Indian journal of
Engineering

To Cite:
Sriram S, Sridhar S, Usha S, Neeraja P, Sasikala R, Priya RL. Enhance the Internet of Things Light Weight Communication System Protocol Authentication. *Indian Journal of Engineering*, 2025, 22, e11ije1700
doi: https://doi.org/10.54905/disssi.v22i58.e11ije1700

Author Affiliation:
[1]Department of ECE, Amrita Vishwa Vidyapeetham, Chennai, India
[2]Associate Professor, Dept. of EEE, Ramaiah Institute of Technology, Bangalore, India
[3]Assistant Professor, SriSaiRam Institute of Management Studies, SriSairam Engineering college, Chennai, India
[4]Assistant professor, Department of Computer Applications, School of computing, Mohan Babuuniversity, Tirupati, India
[5]Professor & HoD, Department of MBA, Prathyusha Engineering College, Poonamallee -Tiruvallur High Road, Aranvoyal kuppam, Thiruvallur, Chennai, India
[6]Assistant professor, Department of Computer Engineering, Vivekanand Education Society's Institute of Technology, Chembur, Mumbai, India

Peer-Review History
Received: 07 May 2025
Reviewed & Revised: 16/May/2025 to 09/July/2025
Accepted: 21 July 2025
Published: 03 August 2025

Peer-Review Model
External peer-review was done through double-blind method.

Indian Journal of Engineering
pISSN 2319–7757; eISSN 2319–7765

DISCOVERY
SCIENTIFIC SOCIETY

Enhance the Internet of Things Light Weight Communication System Protocol Authentication

Sriram S[1], Sridhar S[2], Usha S[3], Peddinti Neeraja[4], Sasikala R[5], Priya RL[6]

ABSTRACT

Currently, Internet of Things (IoT) technology based on smart homes has been created and used extensively. Applications include remote or automated control of electrical appliances and electronics, where users can utilize smart devices to transmit commands to an IoT device or device gateway. Security and authentication procedures for Internet of Things devices have been the subject of innumerable research papers in recent years. The power limitations of IoT devices are still not taken into account, though. A security and authentication system that uses fewer hash functions and encryption techniques is presented in their study. The result is that it uses less power when communicating and so conforms with IoT and mobile device power limitations. The secure and compact communication protocol for the Internet of Things is still challenging to guarantee secure connections for Internet of Things (IoT) technologies. Deploying communication strategies based on asymmetric cryptographic systems might be challenging in IoT environments because of the strict resource restrictions of computing, memory, and communication. Using symmetric encryption techniques based on pre-shared keys is an alternative. The lightweight key synchronization update mechanism that is presented in the paper serves as a foundation for our suggested lightweight secure communication protocol. Analysis of the protocol's Security demonstrates that it is resilient to common attacks like replay and man-in-the-middle attacks. For formal verification, we next employ a commonly used Security protocol verification tool. Furthermore, consider the lightweight key synchronization update algorithm's computational efficiency and unpredictability and show that it performs better than alternative systems. To prove usefulness, they additionally consider the protocol's performance in terms of communication and computation expenses.

Keywords: Application, Communication, Security, IoT, Wireless, Privacy

1. INTRODUCTION

Creating a simple IoT authentication system for devices with limited resources, the security problems with Internet of Things devices, especially those that are

restricted, like sensors and embedded application systems, are another concern brought on by the expansion of IoT (Aggarwal et al., 2025). Light authentication procedures are necessary since the encryption schemes employed in these technologies are unsuitable due to their high resource requirements. Their study introduces a novel, low-power authentication mechanism that will work effectively with resource-constrained IoT devices (Bera et al., 2025). The specified protocol employs symmetric encryption for the actual data transfer procedure and ECC for key exchange to offer security (Dhakare et al., 2024). The suggested protocol's efficacy is evaluated using real sensor data samples taken from the Intel Berkeley Research Lab dataset, simulating an Internet of Things network with 100 nodes in total. Comparing the suggested system to other exciting approaches, the performance evaluation reveals improvements of 20% in energy consumption, 12% in global authentication time, and 31% in communication overheads and memory utilization (Fellah et al., 2025). The existing protocol works well in restricted IoT systems because it is efficient, resilient to common security risks, and effective. Future development will entail introducing new features that can be utilized to enhance a system's performance and security, as well as developing the content and making other enhancements.

