International Journal of Emerging Engineering and Technology (IJEET)
ISSN (e): 2958-3764
Volume: 5, Number: 1, Pages: 55 - 61, Year: 2026

Cybersecurity Challenges and Defense Mechanisms in IoT: A Comprehensive Analysis of Emerging Threats and Intelligent Solutions

Humaira Ramzan[1,*], Irshad Ahmed Sumra[2], and Syed Bilal Gillani[3]

[1]Department of Information Security, University of Management and Technology, Lahore, Pakistan
[2]Department of Computer Science, University of Management and Technology, Lahore, Pakistan
[3]Department of Artificial Intelligence, University of Management and Technology, Lahore, Pakistan
[*]Corresponding author: Humaira Ramzan (Email: s2025375006@umt.edu.pk)

Received: 12/02/2026, Revised: 22/05/2026, Accepted: 15/06/2026

Abstract: **In the modern world, connected devices have revolutionized almost every aspect of life, from hospitals and factories to homes and city infrastructure. Today's large-scale IoT deployments have significantly expanded the attack surface, making it increasingly difficult for organizations to manage emerging cybersecurity risks. Legacy communication protocols, resource-constrained devices, and inadequate authentication mechanisms are frequently exploited for botnet recruitment, data theft, and service disruption. This paper provides a comprehensive overview of the IoT threat landscape and reviews defense mechanisms proposed to address these security challenges. It also examines the application of artificial intelligence (AI) and blockchain technologies in IoT security architectures while discussing emerging research directions, including federated learning, explainable AI, edge-native security, and post-quantum cryptography. The review concludes that no single security mechanism is sufficient to protect modern IoT ecosystems. Instead, a multilayered security strategy that integrates conventional security mechanisms with intelligent, adaptive technologies provides a more effective defense against evolving cyber threats**.

***Index Terms*—Internet of Things, Cybersecurity, Intelligent Threat Detection, Artificial Intelligence, Machine Learning, Intrusion Detection Systems, Lightweight Cryptography, Zero-Trust Architecture.**

I. INTRODUCTION

The Internet of Things has evolved from a research concept into a mainstream technology over the last decade. Data is continuously generated by sensors embedded in hospital equipment, robots on assembly lines, traffic management systems, agricultural monitors, and consumer appliances. According to Lu and Xu, the number of active IoT devices is projected to exceed 30 billion within the next few years, with the largest deployments in healthcare, smart grids, and industrial applications. Similarly, Granjal et al. reported that the rapid growth of IoT connectivity has outpaced the ability of many organizations to effectively manage the expanding attack surface [1-5].

The hardware of IoT devices, by contrast, is usually designed under strict power and cost constraints and does not have the processing power, memory, or battery capacity required to support traditional security controls Vulnerabilities identified after deployment can remain on a device throughout its operational lifetime, as update mechanisms are often unavailable or poorly designed. M. Ammar et al. analyzed the security of IoT frameworks and identified default credentials and unsigned firmware as the two most common causes of device-level compromise [6-10].

These risks have been demonstrated in real-world scenarios. In 2016, the Mirai botnet compromised hundreds of thousands of cameras and home routers, creating a large-scale DDoS attack that disrupted major DNS infrastructure, as documented by [11,12]. More recently, as P. P. Ray points out in his architectural survey [13-16], ransomware attackers have increasingly targeted connected medical devices and industrial controllers because disrupting critical services often enables them to obtain ransom payments more quickly than data exfiltration alone.

A variety of solutions have been proposed in response to these security challenges. A. Dorri et al. proposed blockchain-assisted identity registries to eliminate the need for a central trust broker [3]. M. Roopak et al. demonstrated that unusual traffic patterns can be identified using deep-learning classifiers without requiring full-packet capture [5]. Diro and Chilamkurti proposed a distributed attack detection approach for IoT networks with different topologies [6]. However, these advancements are not sufficient to keep pace with the rapidly evolving threat landscape.

This paper is a collection of the latest research on IoT security. It includes the main attack types and attack vectors, existing and emerging defense methods ranging from cryptography to zero-trust architectures, the application of AI and blockchain in operational security, and open research challenges that require further investigation. The methodology is described in Section II. Section III presents the threat landscape, Section IV discusses defense mechanisms, Section V

explores AI and blockchain technologies, Section VI highlights future research directions, and Section VII concludes the paper.

II. RESEARCH METHODOLOGY

The review is structured with a literature search that aims at surfacing high quality and recent literature related to IoT cyber security. IEEE Xplore, ACM Digital Library, Science Direct, Springer Link and Google Scholar databases were searched. Search strings included terms for IoT security, machine learning-based intrusion detection, and blockchain trust management, lightweight cryptographic protocols, federated learning, and zero-trust network design, and were limited to publications from 2013 to 2026. The inclusion criteria were guided by four research questions. RQ1: What are the most frequent types of attack on IoT ecosystems, and how? RQ2: What are the methods for lowering risk during deployments in resource limited environments? RQ3: What are the applications and challenges of using AI and blockchain with IoT security architectures? RQ 4: What are the current methods lacking and what are the prospects for future research? Papers were initially evaluated based on title and abstract, and subsequently full text by applying methodological assessment. Non-peer reviewed content and short abstracts with no findings were excluded as well as content which was duplicate. The selection process is illustrated in Fig. 1 and a summary of the results at each stage is given in Table I.

