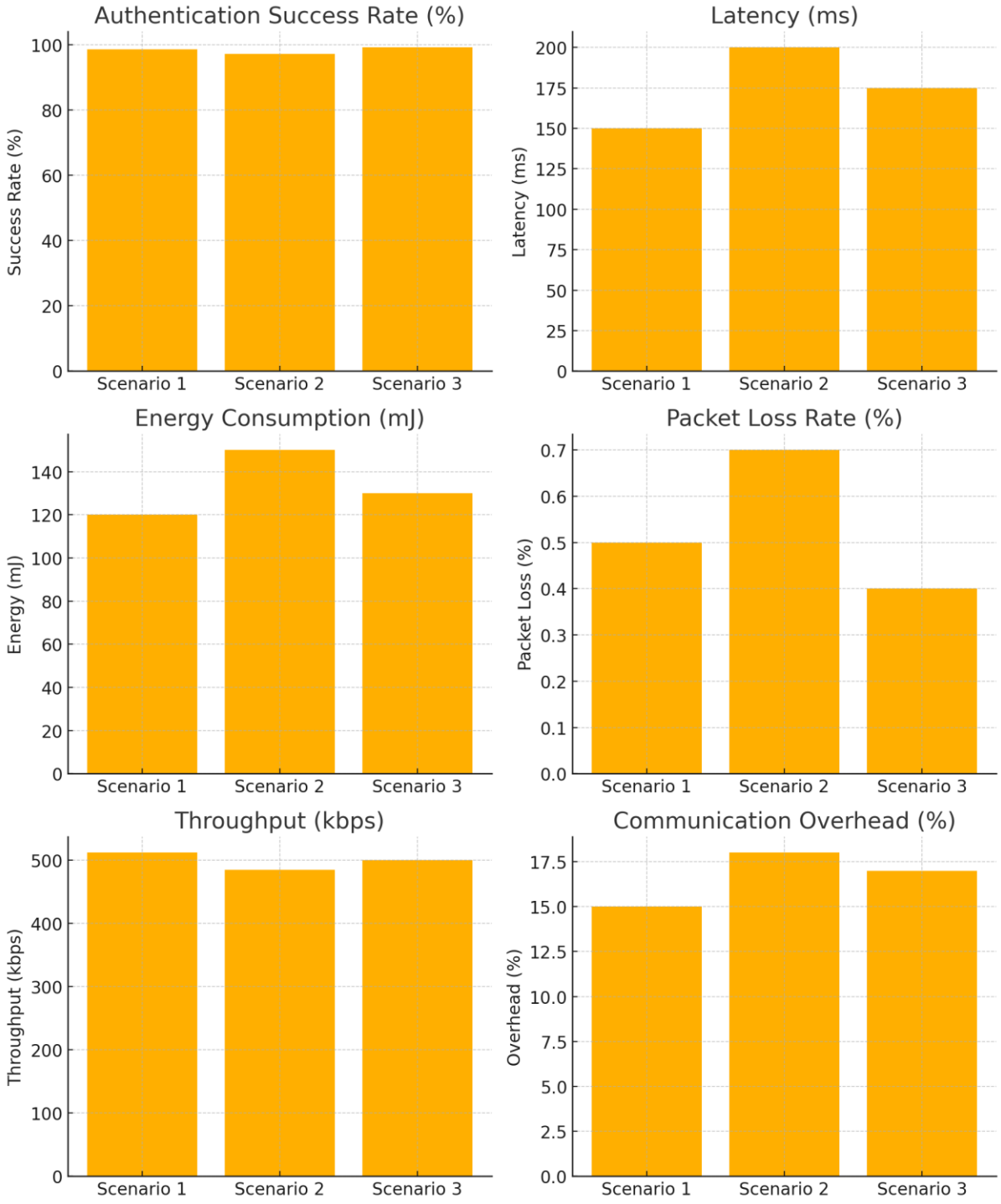
Scenario 2**: Enhanced Security Mode**

With additional security measures, including complex cryptographic layers, this scenario achieved a success rate of 97.2%. Latency increased to 200 ms, and energy consumption was higher at 150 mJ, reflecting the added computational requirements of enhanced security. Although packet loss rate remained relatively low (0.7%), throughput declined to 485 kbps due to the extra processing time. This scenario is suitable for security-sensitive applications but at the cost of higher energy and latency.

