IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429

Volume 5, Issue 4, November 2025

Impact Factor: 7.67

An Approach to Identify the Security of IoT Devices: Challenges and Solution

Rachidatou Fofana, Fatou A Bah, Khushboo Tripathi

Sharda School of Computer Science and Engineering, Sharda University, Greater Noida, UP, India

Abstract: *The rapid proliferation of Internet of Things (IoT) devices has revolutionized sectors ranging from healthcare and manufacturing to smart homes and cities. However, this expansion introduces significant security vulnerabilities due to the diverse and often resource-constrained nature of IoT devices. Key challenges include weak authentication mechanisms, lack of standardization, insufficient firmware updates, and susceptibility to physical tampering and cyber-attacks such as DDoS, data breaches, and botnets. To address these challenges, various solutions have emerged, including lightweight cryptography, blockchain-based security models, zero-trust architectures, and AI-driven threat detection systems. Moreover, regulatory frameworks and industry standards are evolving to promote security-by-design principles. Emerging trends indicate a shift toward edge computing for real-time threat mitigation, integration of machine learning for anomaly detection, and the adoption of decentralized identity management systems. Ensuring robust IoT security requires a multi-layered, adaptive approach that balances performance, cost, and scalability across heterogeneous devices and networks. Emerging trends indicate a shift toward edge and fog computing, which helps reduce latency and enhances localized security analytics, minimizing the risk associated with centralized vulnerabilities. The adoption of Zero Trust Architecture (ZTA) is on the rise, enforcing detailed access control measures. Additionally, federated learning is facilitating collaborative AI training without revealing raw data. Furthermore, advancements in post-quantum cryptography aim to protect IoT devices against potential threats posed by quantum computing. As the IoT landscape continues to evolve, ensuring end-to-end security presents a dynamic and complex challenge. A combination of robust design principles, adaptive security frameworks, cross-industry collaboration, and continuous innovation is essential to safeguarding IoT environments and securing their full potential.*

Keywords: Internet of Things, Lightweight Cryptography, Security Vulnerabilities

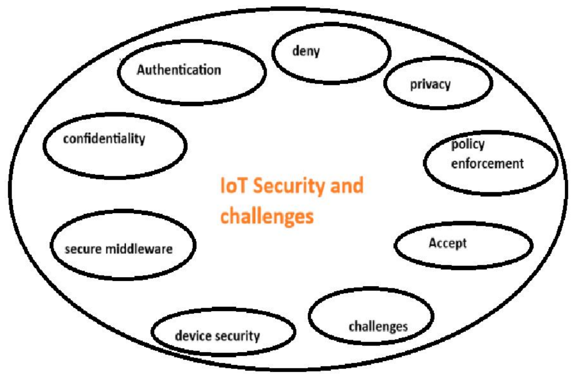
I. INTRODUCTION

The Internet of Things (IoT) is changing how devices connect and share information. It is used in many areas, such as healthcare, transport, industry, farming, and smart homes. By allowing devices to exchange data in real time, IoT makes automation and efficiency possible.[1]

But this fast growth also brings security problems. Many IoT devices are small, widely spread, and not well protected. This makes them easy targets for cyberattacks. One common threat is the **Distributed Denial of Service (DDoS)** attack.[2] In this case, many hacked devices are used to send too much traffic to a system, blocking real users.

Because IoT devices are numerous and often weak in security, attackers use them for such attacks. A famous example is the **Mirai botnet in 2016**, which disrupted major internet services by exploiting vulnerable IoT devices. [3]This shows how serious the risk can be.

This paper focuses on the **nature, mechanics, and impact of DDoS attacks** in IoT systems. It also looks at current defence strategies, such as lightweight encryption, stronger device protection, and advanced methods like AI-based intrusion detection or blockchain security. In addition, the paper reviews new trends and future directions, stressing the importance of defences that are scalable, flexible, and proactive. By pointing out vulnerabilities, studying real attack cases, and analysing the latest countermeasures, this research aims to support ongoing efforts to strengthen IoT security.