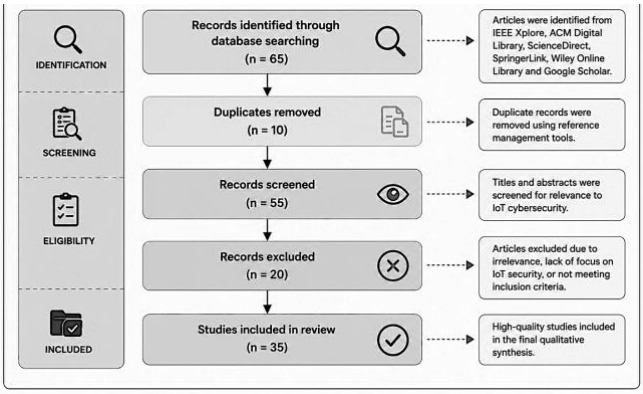

Fig. 1 Literature selection process: records were identified from five databases, duplicated, screened by title and abstract, and assessed for eligibility before final inclusion.

TABLE I. LITERATURE SELECTION AT EACH STAGE OF THE REVIEW

Stage	Articles
Database search results	65
After deduplication	55
After title/abstract screening	43
Excluded on full-text review	8
Included in final review	35

Thirty-five studies met all the criteria and are used as the main evidence base as shown in Table I. These cover the fundamental concepts of network security, applied cryptography, machine learning, and distributed systems, which are all multidisciplinary areas of research for IoT security [17-24].

A. Overview of Reviewed Studies

The six studies selected as representative, along with their focus and contribution, as well as the most significant limitation each acknowledged are presented in Table II. These range from blockchain-based trust, deep learning intrusion detection, to AI-augmented security – covering the key technical threads throughout the paper.

TABLE II. REPRESENTATIVE STUDIES: FOCUS, CONTRIBUTION, AND ACKNOWLEDGED LIMITATION

Study	Focus	Key Contribution	Main Limitation
Lu & Xu [1]	IoT security survey	Taxonomy of threats and controls	Limited AI-specific coverage
Dorri et al. [3]	Blockchain for IoT	Decentralised trust management	Scalability at large device counts
Diro & Chilamkurti [6]	Deep-learning IDS	Distributed attack detection	High inference overhead
Jolfaei & Kant [10]	AI + blockchain	Hybrid security model	Integration complexity
Restuccia et al. [18]	ML-driven security	Adaptive threat detection	Resource demands on edge devices
Sharma & Gupta [20]	Blockchain trust	Decentralised authentication	Latency and interoperability gaps

It is apparent from the set of proposals in Table II that there are frequently compromises between security level and use of resources that are discussed throughout subsequent sections.

III. THREAT LANDSCAPE FOR IoT SECURITY

From the physical devices and hardware to communication channels, network infrastructure, cloud-based back-ends and application interfaces, each layer in the stack is a potential target for an attack on IoT devices. An extensive discussion on the problems of IoT security has been carried out by S. Sicari et al., which highlighted this multi-layered attack surface [9] and R. Roman et al. have extended these findings for distributed deployment scenarios [8]. The important architectural layers, presented in Fig. 2, are mapped against these attack surfaces.

A. Weaknesses at the Device Level

Security is frequently neglected when IoT goods make it to the market. In their analysis of IoT framework vulnerabilities, M. Ammar et al. discovered that hard-coded or default credentials are still common in a variety of product categories [4]. The mechanism of delivering firmware updates is often not secure, allowing attackers to send out malicious images as if they were a legitimate patch. When hardware is installed in public spaces like on-street traffic sensors, utility meters, or farm monitors, the risk is different: if the attacker has a few short minutes of hands-on access, he or she could remove software, or install a hardware backdoor.

B. Communication and Protocol Weaknesses

Efficiency was the main consideration in the creation of the lightweight message protocols (MQTT, CoAP, ZigBee, BLE, and LoRaWAN) that enable IoT on limited hardware. However, J. Granjal et al. have analysed these protocols' security features

and found that many early versions did not include message encryption and mutual authentication [2]. Even if TLS were technically supported, it is hard to administer certificate on devices lacking a real time clock and persistent storage. In real world attacks, spoofing, replay, and man in the middle attacks all exploited these vulnerabilities as shown in further research by [21, 25].

The volume of deployments is a natural feed for a botnet. E. Bertino and N. Islam [22] demonstrated the Mirai campaign's ability to generate traffic that could knock over large DNS providers by hijacking a few hundred thousand webcams. Agustin Novo [23] shows that the most common attack vector in cloud-based IoT architectures is poorly secured APIs at the cloud-level. Many platforms offer REST endpoints where token validation is weak and/or there is no rate limiting, allowing the hacker to access an account from one device.