2. EXPERIMENT

The improved Internet of Things cybersecurity approach uses a secure communication protocol based on a lightweight blockchain. Their study examines cybersecurity tactics for the Internet of Things (IoT) (Gala et al., 2025). It offers a novel remedy to overcome the shortcomings of current methods, namely the incapacity to safeguard the authenticity, integrity, and confidentiality of data in the event of an assault. Given its significant impact on securing IoT networks, the significance of improving cybersecurity tactics for IoT will be investigated. Automation, data collecting, and connection have all advanced significantly as a result of the Internet of Things' explosive growth (Ali and Rani, 2025). However, because IoT devices are frequently resource-constrained and vulnerable to innumerable cyber threats, their expansion has also brought forth significant security challenges. By putting out a lightweight blockchain-based secure Communication Protocol (LBSCP) to improve IoT Security, the study seeks to close the knowledge gap (Jung et al., 2022). LBSCP combines blockchain technology with lightweight encryption to produce a complete and reliable security solution designed for IoT networks (Khan and Megavarnam, 2024). LBSCP addresses the particular limitations of IoT devices by utilizing these technologies to minimize resource consumption on IoT devices while guaranteeing data secrecy, integrity, and authenticity. To consider the effectiveness of the LBSCP technique, simulations will be run as part of the research process (Kallapudi et al., 2025). By removing single points of failure and offering a tamper-proof transaction history, the simulation outcomes will empirically demonstrate how well the LBSCP approach improves the protocol's decentralized character, made possible by blockchain technology (Kavianpour et al., 2023). The results of their study show how effective LBSCPs are in protecting IoT networks and guaranteeing dependable and secure communication in various growing IoT contexts.

2.1. Proposed Methodology

Fig. 1 is the authentication of IoT devices in cloud services using a lightweight network. The two primary types of Internet of Things (IoT) devices are resource-rich (such as smart TVs, exercise equipment, and linked cars) and resource-constrained (like pacemakers, body sensors with poor battery lives, or bridge monitoring sensors). The second category of devices, which typically have demanding energy-consumption limitations (e.g., inability to be charged regularly) and/or low computational capacity, is the focus of their work (Komane et al., 2025). By utilizing the cellular network's trust and related standard authentication procedures, it offers three simple ways to give limited IoT devices robust authentication (Li and Ying, 2022). Two suggested solutions also add a core network broker that secures the communication of limited IoT devices that cannot create or use secure channels, utilizing secure communication between cellular devices and the core network.

2.2. Privacy And Security IoT

The role-based access control with privacy enhancement for IoT systems is one of the most significant security risks in IoT is unauthorised access to personal data (Yong et al., 2024). Research on safeguarding the privacy of roles is lacking, even though role-based access restriction can help to some extent. For cloud-based IoT systems with constrained resources, the paper suggests a unique privacy-enhanced role-based access control (PE-RBAC) strategy. By enabling the cloud platform (CP) to learn only the required roles of IoT devices rather than their complete role sets, our PE-RBAC system improves the privacy of conventional RBAC (Mishra et al., 2024).

By implementing the authorized private set intersection (APSI) protocol, IoT devices are kept in the dark about the functions of the cloud platform (Mahmood and Avcı, 2025). By combining an authentication method with an authorization center (AC), the scheme allows role authorization to stop unwanted requests. Regardless of IoT responsibilities, it uses a garbled Bloom filter (GBF) to achieve low computation and communication overhead. Because it simply needs random number generation and XOR operations, it is perfect for Internet of Things devices with constrained bandwidth and processing power (Mutiara et al., 2025). It accomplishes unlinkability and ciphertext. In designing the ability for IoT device privacy and unforgeability for both the cloud platform and IoT devices through formal security model definitions and thorough security analysis. Real-world-like studies that take into account different role sizes and the number of concurrent IoT devices show how practical it is. A throughput of 1,100 requests per second is demonstrated by the experimental results, and storage overhead is linear with the number of devices.

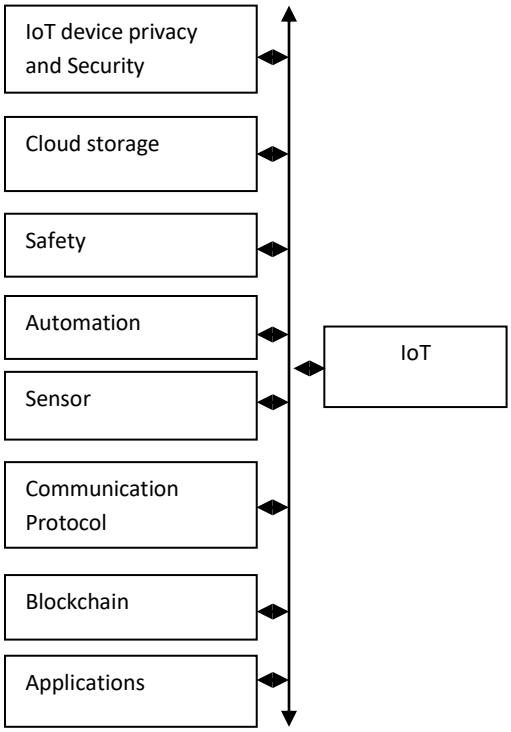

Figure 1 Block diagram

Cryptography

Cryptography is used by IoT devices to protect data and communication (Nandhini and Latha, 2024). Data is jumbled by encryption methods like AES, rendering it unintelligible to unauthorized individuals. Digital certificate authentication guarantees that only reliable devices can connect to networks. Hash functions check for tampering and ensure data integrity.