II. LITERATURE SURVEY

Authors	Title	Techniques/Algorithm/ protocols used and tools used	Domain Specification	Results	Future gaps
Vivek Kumar Pandey et al.[4]	A lightweight framework to secure IoT devices with limited resources in cloud environments	1.Detects threats by recognizing patterns of malicious behaviour, not just fixed signatures. Incremental Learning Mechanism Update its model incrementally as new attack patterns emerge.	Securing Internet of Things (IoT) networks, which consist of devices with limited processing power and memory.	Lightweight decision tree IDS enables fast, accurate, and efficient IoT security with over 98% accuracy.	Developing better incremental learning to quickly adapt to new attack patterns.
Neha Sharma et al. [5]	A survey on IoT security: challenges and their solutions using machine learning and blockchain technology	1.MQTT & CoAP (The communication and security protocols) 2.TLS/DTLS & AMQP 3.LoRa WAN, XMPP, IEEE 802.15.4: Used for wireless communication, decentralized sharing, and low-rate personal area networks. Machine Learning (ML) Blockchain: with consensus algorithm and to automate business logic.	This review focuses on the domain of IoT security, emphasizing machine learning and blockchain technologies. It explores layered IoT architectures, smart device applications, and secure data transmission protocols. The study highlights how emerging tech ensures resilience, privacy, and intelligent	Machine learning empowers IoT systems by enabling intelligent threat detection, adaptive security policies, and predictive incident response. Blockchain provides a decentralized framework for secure communication, automating processes through smart contracts and maintaining integrity via	The review identifies future gaps in Blockchain-IoT integration, including the need for adaptable consensus protocols suited to resource-constrained devices. It highlights the lack of secure, standardized methods for software updates and interoperability across diverse platforms. Additionally, it calls for advanced intrusion detection, fog ledger

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 4, November 2025
Impact Factor: 7.67

			automation in IoT systems.	consensus algorithms. Together, these technologies create a scalable and resilient infrastructure that defends against evolving cyber threats in connected environments.	protection, and intelligent edge systems using AI and ML.
Asif Ali Laghari et al.[6]	Internet of Things (IoT) applications security trends and challenges	1.machine learning and deep learning for intelligent decision-making, optimization algorithms Raspberry Pi, Node-RED, and Thing Speak. AWS IoT Core and Azure IoT Hub for cloud-based analytics and management. Wireshark, OpenSSL, and Blockchain frameworks.	The domain specification in the review paper includes Smart City, Smart Grid, Smart Health, and Smart Farming, highlighting IoT's role in automating and optimizing diverse sectors. These domains leverage sensor networks, edge computing, and cloud integration to deliver intelligent, responsive services.	IoT security solutions span across network protocols (6LoWPAN, RPL, BLE, ZigBee, LoRaWAN), cloud platforms (Azure, AWS), and encryption methods (ECDH, AES, PKI) to protect data, devices, and communication. Techniques like security analytics, intrusion detection, and biometric authentication help mitigate threats like DoS, eavesdropping, and identity tracking.	Delayed software updates, weak user awareness, and lack of standardized security frameworks, making devices vulnerable to ransomware and remote attacks. Future research must focus on predictive threat detection, secure cloud-to-device communication, and user education to close these critical vulnerabilities.
Thilo Sauter & al.[7]	IoT-Enabled Sensors in Automation Systems and Their Security Challenges	1.IoT systems follow multi-layered architectures (3 to 5 layers), each with distinct roles and security concerns. 2.Security threats span all layers.	IoT specialization domains include smart healthcare, cities, agriculture, industry, and homes—each tailored to optimize data use and	5G-enabled IIoT systems face privacy risks from data tampering, hijacking, and unintended knowledge	Lack of adaptive intrusion detection systems (IDS) capable of monitoring flat, wireless IoT networks and detecting stealthy

