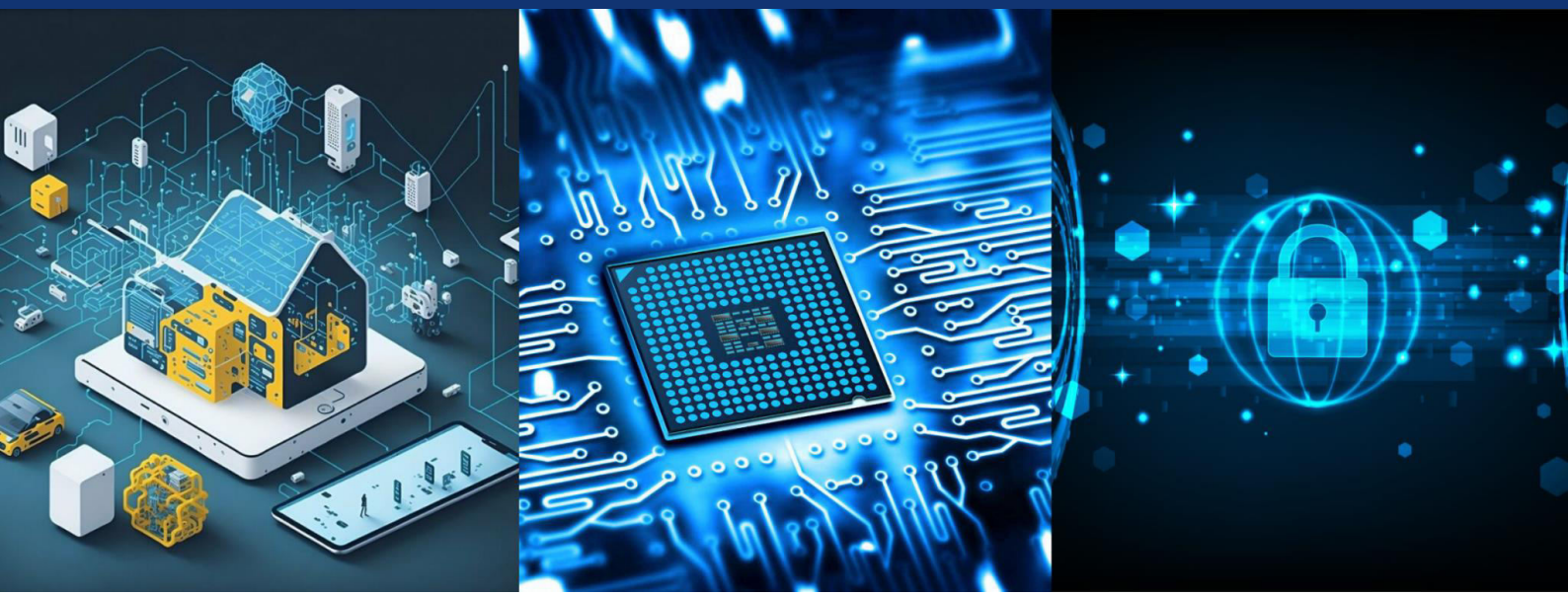
IJIRCCE

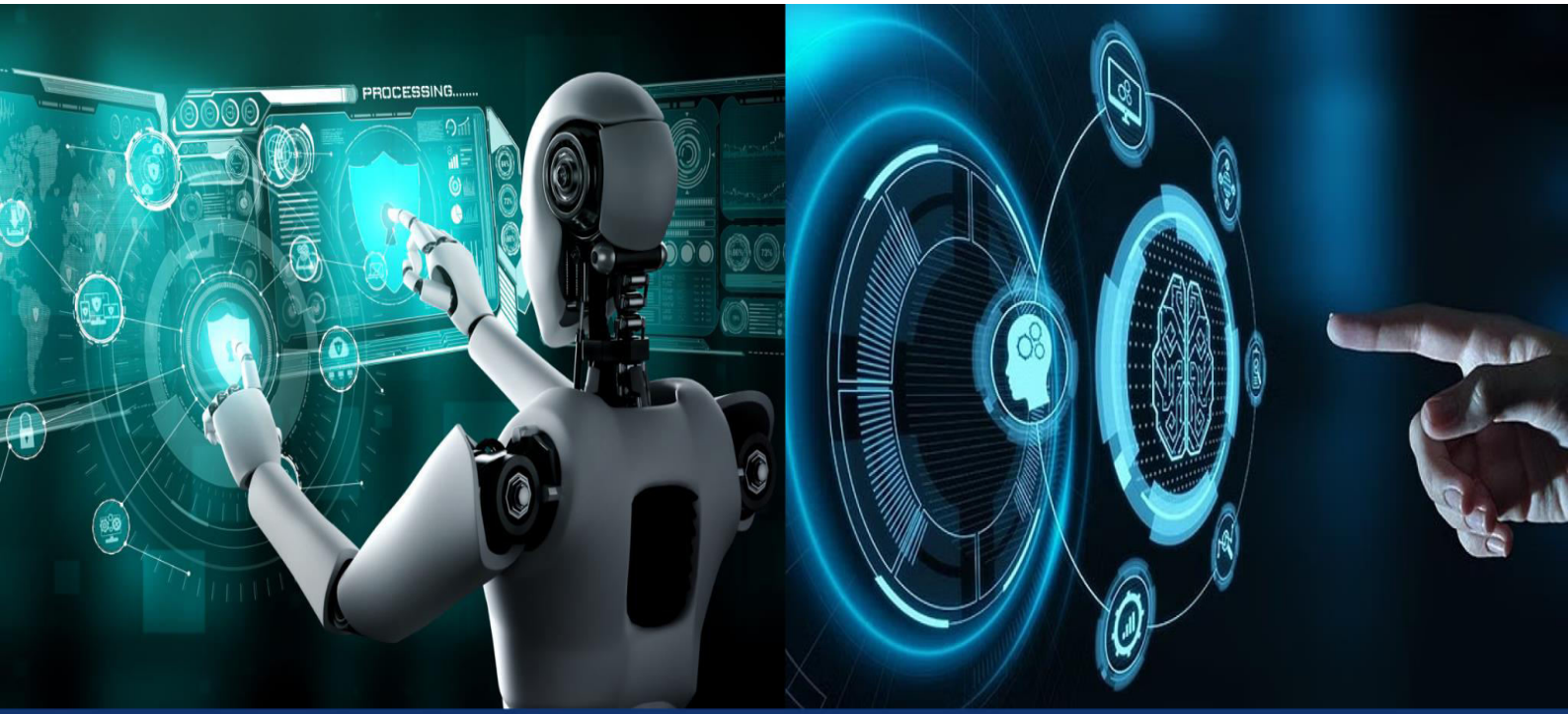
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 9.927

Volume 14, Issue 10, October 2026

© 2026 IJIRCCE | Volume 14, Issue 10, October 2026 DOI: 10.15680/IJIRCCE.2026.1410012

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Security Issues in IoT Networks

Dr. J.S.Prasath, Mahalakshmi H S

Professor, Department of CSE, Sapthagiri NPS University, Bengaluru, India

B.E Student, Department of CSE, Sapthagiri NPS University, Bengaluru, India

ABSTRACT: Internet of Things (IoT) is widely used in variety of applications including weather monitoring, agriculture crop yield prediction, retail, logistics, healthcare, waste management, pollution monitoring, smart traffic management, has integrated smart devices into critical sectors such as healthcare, agriculture, smart cities, and industrial automation. The large number of interconnected devices across IoT has introduced unique security vulnerabilities. Conventional security protocols, designed for huge resource computing systems are often incapable of handling constrained hardware, inadequate battery life, and low-latency requirements of IoT edge devices. This proposed work presents a comprehensive review of investigating latest advancements in IoT data security. This proposed work addresses the security issues, evaluates the features of lightweight cryptographic algorithms, and various challenges in IoT networks. The comparative analysis of existing models is done based on accuracy, energy efficiency, computational overhead, and scalability. It is essential to propose the lightweight cryptography (LWC) algorithms for constrained devices with the consideration of processing power, memory size, and battery power consumption. Traditional public-key algorithms like RSA and Elliptic Curve Cryptography (ECC) rely on the extreme difficulty of factoring massive prime numbers or solving discrete logarithms. Quantum cryptography can be used to generate and distribute secure encryption keys. Post-Quantum Cryptography uses advanced, new mathematical algorithms that run on classical computers and it is strong enough to resist quantum attacks without requiring special quantum hardware.