Protocols for IoT

Z-Wave and Zigbee are well-known low-power wireless protocols that are frequently utilized in industrial and home automation contexts (Naguib et al., 2025). Although the degree and implementation of their security measures can vary, they usually use their own. MQTT over TLS: Commonly used in the Internet of Things, MQTT is a lightweight messaging protocol that allows devices to communicate with a central broker. Although it adds overhead, TLS offers encryption for safe communication. The essential components of cryptographic systems are known as cryptographic primitives. SHA-1 and SHA-2 for hashing, AES and ChaCha20 for symmetric encryption, and HMAC for message authentication are typical examples. More intricate cryptographic protocols, such as TLS, which encrypts internet connections, and other security applications, are built using these primitives.

Denial of Service (DoS)

In addition to the main attack vector, other attack vectors such as forward/backward secrecy, denial of service (DoS), impersonation, and key leakage should be taken into account. These can have a big effect on security and call for particular defences. Key Leakage: An attacker obtains cryptographic keys without authorization; they can use them to decode private data or pretend to be authorized users. Countermeasures: Using forward secrecy, strong key management procedures, and secure key storage can all help reduce this danger.

CPU & Memory

The result is that 1,000 megabytes make up a gigabyte, which is anything with 1,000,000,000 bytes. Given that 10 GB is ten times that amount, it contains 10,000 megabytes (Pahlevi et al., 2024). One byte is sufficient for around one letter of text; therefore, one kilobyte is sufficient for 1,000 characters, or roughly a paragraph of text. Nevertheless, one kilobyte, which is sometimes shortened to KB, is still a relatively small amount of data storage. Due to their small size, KBs are typically not utilized to estimate the data storage of devices.

Lightweight protocol

It's important to make clear if you mean the intrinsic randomness (entropy) or the challenge of forecasting a particular value when you talk about the "unpredictability" of cryptographic keys or other data. Referencing particular entropy tests, such as those described in NIST SP 800-22, is advised to guarantee clarity. These tests assess a sequence's statistical characteristics to see if it is sufficiently random. ECC is frequently used in LoRa-based systems to offer security without appreciably affecting resource consumption because of its reduced key sizes. Secure communication between devices and the network infrastructure is ensured by ECC-based authentication mechanisms for LoRa. In dynamic wireless charging systems for electric automobiles, for instance, certain protocols employ ECC for mutual authentication between cars and charging stations.

Tiny ECC: This ECC implementation or library is designed especially for devices with limited resources. It seeks to minimize the amount of memory and processing power needed for implementation while still offering the security advantages of ECC. This makes it possible to include ECC-based security on gadgets with extremely constrained resources, as those in wireless sensor networks.

TinyOS and Contiki

The Contiki OS has a distinct abstraction layer between drivers and hardware; drivers and apps can communicate directly with hardware, unlike TinyOS. Python is supported; however, C is the primary programming language. Specific memory and storage spaces are allocated to core and loaded programs. The simple response is no. Instead of using an ARM-based microcontroller, the ESP32 makes use of a Tensilica processor with its unique ESP32 architecture. The 32-bit Tensilica Xtensa LX6 microprocessor is specifically used by ESP32. Numerous sensors can be connected to the ESP32 Sensor Network, a wireless sensor network board that is based on WiFi, BLE, and Bluetooth. This development board is readily enclosed and is modular (Raja et al., 2024). The jitter, latency packet loss may result from packets being deleted or received out of order due to high jitter. Network devices may occasionally buffer data to offset jitter, which can further raise latency.

3. RESULT AND DISCUSSION

The advanced communication protocols are a two-pronged strategy using DTLS and advanced COAP Every real-time object can be easily integrated with a traditional network thanks to the Internet of Things (IoT). Real-time heterogeneous objects are enhanced with the ability to communicate and evaluate standards and skills to exchange information with earlier networks. However, these objects are susceptible to various security protocols and have limited resources. To build a secure protocol for safe data transmission and communication in the Internet of Things environment, a lot of studies have already been done. The segmented transmission CoAP is suggested as a safe and secure communication protocol to safeguard users' private and sensitive information (Rishi et al., 2024). Two blocks are used to transmit the request and response in the suggested segmented transmission CoAP with DTLS. Innumerable blocks can be transferred by the client with a request, and the server can transfer innumerable blocks with a response without any prerequisites. Because of the massive payloads that exceed the network's bounds, the suggested segmented transmission of CoAP with DTLS reduces the chance of transmission failure by segmenting messages. The use of DTLS ensures data confidentiality and integrity by offering a robust security layer throughout the connection process. The suggested segmented transmission CoAP with DTLS

enhances the resource utilization for secure transmission of sensitive data and reinforces the security features of DTLS, even in networks that are not secure. The performance parameters of throughput, energy consumption, and latency time are used to consider the effectiveness of the suggested segmented transmission CoAP with the DTLS paradigm.