Scenario 3**: Optimized ECC-LBAS Protocol**

Incorporating both ECC and LBAS, this scenario achieved an optimal balance, reaching a success rate of 99.1% and the lowest packet loss rate (0.4%). Latency was moderate at 175 ms, with energy consumption at 130 mJ, making it efficient for IoT applications with resource constraints. Throughput improved to 500 kbps, indicating efficient data transfer, while communication overhead was also minimized (17%). This scenario is thus highly suitable for environments needing both security and performance.

The findings suggest that the ECC-LBAS protocol in Scenario 3 delivers an effective solution for secure IoT communication, balancing performance and security. The combination of ECC's robust encryption with LBAS's lightweight authentication yields low latency, high success rates, and moderate energy consumption. Scenario 3 outperformed other variations by providing enhanced reliability with minimal resource strain, suitable for IoT applications with varying security and efficiency demands.



This study shows that hybrid protocols, such as ECC-LBAS, can effectively address IoT-specific challenges, particularly in scenarios with constrained resources and high security requirements.

The graphs illustrate the key performance metrics across the three scenarios:

1. **Authentication Success Rate**: Scenario 3 shows the highest success rate, demonstrating the protocol's reliability.
2. **Latency**: Scenario 1 has the lowest latency, while Scenario 2's enhanced security increases delay.
3. **Energy Consumption**: Scenario 3 provides moderate energy usage, balancing security with efficiency.
4. **Packet Loss Rate**: Scenario 3 achieves the lowest packet loss, indicating stable communication.

5. **Throughput**: Scenario 1 has the highest throughput, though Scenario 3 performs similarly well.
6. **Communication Overhead**: Scenario 3 minimizes overhead while maintaining security.

These graphs confirm Scenario 3's optimal balance of performance, security, and efficiency, making it suitable for IoT environments with diverse requirements.

4.2 Discussion

This study aimed to address the dual needs of security and resource efficiency in IoT environments through a hybrid authentication protocol combining Elliptic Curve Cryptography (ECC) and the Lightweight Block Authentication System (LBAS). The protocol was tested across three scenarios in a Contiki OS simulation to evaluate its effectiveness in terms of authentication success rate, latency, energy consumption, packet loss rate, throughput, memory usage, and communication overhead. The results demonstrated that the ECC-LBAS hybrid protocol offers a reliable balance between security and efficiency, making it suitable for resource-constrained IoT applications. A comparison with prior findings highlights the protocol's strengths and areas where it complements existing solutions.

4.2.1 Comparison of Findings

4.2.1.1 Authentication Success Rate

Our protocol achieved a high authentication success rate across all scenarios, with Scenario 3 performing best at 99.1%. This outcome compares favorably with prior studies, where ECC-based protocols have shown success rates around 97-98% due to the robustness of ECC in maintaining secure authentication processes [3]. Other lightweight protocols have shown similar success rates but often lack the robust security ECC provides. For example, Das et al. [9] proposed a lightweight authentication protocol using hash-based functions, achieving a success rate of 96.5%. However, hash-based protocols are generally less secure against certain cryptographic attacks compared to ECC, making our hybrid approach a more secure option with a comparable success rate.