KEYWORDS: Internet of Things, Data Security, Lightweight Cryptography, Intrusion Detection Systems (IDS), Data Security.

I. INTRODUCTION

Internet of Things (IoT) represents a paradigm shift in ubiquitous computing, where physical objects are embedded with sensors, processing capabilities, and communication modules to exchange data over the internet. As of recent estimates, the number of connected IoT devices has surpassed tens of billions, driving innovations in smart homes, automated agriculture, industrial control systems, and wearable healthcare devices. While the benefits of IoT are immense, including enhanced operational efficiency and real-time decision-making, the security implications of deploying billions of relatively unsecured endpoints are profound. IoT networks are inherently vulnerable due to their unique architectural characteristics. Unlike traditional IT infrastructure, IoT devices often operate in physically exposed environments, making them susceptible to tampering. Furthermore, these devices are heavily constrained in terms of computational power, memory, and energy. Consequently, standard security mechanisms such as the Advanced Encryption Standard (AES) with large key sizes or complex handshake protocols introduce unacceptable latency and drain battery life rapidly. Attackers exploit these vulnerabilities to launch devastating cyber-attacks, including Distributed Denial of Service (DDoS) campaigns orchestrated by botnets (e.g., Mirai), ransomware, data breaches, and privacy violations. The core objective of data security in IoT networks is to maintain the fundamental tenets of information security: Confidentiality, Integrity, and Availability (CIA), while adapting to the resource limitations of the network. This has spurred a massive wave of academic and industrial research focused on "lightweight security." Researchers are exploring novel cryptographic ciphers that minimize clock cycles, machine learning models that can detect zero-day anomalies at the edge, and decentralized architectures like block chain and federated learning to secure data transmission without relying on vulnerable central servers. This literature review systematically investigates recent high-quality research papers addressing these specific IoT security domains. The review is structured to first establish the background of IoT security challenges, followed by an in-depth analysis of selected contemporary methodologies. We then present a comprehensive comparative analysis of these approaches, highlighting their real-world applicability, advantages, and technical limitations. Finally, we synthesize these findings to identify critical research gaps and outline future scopes for emerging scholars and engineers.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