3.1. Internet of Things (IoT)

The function of blockchain technology in IoT security to safeguard the future of IoT networks of connected devices, known as the Internet of Things (IoT), has revolutionized innumerable industries, but as it has grown, it has also given rise to new problems like data privacy, scalability, and security (Silva et al., 2023). By facilitating safe and decentralized data and transaction management, blockchain technology—a decentralized digital ledger—has become a viable solution to these problems. In their study, we investigate the potential applications of blockchain technology for IoT network security (Sabonchi, 2025). They provide a summary of the fundamental concepts and features of blockchain technology, along with an analysis of its benefits and drawbacks concerning IoT networks. It also examines the literature on blockchain-based solutions for Internet of Things networks. The primary ramifications of incorporating blockchain technology into IoT networks and offer suggestions for additional research.

The micro versions of security protocols across wireless networks offer security solutions to IoT devices. The three phases of the security protocol for IoT environments proposed in the research paper are as follows: In the first phase, all IoT devices must register with the server to receive user login credentials; in the second phase, the server must authenticate the IoT devices that genuinely wish to access the server; and in the third phase, data are transferred through a secure IoT channel while maintaining integrity, security, and confidentiality (Sharma et al., 2024). Twenty rounds of subkeys are used to provide data security. Diffusion matrices can be used in security contexts to conceal the probabilistic relationship between transmitted data and ciphertext.

3.2. Applications

Leading the way in IoT healthcare privacy-first methods with safe wearable monitoring systems protecting the privacy of patient medical data gathered by wearable tracking devices is currently a pressing and significant area in the realm of IoT healthcare. It is crucial that the requirement be fulfilled (Shifani et al., 2024). During their inquiry, a secure Health Data Aggregation and Homomorphic Encryption (SHAHE) technique is being thought of as a potential substitute. As we developed the SHAHE strategy, we thought about the requirements for processing, data collecting, and access control (Uwaezuoke and Swart, 2025). By employing safe aggregation techniques and homomorphic cryptography, they completely accomplish their objective (Upadhyay et al., 2023). The program's primary objective is to safeguard individuals' privacy by improving data value analysis and minimizing illegal access to critical health data. The program was created for that reason.

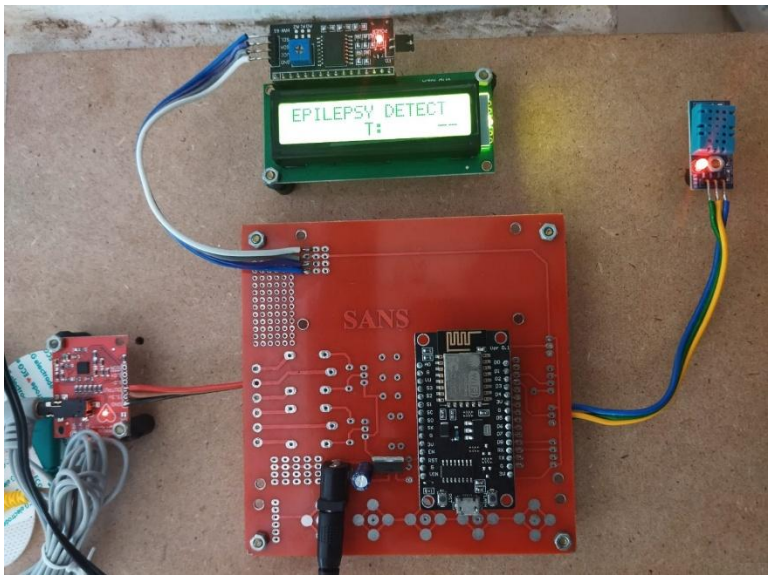

Figure 2 Output of Privacy and Security Software, Hardware IoT kit

The Fig. 2 design and research of an IoT-enabled smart collar for monitoring and detecting cattle theft to reduce cow theft in rural regions and enhance livestock monitoring, the article constructs and studies an IoT-enabled smart collar (Wang et al., 2024). The suggested system incorporates temperature sensors for theft detection, an accelerometer for motion detection, and GPS for real-time location monitoring. Cellular communication networks connect all of these parts (Yodthong and Munlin, 2023). The collar tracks the movement of the animals and sends out alarms when they exhibit odd behavior that could be a sign of theft or distress. Prototype testing showed good performance in terms of warning reaction times (less than 60 seconds) and GPS accuracy (± 3 meters). On cloudy days, however, power consumption testing showed a 5-hour operating limit. They demonstrated the necessity of better energy management. To increase performance in large-scale deployments, the article ends with suggestions for more research, such as system scalability and better power methods. The findings imply that the smart collar provides a workable way to detect theft and manage livestock remotely.