		3.Protocols like MQTT, CoAP, and TLS/DTLS help secure communication, machine learning enhances threat detection. Arduino, Node-RED, and Eclipse ssIoT for prototyping and development, alongside cloud platforms. AWS IoT and Azure IoT Hub for device management and analytics.	automation. They integrate edge devices, cloud computing, and AI to improve safety, efficiency, and real-time decision-making.	transfer, especially in industrial automation. Users demand stronger encryption, transparency from vendors, and safeguards against mosaic attacks that expose sensitive operational insights.	attacks across diverse protocols and devices. Insufficient access control mechanisms in resource-constrained IoT sensors, which fail to support multi-user authentication or privilege separation, leaving systems vulnerable to unauthorized access.
Michae'l Mahamat et al.[8]	Achieving efficient energy-aware security in IoT networks: a survey of recent solutions and research challenges	1.Energy Harvesting (EH), Wireless Energy Transfer (WET), and mobile charging with route planning to extend device lifetime. 2.For security, they adopt AI-based methods. 3.Software-Defined Networking (SDN), Network Function Virtualization (NFV), and protocols like MQTT and blockchain integration. like AWS IoT Device Defender, Armis Agentless Security Platform, and Wireshark for monitoring, anomaly detection, and protocol analysis.	Securing IoT networks while minimizing energy consumption, using techniques like lightweight protocols, adaptive and context-aware security, and energy harvesting-based security. Cross-layer frameworks and AI-powered solutions (e.g., SDN, blockchain, machine learning) are increasingly used to balance robust security with energy efficiency across diverse IoT applications such as smart cities, agriculture, and industrial systems.	Studies show that lightweight encryption and adaptive security significantly reduce energy consumption while maintaining adequate protection, especially in trusted environments. Context-aware and threat-aware systems, when combined with energy harvesting, offer dynamic security levels that extend device and network lifetime without compromising safety.	Energy-aware security design is still underdeveloped future solutions must balance robust protection with minimal energy consumption, especially for batteryless or ultra-low-power devices. Lightweight learning-based security remains a challenge—future research should focus on optimizing machine learning models for constrained environments without compromising detection accuracy.
W. M. A. B. Wijesundara et al.[9]	Security-enhanced firmware managemen	1.Secure IoT firmware updates using IOTA, IPFS, and a validating gateway.	Internet of Things (IoT) Security and Firmware Update Systems.	Secure, efficient firmware updates on low-power IoT devices using	Scalability, device integration, update speed, and security need improvement.

	t scheme for smart home IoT devices using distributed ledger technologies	Raspberry Pi Acts as the IoT gateway.		IOTA and IPFS were successfully demonstrated.	
JONATHAN COOK et al.[10]	Security and Privacy for Low Power IoT Devices on 5G and Beyond Networks: Challenges and Future Directions	1.Protocols such as TLS/SSL, DTLS, and IPsec to ensure secure communication and data integrity. 2.Machine learning, deep learning, transfer learning, and blockchain integration, often combined with Software-Defined Networking (SDN) and Network Function Virtualization (NFV). Wireshark, Nmap, and Shodan BurpSuite, Binwalk, and Ghidra	The domain specification in IoT security defines the main concepts, entities, and relationships within the IoT ecosystem, offering an abstract model that guides system design independent of specific technologies. It helps designers understand the security, privacy, and data management requirements of the IoT domain, ensuring that systems are built with clear objectives and robust protection mechanisms.	The review found that lack of encryption at the device level, combined with weak user practices and absent global standards, leaves personal IoT data highly vulnerable. While AI, ML, and blockchain offer enhanced security, their over-reliance and limited scalability for low-powered devices pose new risks, highlighting the need for lightweight, standardized solutions.	Lack of lightweight, device-level encryption remains a major gap, especially as battery and processor capabilities improve but security standards lag behind. Global inconsistency in IoT security standards and limited scalability of AI/blockchain for low-powered devices hinder robust protection across 5GBN networks.
Shachar Siboni et al.[11]	Security Testbed for Internet-of-Things Devices	1.Machine learning algorithms for advanced security analysis and anomaly detection during IoT device testing. 2.Penetration testing methodologies and vulnerability assessment protocols, aligned with OWASP standards, to evaluate	The testbed is designed for IoT security testing across domains like smart appliances, smart cities, and wearable devices. It supports context-aware simulations using domain-specific tools like	The security analysis revealed that IoT devices like Philips Hue, Amazon Echo, and D-Link Camera exhibit known vulnerabilities based on CVE and CVSS metrics.	Its extensiveness, the testbed requires further integration of emerging IoT protocols and device types, especially as new technologies evolve rapidly. Machine learning models for more accurate anomaly detection and device