II. LITERATURE REVIEW

This work provides a comprehensive investigation of recently proposed frameworks and developed models targeted at justifying IoT data security challenges. This work provides the insights of lightweight cryptography, quantum-inspired neural networks, and explainable AI. The early reconnaissance phase of cyber-attacks, specifically port scanning is addressed in which attackers map the vulnerable IoT devices before launching destructive payloads [1]. This framework provides a strong first line of defense, blocking attackers before they can establish a foothold. The various standards and classification of cryptographic algorithms, features and variety of lightweight cryptography algorithms is investigated [2]. The requirements of lightweight cryptography are memory size, power and energy consumption, circuit size, throughput, and latency. The various features, benefits, applications, security issues and solutions of 6G IoT are examined [3]. The various key performance indicators associated with 6G networks including peak data rate, mobility requirements, coverage, spectral efficiency, connectivity density, latency, reliability, maximum operating frequency and energy efficiency are discussed. The novel cryptography algorithm is developed for encryption of alphanumeric characters [4]. This cryptography algorithm can be utilized for preventing the theft and fraud in online money transactions. The hybrid security algorithm is proposed along with the exclusive hardware key using embedded system [5]. This security algorithm is cost effective and it prevents the sensitive process information from unauthorized access and modification. The cryptography algorithm is proposed that performs encryption and decryption of combination of alphabets, numbers, and special characters [6]. This cryptography algorithm assures data confidentiality across internet, and data security in remote access. The novel cryptography algorithm is developed for encryption and decryption of string [7]. This cryptography algorithm can be utilized for preventing the credit card fraud, and securing the industrial continuous varying process variables. The innovative cryptography algorithm is proposed for encryption of text messages [8]. It generates large number of bits as cipher text during encryption for a smaller text input. The hybrid cryptography is proposed which includes symmetric AES, asymmetric RSA and hash functions that strengthens the data security across IoT [9]. It is developed and implemented in real-time environment using embedded system with IoT. The physical and environmental security of agricultural IoT systems is addressed [10]. Conventional farm security relies heavily on manual guarding or basic CCTVs, which are inefficient and prone to high false alarm rates. The comprehensive taxonomy and survey on security risk assessment frameworks tailored for IoT is examined [11]. This work provides a highly structured theoretical foundation for understanding IoT vulnerabilities. The highly sophisticated framework for real-time malware defense combining quantum-inspired AI and advanced cryptography is introduced [12]. This work highlights the inability of standard deep learning models to process complex, high-dimensional IoT malware signatures quickly and accurately. The specific problem of securing visual data generated by resource-constrained IoT cameras is addressed [13]. Real-time video encryption using AES (Advanced Encryption Standard) rapidly depletes battery life and causes frame drops. The high-dimensional IoT network traffic overcomes standard machine learning algorithms, causing high latency in anomaly detection is addressed [14]. The immense reduction in computational overhead makes this system ideal for rapid detection on edge gateways. The optimal secure defense mechanism for Distributed Denial of Service (DDoS) in IoT network using feature optimization and intrusion detection system is proposed [15]. The hybrid deep learning model is designed which integrates convolutional neural network (CNN) and diagonal XG boosting (CNN-DigXG) for the fast and accurate intrusion detection in IoT network. The dual challenges of data privacy and distributed threat detection is addressed [16].This mechanism perfectly preserves user privacy and reduces bandwidth usage. The black box problem of Artificial Intelligence in cyber-security is examined [17]. It enhances the usability of AI security systems for human operators and accelerates incident mitigation. The innovative hybrid security algorithm is developed and implemented in real-time using an embedded system [18]. This hybrid security algorithm allows secure monitoring of harmful gases include liquefied petroleum gas, propane, methane, butane, alcohol and hydrogen in the industrial environment. The physical layer reliability of IoT networks related to signal degradation in environments with physical obstacles and multipath propagation is addressed [19]. The integrated compound models provide a significantly more accurate estimation of Quality of Service (QoS) and link reliability than traditional singular fading models. The security system is proposed for wireless monitoring of accident information through the internet [20]. The accident detection device installed in a vehicle will transmit information to the pre-installed numbers of the driver's family members, police station, ambulance and nearest hospital. The modified security algorithm along with the dedicated hardware key using embedded system is proposed which enables secure transmission and monitoring of process parameters through the internet [21]. This modified security algorithm integrates asymmetric, symmetric, and hash-value generation algorithms to protect data confidentiality, integrity, and authentication. The modified asymmetric and hash algorithm is proposed which generates the large key size of 2048-bit and 512-bit respectively [22]. It prevents malicious modification of industrial devices, and ensures authentication across internet. The real-time implementation of embedded system for secure monitoring of wastewater treatment

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

process through the internet is proposed [23]. The content of dissolved oxygen and pH value is encrypted using embedded system and transmitted across wireless networks. The innovative bank security system is proposed which is highly secure and it is based on cost-effective embedded system that ensures bank security through the release of knock-out gas [24]. It is fully automated system which ensures safety to highly valuable customer's documents, cash, and expensive ornaments present in the bank locker. The various security issues and security attacks related to industrial control system is examined [25]. It is essential that every industry should follow security standard and security mechanisms in order to protect the industrial equipment and should assure safety to the operator.

III. SECURITY ISSUES IN IOT NETWORKS

The Perception Layer

This layer comprises physical sensors and actuators that collect data from the environment. Security threats in perception layer include physical tampering, node capture, and signal jamming. Since data is often stored locally in plaintext before transmission, physical access can lead to direct data compromise.

The Network Layer

This layer is responsible for transmitting data through protocols like Wi-Fi, Zigbee, LoRaWAN (Long Range Wide Area Networks) or cellular networks. Vulnerabilities include eavesdropping, Man-in-the-Middle (MitM) attacks, routing attacks, and spoofing. Secure data transmission relies heavily on the robustness of this layer.

The Middleware Layer

This layer aggregates, processes, and stores data, often involving cloud or edge computing infrastructure. It is targeted by malware, SQL injection, and DDoS attacks aimed at overwhelming processing capabilities or corrupting databases.

The Application Layer

This layer is user-interface layer where data is visualized and controlled. Weak authentication, insecure APIs, and poor access controls make this application layer a major target for unauthorized access and data theft.