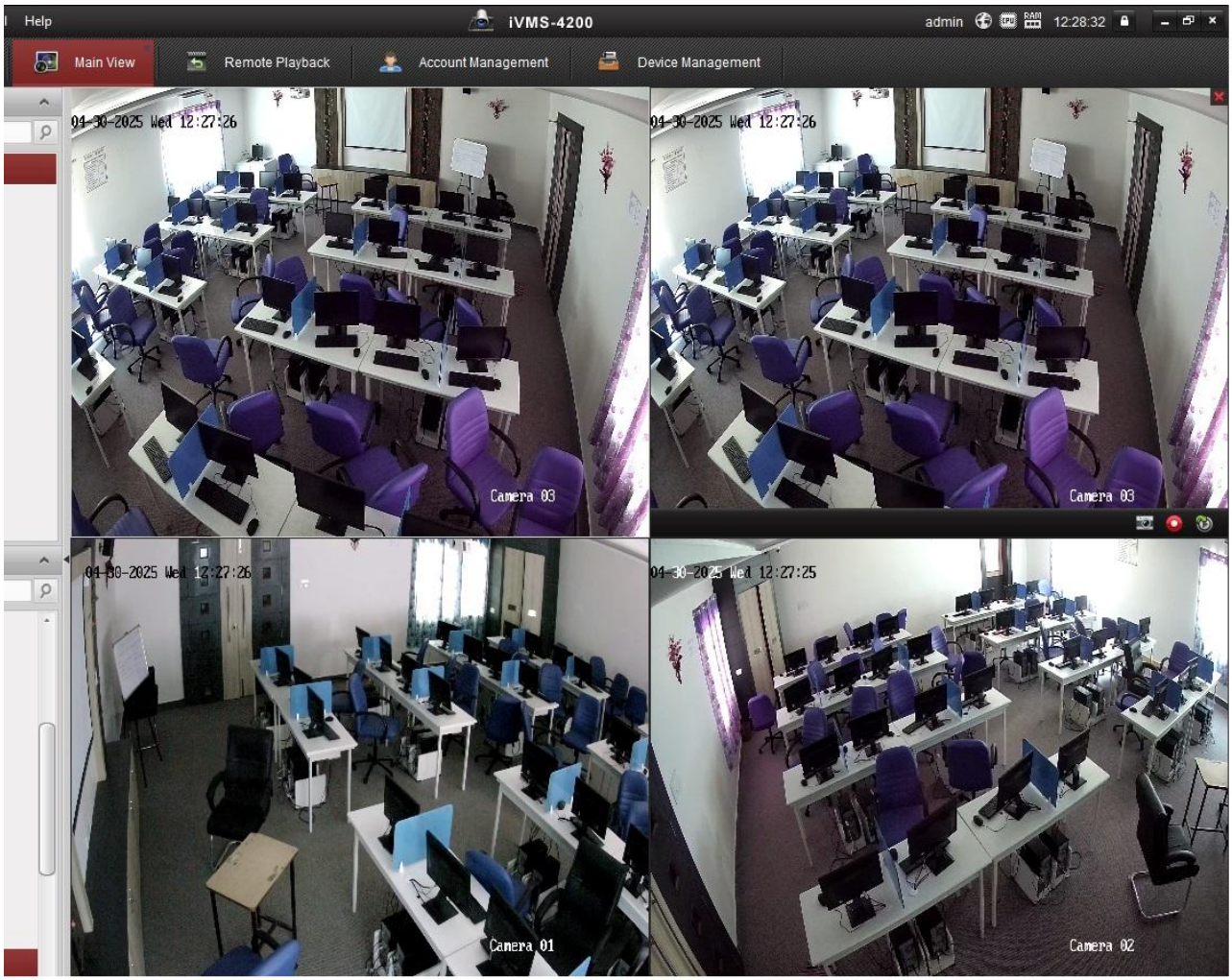

Figure 3 Output of Hardware Privacy and Security

3.3. Everyday Lives Electronics Gadgets

The Fig. 3. Security in Wearable Technology and Bluetooth wearable technology and Bluetooth technology have significantly altered our Everyday lives. These gadgets are incredibly convenient and facilitate communication in various domains, including daily activities, fitness, and healthcare. However, given their rapid growth, we also need to consider privacy and other crucial considerations. Many people use Bluetooth for wireless communication; however, there are a number of Security dangers. Threats include device spoofing, man-in-the-middle attacks, and eavesdropping. All of these flaws could result in illegal access, data breaches,