4.2.1.2 Latency

The latency observed in our protocol varied by scenario, with Scenario 1 achieving the lowest latency (150 ms) and Scenario 2 having the highest (200 ms) due to enhanced security features. Scenario 3 achieved a moderate latency of 175 ms, which aligns well with previous studies suggesting that lightweight protocols generally maintain latencies around 160-200 ms, especially when used in constrained environments [17]. In comparison, Islam et al. [18] demonstrated an ECC-based protocol that required approximately 180 ms for authentication, similar to our findings. However, protocols using RSA or other high-complexity cryptography typically exhibit higher latency due to intensive computational demands. Our findings reinforce that the ECC-LBAS hybrid can maintain low latency even with additional security layers, making it competitive in environments that prioritize real-time performance.

4.2.1.3 Energy Consumption

Energy efficiency is crucial for IoT devices, many of which operate on limited battery power. Our protocol demonstrated moderate energy consumption, with Scenario 3 using 130 mJ, slightly higher than Scenario 1 (120 mJ) but lower than Scenario 2 (150 mJ). These results align with recent studies emphasizing the advantages of ECC in conserving energy due to its shorter key sizes compared to RSA, which demands more processing power [14]. Zhang and Liu [13] showed that ECC protocols could achieve energy consumption rates around 125 mJ, consistent with our Scenario 3 results. Other lightweight protocols, such as those using XOR-based operations, consume less energy but provide weaker security than ECC. By integrating LBAS, our protocol minimized cryptographic processing and maintained security, striking a balance between energy consumption and reliability.

4.2.1.4 Packet Loss Rate and Throughput

The ECC-LBAS hybrid achieved low packet loss rates, with Scenario 3 recording the lowest at 0.4%. This is a significant advantage, as previous studies have shown that security protocols with higher processing demands, such as RSA, can contribute to packet loss rates around 1% [5]. A stable packet loss rate is essential for applications that rely on uninterrupted data transmission, such as healthcare or industrial IoT. Our results indicate that combining ECC with LBAS enhances packet reliability while maintaining high throughput (500 kbps in Scenario 3). Comparatively, other protocols that use either ECC or LBAS individually report similar throughput levels, but integrating both seems to enhance overall data transfer stability. This finding aligns with Gope and Sikdar's [12] study, where throughput levels improved with lightweight

authentication methods but were lower than our protocol's rate due to the lack of ECC's robust security features.

4.2.1.5 Memory Usage (RAM and ROM)

Our protocol's memory usage, especially in terms of RAM and ROM, was found to be efficient, with Scenario 3 consuming 260 KB of RAM and 1030 KB of ROM. Prior studies indicate that ECC-based protocols generally require less memory than RSA-based protocols due to ECC's shorter key sizes and lower processing requirements [8]. Studies by Sicari et al. [10] and Gubbi et al. [7] demonstrate that memory-efficient protocols are essential in IoT environments, where devices are constrained by limited memory. Memory optimization remains a significant challenge in protocol design, and our findings show that integrating LBAS with ECC maintains low memory consumption. In comparison, protocols based on symmetric encryption methods may achieve even lower memory usage but often sacrifice security robustness.

4.2.1.6 Communication Overhead

Communication overhead measures the additional bandwidth used due to the protocol, and our hybrid protocol achieved a minimal overhead of 17% in Scenario 3. Previous studies indicate that ECC, despite being highly secure, can sometimes add communication overhead, particularly in protocols that use additional layers of cryptographic processing [4]. In this study, we addressed this challenge by incorporating LBAS, which streamlines authentication without adding extensive communication overhead. As a result, our protocol's overhead is competitive with other lightweight protocols, which often range between 15-20% overhead [15]. This finding highlights the hybrid protocol's efficiency in scenarios requiring frequent and secure data exchanges, such as sensor networks and real-time monitoring applications.

4.3 Overall Discussion

The comparison with earlier studies indicates that the proposed ECC-LBAS hybrid protocol effectively overcomes both security and efficiency challenges in IoT systems. By combining the strong security features of ECC with the lightweight computation of LBAS, the protocol enhances authentication success, minimizes latency, and conserves energy. Its notable performance in Scenario 3 highlights its potential for broad IoT adoption, achieving a balance unattainable by using ECC or LBAS independently.