IV. NEED FOR LIGHTWEIGHT SECURITY ALGORITHMS

Traditional cryptographic algorithms, such as RSA and standard AES, require substantial computational overhead. In an IoT context, executing these algorithms can cause unacceptable delays, particularly in real-time systems like autonomous vehicles or remote healthcare monitoring. Moreover, the energy required for complex cryptography drastically shortens the lifespan of battery-operated sensors. Conventional security mechanisms are more expensive and very slow for real-time applications and high-frequency data transmission, resulting underpowered devices to run insecurely. Lightweight Cryptography (LWC) such as lightweight block ciphers, stream ciphers, and tailored Elliptic Curve Cryptography reduces gate density, chip area, latency, and power consumption. LWC aims to balance security and performance by utilizing smaller block sizes, simplified rounds, and optimized mathematical structures. Constrained networks are the major targets for DoS, node cloning, packet fabrication, and man-in-the-middle attacks. Lightweight authentication protocols, hash chains, and IDS protect the network without crushing node resources.

Hybrid encryption techniques integrate symmetric and asymmetric cryptography methods to accomplish both efficiency and security. Elliptic Curve Cryptography (ECC) based hybrid encryption mechanism offer a exciting balance between security and computational efficiency.

V. COMPARATIVE ANALYSIS OF EXISTING SECURITY MECHANISMS

To synthesize the reviewed literature, we present a comparative analysis of the methodologies based on critical IoT performance metrics: Security Method, Accuracy, Energy Efficiency, Computational Overhead, Scalability, and Limitations. Table 1 shows the comparison of various existing security mechanisms based on accuracy, energy and computational overhead, scalability, and limitations.

© 2026 IJIRCCE | Volume 14, Issue 10, October 2026 DOI: 10.15680/IJIRCCE.2026.1410012

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Table 1 Comparison of Existing Security Mechanisms

Reference	Security Method / Algorithms	Accuracy / Performance	Energy and Computational Overhead	Scalability	Key Limitations
Almomani et al. (2026)	Ensemble ML (XGBoost, Random Forest) for Port Scans	High precision on IoTID20 dataset	Moderate (requires edge gateway processing)	High (Distributed edge)	May miss sophisticated zero-day payload exploits
Chowdhury et al. (2025)	Multi-sensor fusion (PIR, Laser, MQ-2, Flame) + Threshold logic	94.38% nighttime detection efficiency	Highly energy efficient; low overhead (Arduino)	Moderate (Farm-scale)	Lacks AI predictive analytics; relies on GSM availability.
Kumari (2025)	QSANN + Polar Codes Cryptography + MOFDOA	99.5% accuracy, 96% precision	High computational overhead for QSANN training	High (Cloud/ Edge integration)	Difficult to deploy purely on constrained microcontrollers.
Aribilola et al. (2025)	SuPOR lightweight stream cipher (Möbius transformations)	Cryptographically secure (passes NIST tests)	Very Low overhead (Linear time complexity)	High (Per-device encryption)	Network communication overhead not fully evaluated.
Punia et al. (2025)	Whale Transfer + Sine-Cosine Feature Selection + ML	High anomaly detection rate on Bot-IoT dataset	Low runtime overhead; High training overhead	High (Network layer)	Meta-heuristic optimization is slow during initial setup.
Rahmati (2024)	Federated Learning (RNN) + Homomorphic Encryption	>98% accuracy for DDoS	Moderate edge energy; High server computation	Very High (Decentralized)	Homomorphic encryption adds aggregation latency.
Baral et al. (2024)	XAI (SHAP/ LIME) + Large Language Models (LLMs)	High human-interpretability	Very High overhead (requires LLM hosting/API)	Moderate (Backend processing)	Unfeasible for offline, disconnected edge environments.

© 2026 IJIRCCE | Volume 14, Issue 10, October 2026 DOI: 10.15680/IJIRCCE.2026.1410012

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

VI. SECURITY CHALLENGES IN IOT NETWORKS

Despite significant advancements, implementing robust data security in real-world IoT networks presents several persistent challenges.

Resource Constraints

The fundamental challenge remains the lack of CPU, memory, and battery power on edge devices. Energy consumption is a major concern in IoT device adoption and the resource-constrained devices seek to reduce energy consumption. Resource-constrained IoT devices are embedded devices ranging from microcontroller units to single-board computers whose compute, memory, storage, and energy budgets are strongly limited. Memory constraints can be overcome by utilizing data compression, efficient memory management, and prioritization of critical data to ensure optimal functionality. The various power management mechanisms such as sleep modes and energy harvesting, are employed to guarantee these devices can function independently for long periods.