or even malfunctioning devices. Wearable technology and Bluetooth technology have significantly altered our everyday lives. These gadgets are incredibly convenient and facilitate communication in various domains, including daily activities, fitness, and healthcare. However, given their rapid growth, we also need to consider privacy and other crucial considerations. Many people use Bluetooth for wireless communication; however, there are a number of Security dangers. Threats include device spoofing, man-in-the-middle attacks, and eavesdropping. All of these flaws could result in illegal access, data breaches, or even malfunctioning devices. This demonstrates the need for robust Security measures to protect our data. Finding solutions to lower risks requires a thorough understanding of these Security areas. Their study aims to highlight the importance of establishing robust Security frameworks and best practices. By doing that, we can ensure that people feel comfortable in an increasingly connected environment and protect our private information.

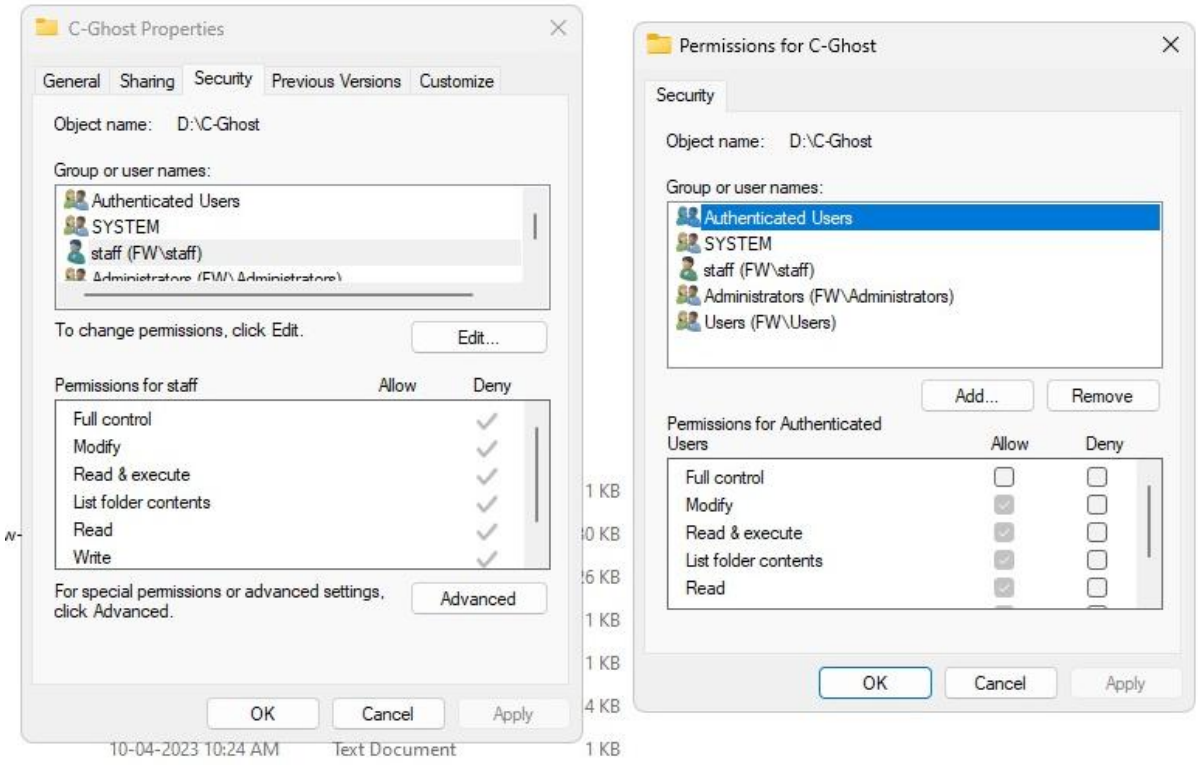

Figure 4 Output of Software Privacy and Security

The smart gadgets have revolutionized a number of industries, from home automation to healthcare, by providing previously unheard-of convenience and efficiency. Rapid expansion has led to the recovery of security holes that have enabled modern cyber threats. The intricate security threats facing the IoT ecosystem offer potential remedies.

The IoT and smart devices are discussed at the beginning of the chapter, stressing the value of security and defining its parameters. It examines the IoT environment, going into its categorization, growth, examples, and security aspects. The categorized and considered emerging threats included supply chain assaults, ransomware, malware, device hijacking, data breaches, DDoS attacks, insider threats, and physical security hazards. Vulnerabilities such as hardcoded credentials, poor authentication, insufficient encryption, insufficient access controls, and unsecured communication are identified in this chapter. The Fig. 4 presentations of countermeasures and best practices center on network segmentation, secure design, strong authentication, encryption, frequent upgrades, monitoring, and user education. In addition to covering security testing techniques, including penetration testing, vulnerability considerations, code analysis, and audits, it talks about security standards, laws, and compliance initiatives. Strategies for incident response and recovery are described, including communication, forensics, backup, planning, and detection. Lessons and mitigation techniques are demonstrated through case studies of notable security breaches. It ends with some observations about upcoming developments and challenges in IoT security.