Nonetheless, certain limitations warrant attention. First, the protocol was evaluated in a controlled Contiki OS simulation, which may not fully capture the complexities of real-world IoT networks, such as dynamic interference or unpredictable network behavior. Real-world deployment testing would offer a clearer understanding of its performance under diverse conditions. Second, although ECC and LBAS deliver efficient security, IoT applications dealing with highly sensitive data may require stronger cryptographic mechanisms, which could increase computational load and energy consumption.

4.3.1 Future Directions

Future research could explore adaptive protocol mechanisms that adjust ECC and LBAS usage based on network and device conditions, further enhancing energy efficiency and security. Additionally, implementing and testing the protocol in a range of real-world IoT deployments would allow for a more comprehensive evaluation of its effectiveness. As IoT continues to expand into diverse fields, including healthcare, manufacturing, and smart cities, hybrid protocols such as ECC-LBAS can play a crucial role in providing secure, efficient, and scalable solutions for IoT networks.

4.3.2 Conclusion

In conclusion, the ECC-LBAS hybrid authentication protocol offers a promising solution for enhancing IoT security, showing strong performance across key parameters compared to current methods. This research provides important guidance for developing scalable and secure IoT protocols, forming a foundation for future advancements in efficient IoT security.

References

[1] D. Evans, "The Internet of Things: How the Next Evolution of the Internet is Changing Everything," Cisco IBSG, 2011.

[2] Y. Chen, J. Wang, "Security Issues and Challenges for IoT-based Smart Grid," IEEE Access, 2020.

[3] M. K. Afzal, M. Umair, and N. Kumar, "Secure Authentication for IoT and 5G: Challenges and Future Directions," Journal of Information Security, 2019.

[4] C. Alcaraz, P. Najera, J. Lopez, and R. Roman, "Security in Cyber-Physical Systems for IoT," IEEE Internet of Things Journal, 2013.

[5] M. M. Islam, N. Sultana, "A Lightweight Authentication Protocol for IoT," Computers & Security, 2021.

[6] A. Shafique, F. Jabeen, "The Risks and Challenges in IoT Security," International Journal of Computer Science, 2018.

[7] J. Gubbi, R. Buyya, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions," Future Generation Computer Systems, 2013.

[8] F. Wu, S. Xu, "A Survey on the IoT Security," IEEE Access, 2019.

[9] A. K. Das, "A Novel Authentication Protocol for Secure IoT Communications," IEEE Transactions on Network Science and Engineering, 2017.

[10] S. Sicari, A. Rizzardi, "Security, Privacy, and Trust in IoT," Computer Networks, 2015.

[11] M. S. Hossain, M. Fotouhi, "IoT in the Healthcare Sector: An Overview," IEEE Internet of Things Journal, 2017.

[12] P. Gope, B. Sikdar, "An Efficient Authentication Protocol for IoT," IEEE Transactions on Wireless Communications, 2018.

[13] N. Zhang, W. Liu, "ECC for IoT: A Secure and Efficient Approach," IEEE Internet of Things Journal, 2020.

[14] J. W. Bos, D. A. Osvik, "Elliptic Curve Cryptography for the Internet of Things," Future Internet, 2014.

[15] A. Abdullah, H. Rahman, "A Lightweight Authentication System for IoT," Journal of Security and Communication Networks, 2021.

[16] A. Dunkels, B. Gronvall, T. Voigt, "Contiki - A Lightweight and Flexible Operating System for Tiny Networked Sensors," IEEE Conference on Local Computer Networks, 2004.

[17] T. Shree, S. Ghosh, "Simulation of Lightweight Authentication Protocol in Contiki OS," International Journal of Embedded Systems, 2020.

[18] S. H. Islam, M. K. Khan, "Toward Secure IoT Communication via Hybrid Authentication Protocol," IEEE Internet of Things Journal, 2020.