Heterogeneity and Interoperability

IoT networks consist of diverse devices from various manufacturers using different protocols such as Zigbee, Bluetooth, Wi-Fi, and LoRaWAN. Devices transmit and structure data using a multitude of different application-layer protocols, including MQTT, AMQP, CoAP, XMPP, and HTTP. Designing a unified, cross-platform security framework is extremely difficult. Interoperability ensures that data is structured and formatted in a common way. Devices built with different hardware or software can still communicate and coordinate because they adhere to the identical standards. Interoperability makes it easier to scale IoT deployments globally, as devices won't be locked into a single vendor ecosystem.

Zero-Day Attacks

Hackers can exploit zero-day vulnerabilities before their targets even know about them, allowing threat actors to sneak into networks undetected. When the hacker exploits a zero-day vulnerability to break into a network, zero trust architecture can limit the damage. Zero trust uses continuous authentication and least privilege access to prevent lateral movement and block malicious actors from reaching sensitive resources. The attacker gains unauthorized access, turning the device into a botnet node, stealing data, or breaching the broader home or enterprise network. While zero day vulnerabilities are unknown, regular updates can sometimes include fixes for related vulnerabilities or strengthen overall system security. When a zero day exploit is released or discovered to be in use, it can propagate rapidly across targets worldwide, especially if it is easily automatable or integrated into malware toolkits. Attackers may leverage phishing, drive-by downloads, or compromised websites to distribute the exploit, resulting in large-scale breaches.

Physical Vulnerability

Many IoT devices (e.g., agricultural sensors, smart city cameras) are deployed in public spaces. Attackers can physically access the hardware to extract hardcoded cryptographic keys via side-channel attacks (power analysis) or JTAG interfaces. IoT device vulnerability refers to any weakness or flaw in an IoT device that can be exploited by attackers to compromise the device's functionality, gain unauthorized access, or steal sensitive data. These vulnerabilities arise from various factors such as weak passwords, insecure network services, outdated software components, and insufficient physical or software protections. Physical access allows an attacker to pull out internal memory cards or storage media to reverse-engineer software, read local logs, or steal hardcoded credentials. Vulnerabilities in IoT devices results in substantial security risks for both users and industries. Cooperated devices can be stolen to introduce attacks such as botnets or Distributed Denial-of-Service (DDoS) attacks, resulting in service disruptions. They can also expose sensitive data, including personal and corporate information, leading to data breaches and compliance violations. Furthermore, attackers can use vulnerable IoT devices to gain access to internal networks, jeopardizing critical systems and physical infrastructure, especially in environments that lack robust IoT fingerprinting and identity management.

VII. RESEARCH GAPS

Most current systems utilize static encryption algorithm regardless of the device's current battery state. A gap exists for algorithms that can dynamically downgrade encryption strength slightly when the battery is critical, prioritizing availability while maintaining an acceptable security baseline. The Federated Learning effectively addresses privacy issues, the integration of Homomorphic Encryption introduces significant latency. It is essential to propose lightweight

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

privacy-preserving aggregation mechanisms that do not rely on heavy mathematical transformations, ensuring real-time threat sharing. Explainable AI (XAI) is currently too heavy for the edge solutions like Large Language Models (LLMs) and Shapley Additive Explanations require immense backend computing. Developing lightweight, on-device interpretability models that can instantly explain an anomaly directly at the gateway level is an unsolved problem. Due to the advancement in quantum computing, present lightweight ciphers which often rely on Elliptic Curve Cryptography (ECC) or simplified stream ciphers are outdated. Post-Quantum Lightweight Cryptography tailored particularly for constrained devices and requires extensive empirical validation.