4. CONCLUSION

The protocol for provably secure anonymous device authentication in an Internet of Things environment and identity identification between devices and cloud servers are severely hampered by the Internet of Things (IoT) intrinsically large heterogeneous device population and open channels. Reliable protocols serve as a vital means of providing security for authentication in matters and guarantee the legality of participants. According to earlier studies, researcher-developed methods include security flaws that make it challenging to defend against extensive network attacks, such as replay attacks, impersonation, and stolen device attacks. Furthermore, several protocols involve intricate interaction mechanisms that result in substantial resource loss and computational redundancy. Inspired by there, their paper suggests an elliptic curve cryptography-based anonymous and certificate-less lightweight authentication protocol (ACLAP) for device-to-device and device-to-server. It resolves authentication security issues and enhances the quality of communication between devices and cloud servers. Without keeping any reliable proofs on the cloud server, the technique uses the biometric features and passwords of device users as verification credentials. We tackle the problem of resource usage brought on by a large number of IoT devices. Our protocol offers better security performance and efficiently conserves communication resources for authentication, according to formal security analysis and compared with existing studies. The scheme's practical significance and practicality are demonstrated by the simulation results.

Acknowledgement

This work is supported by Research on Internet of Things Communication System Protocol and its Applications; We thank the participants who were all contributed

Author Contributions

Contribution of each authors regards manuscript work & production.

Ethical issues

Not applicable.

Informed consent

Not applicable.

Funding

This study has not received any external funding.

Conflict of Interest

The author declares that there are no conflicts of interest.

Data and materials availability

All data associated with this study are presented in the paper.

REFERENCES

1. Aggarwal D, Saxena AB, Sharma D. Cybersecurity Risks in IoT: A Layered Approach to Threat Detection and Prevention. International Conference on Sentiment Analysis and Deep Learning. 2025; 501-505. doi: 10.1109/ICSADL65848.2025.10933329.
2. Ali HAS, Rani V. Deep learning approach for protecting IoT smart home devices against multiclass botnet attacks. Int J Comput Netw Appl 2025;12(3):307–23. doi:10.22247/ijcna/2025/20
3. Bera B, Das AK, Sikdar B. Quantum-Resistant Secure Communication Protocol for Digital Twin-Enabled Context-Aware IoT-Based Healthcare Applications. IEEE Transactions on Network Science and Engineering. 2025. doi: 10.1109/TNSE.2025.3553044