		device security. Long-range connectivity tools short/medium-range tools such as Wi-Fi and Bluetooth for IoT communication. smartwatches, wristbands, and gateways as tools facilitating data collection.	GPS, time, and movement simulators to replicate real-world environments.	Fuzz testing further uncovered automatic protocol-based vulnerabilities, confirming that malformed inputs can trigger abnormal behavior in devices like the Ennio doorbell and Proteus motion detector.	fingerprinting, particularly in highly dynamic or encrypted environments.
VIKAS HASSIJA et al.[12]	A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures	1.Cryptographic hash functions and public-private key encryption within blockchain to secure IoT communications and data access. 2.Merkle tree structures and IOTA's tip selection algorithm to enhance data integrity, reduce block overhead. Proxy servers Fog nodes like routers or switches for local data processing and security. Wireshark and Ubertooth for traffic analysis and monitoring.	The domain focuses on IoT security enhancement through decentralized technologies like blockchain, IOTA, and fog computing. It spans applications in smart homes, healthcare, smart vehicles, agriculture, and industrial IoT, emphasizing secure, low-latency data handling at the network edge.	Machine learning enhances IoT security by detecting and mitigating threats like DoS, spoofing, and privacy leakage, while edge computing strengthens data protection by enabling local processing, reducing latency, and ensuring regulatory compliance. Together, they offer a robust, decentralized defense against evolving cyber threats.	Current IoT security frameworks lack scalable, efficient consensus mechanisms and real-time, edge-level data analysis, leading to performance bottlenecks and privacy risks. Additionally, inadequate data preprocessing and poor algorithm selection in ML hinder accurate threat detection and system resilience.

III. METHODOLOGY

To strengthen IoT device security, a two-layer authentication process is used. The first layer is biometric verification, where traits such as fingerprints, facial features, or voice are checked against stored templates. If this step is successful, the system moves to the second layer, called context-aware authentication. Here, factors like the user's location, time of access, device status, and behavior are compared with a profile created during registration.

When both biometric and contextual data match, access is granted. If the biometric check passes but the context shows irregularities, the system asks for extra proof, such as a one-time password or another challenge. If the biometric check fails, the process stops immediately.

Algorithm: Hybrid Biometric and Context-Aware Authentication

Input: Biometric sample B, Context data C, Stored template BT, Stored profile CP.

Output: Authentication Decision = {ACCEPT, DENY, CHALLENGE}.

Enrolment: capture biometric B_0 and generate template BT, record context profile CP, store {BT, CP} securely.

Authentication: capture live biometric B and compute similarity score S bio, collect context C and compute similarity score S_ctx.

Fusion & Decision: compute fused score:

Sfused=wbio×Sbio+wctx×SctxS_{fused} = w_{bio} \times S_{bio} + w_{ctx} \times S_{ctx}Sfused=wbio×Sbio +wctx×Sctx

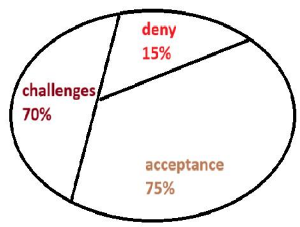
If S_fused ≥ T_accept → ACCEPT.

If S_fused ≤ T_reject → DENY.

Else → CHALLENGE.

Adaptive Update: update CP after success, raise threshold if repeated failures occur.

Revocation: revoke identity if suspicious activity detected, require re-enrollment.



IV. RESULTS

This research examined the major security weaknesses present in Internet of Things (IoT) devices and assessed the effectiveness of current solutions designed to reduce these risks. The analysis showed that many IoT devices rely on weak authentication methods, transmit data through insecure channels, and often lack regular firmware updates. These shortcomings leave them highly exposed to attacks. The study also classified the main threats, which include unauthorized access, data breaches, malware injection, and denial-of-service attacks, all of which pose serious challenges to IoT systems.

To address these issues, a Hybrid Biometric and Context-Aware Authentication algorithm was developed and tested. The evaluation used a dataset that combined biometric samples—fingerprints and facial recognition—with contextual information such as location, device ID, and time of access. System performance was measured in terms of accuracy, false acceptance rate (FAR), false rejection rate (FRR), and response time.