VIII. FUTURE SCOPE

The future work of data security in IoT lies in the convergence of decentralized architectures, autonomous AI, and advanced hardware security. Future research directions include:

- **Edge-Native Federated Learning:** Developing optimized FL algorithms that can run entirely on microcontrollers, allowing swarm-intelligence threat detection without any cloud dependency.
- **Hardware-Assisted Security:** Integrating Physical Unclonable Functions (PUFs) into IoT chipsets. PUFs utilize microscopic manufacturing variations to generate unique, unstealable cryptographic keys, solving the physical tampering problem.
- **Quantum-Resistant Lightweight Algorithms:** Transitioning to lattice-based or hash-based cryptography that provides post-quantum security while remaining lightweight enough for battery-operated devices.
- **Digital Twin Security Testing:** Utilizing IoT Digital Twins (virtual replicas of the physical network) to safely simulate zero-day attacks and train ML models in an isolated environment before deploying the models to the physical network.

IX. CONCLUSION

Securing data in IoT networks requires a paradigm shift from traditional IT security to highly optimized, resource-aware, and decentralized frameworks. This proposed work investigated the security issues in different IoT layers, need for lightweight cryptography algorithms, and security challenges in IoT networks. The security requirements in IoT networks are data confidentiality, data integrity, data freshness, authentication, and authorization. The lightweight security algorithms are essential for constrained devices. The future IoT deployments must embrace a multi-layered defense strategy integrating hardware-level tamper resistance, ultra-lightweight stream ciphers for data-in-transit, and decentralized, federated AI for real-time, privacy-preserving threat detection. By bridging the identified research gaps particularly in quantum-resistant LWC and edge-native Explainable AI, researchers can forge a resilient and secure future for global IoT infrastructure.

REFERENCES

[1] O. Almomani, A. Almomani, and S. Memon, "Enhancing IoT Security Using Machine Learning for Port Scan Attack Detection," Procedia Computer Science, Vol. 275, pp. 532-540, 2026.
[2] J.S.Prasath**, "**Investigation of Lightweight Cryptography Algorithms," International Journal of Computer Science and Mobile Computing, Vol. 15, No. 9, pp. 41-56, 2026.
[3] J.S.Prasath, **"**6G Internet of Things: Issues, Challenges and Applications," International Journal of Science, Engineering and Technology, Vol. 14, No. 4, pp. 1-9, 2026.
[4] J.S.Prasath, "Proposed Cryptography Algorithm for Alphanumeric Characters Encryption and Decryption," Journal of Network and Information Security, Vol. 14, No. 1, pp. 32-50, 2026.
[5] J.S.Prasath, "Proposed Hybrid RSA, AES and SHA Algorithms with Hardware Key Security Mechanisms for Embedded Systems with Internet of Things," The Indonesian Journal of Computer Science, Vol. 15, No. 3, pp. 4299-4313,2026.
[6] J.S.Prasath, "PrasathSrinivasan Cryptography Algorithm for Text Encryption and Decryption," International Journal of Scientific Research in Science, Engineering and Technology, Vol. 13, No. 3, pp. 427-445, 2026.
[7] J.S.Prasath, Sushmitha G S, "PrasathSrinivasan Sushmitha Algorithm for String Encryption and Decryption," International Journal of Engineering and Techniques, Vol. 12, No. 1, pp. 550-56, 2026.
[8] J.S.Prasath, Sushmitha G S, Swathi R, "Development of Novel Cryptography for Information Security," International Journal of Engineering Inventions, Vol. 14, No. 6, pp. 115-120, 2025.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