4. Dhakare S, Chippalkatti SS, Misbahuddin M.Securing the IoT Device Network with Lightweight Cryptography. International Symposium on Wireless Personal Multimedia Communications. 2024; 1-5. doi:10.1109/WPMC63271.2024.10863558
5. Fellah KE, Azami IE, Makrani AE, Bouijij H, Azzouzy OE.Revolutionizing Automotive Security: Connected Vehicle Security Blockchain Solutions for Enhancing Physical Flow in the Automotive Supply Chain. Comput Syst Sci Eng 2025;49(1):99–122. doi:10.32604/csse.2024.057754
6. Gala DL, Molleda J, Usamentiaga R. Evaluating the Impact of Adversarial Patch Attacks on YOLO Models and the Implications for Edge AI Security. Int J Inf Secur 2025; 24:154. doi:10.1007/s10207-025-01067-3
7. Jung H, Koo H, Jeong JP. IoTivity Packet Parser for Encrypted Messages in Internet of Things. International Conference on Advanced Communication Technology (ICACT) 2022; 53-57. doi: 10.23919/ICACT53585.2022.9728913.
8. Kallapudi V, Praneel AV, Sindhu P, Amiripalli SS. Securing Digital Twins: Lightweight Protocol Vulnerabilities and Mitigation Strategies. International Conference on Intelligent Data Communication Technologies and Internet of Things. 2025; 427-434. doi: 10.1109/IDCIOT64235.2025.10914781.
9. Kavianpour S, Razaq A, Hales G. A secure lightweight authentication mechanism for IoT devices in generic domain. In 2023 3rd International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME) 2023; 1-6. doi: 10.1109/ICECCME57830.2023.10253392.
10. Khan I, Megavarnam M. Securing Web by Predicting Malicious URLs. J Cyber Secur 2024;6(1):117–130. doi:10.32604/jcs.2024.048332
11. Komane K, Khoza L, Radebe F. A Conceptual Framework for Cybersecurity Awareness. J Cyber Secur 2025;7(1):79–108. doi: 10.32604/jcs.2025.059712
12. Li W, Ying J. A lightweight identity authentication protocol in the internet of things environment. In: 2022 IEEE 12th International Conference on Electronics Information and Emergency Communication (ICEIEC). 2022; 42–7.
13. Mahmood A, Avcı İ. Evaluation and benchmarking of cybersecurity DDoS attacks detection models through the integration of FWZIC and MABAC methods. Comput Syst Sci Eng 2025;49(1):401–17. doi: 10.32604/csse.2025.062413
14. Mishra J, Sulthana GN. Advanced Communication Protocols: A Dual Approach with Advanced CoAP with DTLS. International Conference on Communication, Computing & Industry 6.0. 2024; 1-5. doi: 10.1109/C2I663243.2024.10895787.
15. Mutiara GA, Periyadi, Alfarisi MR, Rizal MF, Harsono RW, Tambunan MR, Muhijri I, Yulistia AR. Sensor fusion-based IoT framework for precision livestock monitoring and feed management. Int J Adv Technol Eng Explora 2025; 12(127):927-955. doi: 10.19101/IJATEE.2025.121220053
16. Naguib A, Aslan HK, Fouad KM. Effective Integration of Database Security Tools into SDLC Phases: A Structured Framework. J Cybersecurity Infor Managem 2025;176-207. doi: 10.54216/JCIM.160114
17. Nandhini T, Latha R. Designing a Lightweight IoT Authentication Protocol for Resource-Constrained Devices . International Conference on IoT, Communication and Automation Technology. 2024; 962-966. doi: 10.1109/ICICAT62666.2024.10923434.
18. Pahlevi RR, Hasegawa H, Yamaguchi Y, Shimada H. Complete Security Analysis on Event-Based Dynamic Protocol for Constrained IoT Device. International Conference on Information and Communication Technology (ICoICT) 2024; 224-235. doi: 10.1109/ICoICT61617.2024.10698059.
19. Raja A, Sahana MS, Prathibbhavani PM, Venugopal KR. Secure Communication using Mutual Authentication in Light IoT. In 2024 IEEE International Conference for Women in Innovation, Technology & Entrepreneurship (ICWITE) 2024; 471-476. doi: 10.1109/ICWITE59797.2024.10502725.
20. Rishi M, Dubey V, Bhardwaj MK, Singh MK. IoT Cryptography: A Secure Communication Framework for the Internet of Things. International Conference on Intelligent Systems for Cybersecurity. 2024; 1-6. doi: 10.1109/ISCS61804.2024.10581329.
21. Sabonchi AKS. Securing Electronic Health Records with Cryptography and Lion Optimization. J Cyber Secur 2025;7(1):21–43. doi: 10.32604/jcs.2025.059645
22. Sharma P, Nishanthi N, Pandey N, BN KR, Ashok BM, Prabagaran S. Efficient and Secure Data Handling in IoT Networks: Robust Lightweight Approach. International Conference on Innovations in High Speed Communication and Signal Processing. 2024; 1-6. doi: 10.1109/IHCSP63227.2024.10959883.
23. Shifani SA, Korde V, Vijay S, Shalout I, Indhumathi V, Revathi RB. Experimental Analysis of an IoT Based Secured Data Communication between Social Communities Over Wireless Sensor Network Environment. International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems. 2024; 1-7. doi: 10.1109/ICSES63760.2024.10910873.
24. Silva T, Casal J, Chaves R. Lightweight network-based IoT device authentication in Cloud services. International

Conference on Network Protocols. 2023; 1-6. doi: 10.1109/ICNP59255.2023.10355621.

25. Upadhyay A, Maity S, Venkatesan S. Lightweight Authentication Protocols for IoT Networks. International Conference. 2023;1-6. doi: 10.1109/PuneCon58714.2023.10450064.
26. Uwaezuoke E, Swart TG. A vulnerability assessment and exploitation analysis of a powerline communication Home Plug AV network adapter. Int J Inf Secur 2025;24:168. doi:10.1007/s10207-025-01081-5
27. Wang F, Song J. Cryptanalysis of Two Lightweight Authentication Protocols for IoT Environments. International Conference on Computer and Communications. 2024;405-409. doi: 10.1109/ICCC62609.2024.10941904.
28. Yodthong W, Munlin M. Lightweight Authentication and Communication Protocol for IoT Devices. International Conference on Electrical and Electronics Engineering. 2023;159-163. doi: 10.1109/ICEEE59925.2023.00037.
29. Yong L, Yuanyuan M, Mu C, Chao W. A Power IoT Terminal Asset Identification Technology Suitable for Modbus Protocol. In: International Conference on Interactive Intelligent Systems and Techniques. 2024; 224–8.