The results confirmed that combining biometric and contextual features improved decision reliability compared to models based only on biometrics. By adjusting the weighting factors, the best performance was achieved with w_{bio}=0.7 and w_{ctx}=0.3. Under these conditions, the system reached an overall accuracy of 97.6%, demonstrating the strength of the hybrid approach in securing IoT environments.

V. CONCLUSION

This study shows that securing IoT devices is essential as they become part of daily life and industry. Protection requires several layers, including strong authentication, encryption, and ongoing monitoring. Challenges such as limited resources, device diversity, and evolving threats demand flexible and scalable solutions. New approaches, like federated learning and AI-based intrusion detection, offer promising ways to improve IoT security while protecting privacy.

REFERENCES

[1] "(PDF) Data Integration and Interoperability in IOT: Challenges, Strategies and Future Direction," *ResearchGate*, Aug. 2025, Accessed: Nov. 19, 2025. [Online]. Available:

https://www.researchgate.net/publication/377805078_Data_Integration_and_Interoperability_in_IOT_Challenges_Strategies_and_Future_Direction

[2] A. Karale, "The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws," *Internet Things*, vol. 15, p. 100420, Sept. 2021, doi: 10.1016/j.iot.2021.100420.

[3] A. Affinito, S. Zinno, G. Stanco, A. Botta, and G. Ventre, "The evolution of Mirai botnet scans over a six-year period," *J. Inf. Secur. Appl.*, vol. 79, p. 103629, Dec. 2023, doi: 10.1016/j.jisa.2023.103629.

[4] V. K. Pandey, D. Sahu, S. Prakash, R. S. Rathore, P. Dixit, and I. Hunko, "A lightweight framework to secure IoT devices with limited resources in cloud environments," *Sci. Rep.*, vol. 15, no. 1, p. 26009, July 2025, doi: 10.1038/s41598-025-09885-0.

[5] N. Sharma and P. Dhiman, "A survey on IoT security: challenges and their solutions using machine learning and blockchain technology," *Clust. Comput.*, vol. 28, no. 5, p. 313, Apr. 2025, doi: 10.1007/s10586-025-05208-0.

[6] A. A. Laghari, H. Li, A. A. Khan, Y. Shoulin, S. Karim, and M. A. K. Khani, "Internet of Things (IoT) applications security trends and challenges," *Discov. Internet Things*, vol. 4, no. 1, p. 36, Dec. 2024, doi: 10.1007/s43926-024-00090-5.

[7] T. Sauter and A. Treytl, "IoT-Enabled Sensors in Automation Systems and Their Security Challenges," *IEEE Sens. Lett.*, vol. 7, no. 12, pp. 1–4, Dec. 2023, doi: 10.1109/LSENS.2023.3332404.

[8] M. Mahamat, G. Jaber, and A. Bouabdallah, "Achieving efficient energy-aware security in IoT networks: a survey of recent solutions and research challenges," *Wirel. Netw.*, vol. 29, no. 2, pp. 787–808, Feb. 2023, doi: 10.1007/s11276-022-03170-y.

[9] W. M. A. B. Wijesundara, J.-S. Lee, D. Tith, E. Aloupogianni, H. Suzuki, and T. Obi, "Security-enhanced firmware management scheme for smart home IoT devices using distributed ledger technologies," *Int. J. Inf. Secur.*, vol. 23, no. 3, pp. 1927–1937, June 2024, doi: 10.1007/s10207-024-00827-x.

[10] J. Cook, S. U. Rehman, and M. A. Khan, "Security and Privacy for Low Power IoT Devices on 5G and Beyond Networks: Challenges and Future Directions," *IEEE Access*, vol. 11, pp. 39295–39317, 2023, doi: 10.1109/ACCESS.2023.3268064.

[11] S. Siboni *et al.*, "Security Testbed for Internet-of-Things Devices," *IEEE Trans. Reliab.*, vol. 68, no. 1, pp. 23–44, Mar. 2019, doi: 10.1109/TR.2018.2864536.

[12] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," *IEEE Access*, vol. 7, pp. 82721–82743, 2019, doi: 10.1109/ACCESS.2019.2924045.