[9] J.S.Prasath, "Implementation of Internet of Things Based Data Security using Hybrid Cryptography," International Journal of Wireless and Microwave Technologies, Vol. 15, No. 3, pp. 66-77, 2025.
[10] S. Chowdhury et al., "Enhanced IoT-based smart agro-farm security system through multi-sensor fusion and field validation," Smart Agricultural Technology, Vol. 12, 2025.
[11] M. Waqdan, H. Louafi, and M. Mouhoub, "Security risk assessment in IoT environments: A taxonomy and survey," Computers and Security, Vol. 154, 2025.
[12] S. Kumari, "Next-Gen IoT Security using Polar Codes-based Cryptography for malware defence through quantum self-attention neural network," Knowledge-Based Systems, Vol. 321, 2025.
[13] I. Aribilola, S. H. Alsamhi, J. G. Breslin, and M. N. Asghar, "SuPOR: A lightweight stream cipher for confidentiality and attack-resilient visual data security in IoT," International Journal of Critical Infrastructure Protection, Vol. 50, 2025.
[14] A. Punia, M. Tiwari, and S. S. Verma, "A machine learning-based efficient anomaly detection system for enhanced security in compromised and maligned IoT Networks," Results in Engineering, Vol. 26, 2025.
[15] J.S.Prasath, V.Irine Shyja, P.Chandrakanth, B.Kiran Kumar, Adam Raja Basha, "An optimal secure defense mechanism for DDoS Attacks in IoT Network using feature optimization and intrusion detection system," Journal of Intelligent and Fuzzy Systems, Vol. 46, No. 3, pp. 6517-6534, 2024.
[16] M. Rahmati, "Federated Learning-Driven Cybersecurity Framework for IoT Networks with Privacy-Preserving and Real-Time Threat Detection Capabilities," Western University, 2024.
[17] S. Baral, S. Saha, and A. Haque, "An Adaptive End-to-End IoT Security Framework using Explainable AI and LLMs," arXiv preprint arXiv:2409.13177, 2024.
[18] J.S.Prasath, U. Ramachandraiah, S.Prabhuraj, G.Muthukumaran, "Internet of Things based Hybrid Cryptography for Process Data Security," Journal of Mathematical and Computational Science, Vol. 10, No. 6, pp. 2208-2232, 2020.
[19] A. Sehgal, R. Agrawal, R. Bhardwaj, and K. K. Singh, "Reliability Analysis of Wireless Link for IoT Applications Under Shadow-Fading Conditions," Procedia Computer Science, Vol. 167, pp. 1515-1523, 2020.
[20] J.S.Prasath, U. Ramachandraiah, "Embedded Systems with Internet of Things for Secure Monitoring of Vehicle Accidents," Journal of Green Engineering. Vol.10, No. 7, pp. 3291-3299, 2020.
[21] J.S.Prasath, U. Ramachandraiah, G. Muthukumaran, "Modified Hardware Security Algorithms for Process Industries using Internet of Things," Journal of Applied Security Research, Vol. 16, No. 1, pp. 127-140, 2020.
[22] J.S.Prasath, U.Ramachandraiah, "Modified Asymmetric and Hash Algorithms for Internet Enabled Industrial Automation," Test Engineering and Management Journal, Vol. 83, pp. 7431-7444, 2020.
[23] J.S.Prasath, S.Jayakumar, K.Karthikeyan, "Real-Time Implementation for Secure monitoring of Wastewater Treatment Plants using Internet of Things," International Journal of Innovative Technology and Exploring Engineering, Vol. 9, No.1, pp. 2997-3002, 2019.
[24] J.S.Prasath, R. Natesan, N. Jeyakkannan, "Implementation of Embedded based Bank Security System using Knock-out Gas," International Journal of Engineering and Technology, Vol. 7, No. 4, pp. 4654-4657, 2018.
[25] J.S.Prasath, "Security in Industrial Wireless Networks," International Journal of Computer Technology and Applications, Vol. 5, No. 3, pp. 1302-1308, 2014.

AUTHOR PROFILE



Dr. J.S.Prasath received Master of Engineering degree from Annamalai University, Chidambaram and Doctor of Philosophy degree from Hindustan Institute of Technology and Science, Chennai, India. Currently he is working as Professor in the Department of Computer Science and Engineering at Sapthagiri NPS University, Bengaluru, India. He is an interdisciplinary and guiding many Research projects at Under graduate and Post graduate level. Earlier he served as Assistant Professor in SRM University, Hindustan University, KCG College of Technology and Narayana Engineering College. His research interests are Data Science, Artificial Intelligence, Data Security, Internet of Things, Embedded Systems, Wireless Sensor Networks, and Industrial Automation. He has published thirty two research articles in International Journals, presented twenty papers in International Conferences, published two patents, written three books, and three book chapters. He received the best teacher award and the two innovation awards for his research work.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Mahalakshmi H. S. is an engineering student with a keen interest in cyber-security, Internet of Things (IoT), and Network Security. She is passionate about exploring emerging technologies, understanding security challenges in connected systems, and learning about effective approaches to protecting digital networks. Her academic interests include identifying vulnerabilities in IoT networks, understanding potential cyber threats, and exploring security measures to improve data privacy, confidentiality, and system reliability. She is interested in developing the lightweight cryptography algorithms for IoT applications and contributes towards securing interconnected devices in today's digital world.



INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details