C. Data Privacy and Regulatory Risk

There are so many norms about privacy that apply to the Internet of Things, and the devices are likely to be capturing data about users that they don't know they are capturing, or that the user hasn't agreed to be captured. Two of the most neglected privacy protection features of implemented IoT systems are data minimization and access control, as highlighted by [9]. In addition to immediate damage from a fall victim to a breach, businesses that are subject to GDPR, HIPAA, or other privacy regulations face tremendous regulatory risks when connected devices are not properly protected or retained.

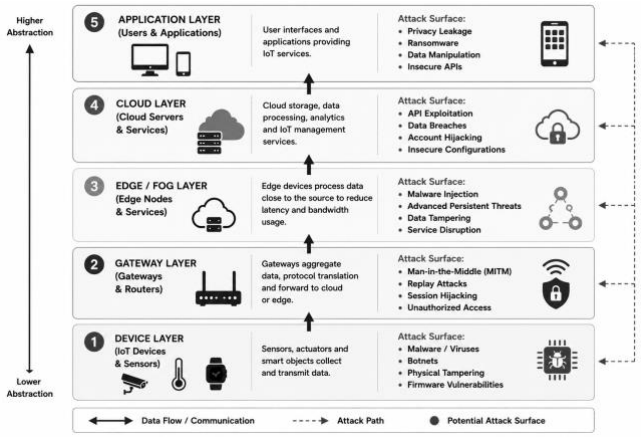

Fig. 2. IoT architecture layers and the primary attack surfaces at each tier, from physical devices at the base to user-facing applications [7].

When combined, the danger categories in Fig. 2 demonstrate that IoT security cannot be resolved at any one stage of the stack. Defenses must be constructed with the entire assault surface in mind [8].

IV. SECURE IOT DESIGN AND DEFENCE MECHANISMS

Most IoT security designs to date follow three basic principles: "keep the attack surface low at each layer," "authenticate all before access" and "always monitor for signs of compromise. M. Conti et al. [15] suggests that this multi-layered approach is important from the standpoint of active protection as well as IoT forensic preparedness.

A. Cryptography controls.

Data is encrypted when it resides in a cloud repository or when it is moving from a sensor to a gateway. Confidentiality and integrity are achieved by AES-128 or AES-256 in GCM mode for devices that have enough processor space. PRESENT, SIMON, and SPECK are cyphers suitable for low technology that are practical alternatives to AES. After doing a thorough analysis of the lightweight cryptography market, T. Nguyen and H. Kim came to the conclusion that the NIST Lightweight Cryptography standardization process is generating solutions for Class-1 IoT devices that strike a balance between security and efficiency [19]. K. Sharma and B. B. Gupta [20] showed that multilevel cryptographic authentication systems can reduce the risk of credential theft without too much computational overhead.

B. Access Control and Authentication

The device must be identified before it is allowed on the network. A. Ouaddah et al. showed that this is feasible with a scalable number of devices in realistic situations, proposing a blockchain-based access control architecture for the IoT which replaces central identity servers with a tamper-evident ledger [24-28]. At the application level, role and attribute-based access control only gives devices what they need; multi-factor authentication and short-lived access tokens reduce the damage caused by a stolen credential.

C. Intrusion Detection and Firmware Integrity

The reason why IoT devices continue to be compromised is that they often have firmware that can be modified without their users' knowledge. In M. Abomhara and G. M. Koien's survey on open challenges in IoT security [17], the secure-boot chain, the code-signing verifier for each update, and the hardware-trusted anchor make it much harder to modify the system without permission. Over-the-air update pipelines need to be end-to-end secured: signed manifests ensure authenticity, differential updating reduces bandwidth costs.

Unlike enterprise network intrusion detection systems (IDS), traffic baseline profiles for IoT are often more consistent. This was demonstrated by Y. Meidan et al. in their N-BaIoT system that uses deep auto encoders trained on device-specific traffic to detect botnets with very few false positives [25]. While actual performance will vary based on the similarity between the training and deployment data sets, M. Roopak et al. demonstrated extremely high detection rates (95%+) on standard test sets [5] for deep-learning classifiers.

D. Architecture of Zero-Trusted. Architecture of Zero-Trust.

All sessions, from any source address, are checked and authorized in a zero-trust way instead of perimeter trust, with continuous verification. J. Samaila et al. [14] have presented zero-trust as one of the most powerful architectural advices that are derived from the IoT security research. To deploy zero-trust, the device inventory must be reliable, the policy engine must be

able to make real-time access decisions and the telemetry pipelines must convey current information about the devices into those decisions. Table III shows a cross-reference of the major types of attacks with the controls often used to respond to them.

TABLE III. IOT ATTACK TYPES AND PRIMARY COUNTERMEASURES

Attack Type	Impact	Primary Countermeasure
DDoS / Botnet	Service disruption	Network segmentation, AI traffic filtering [22], [25]
Malware injection	Device compromise	Secure boot, signed firmware [17]
MITM / Replay	Data interception	Mutual TLS, nonce-based session tokens [2]
API exploitation	Unauthorised access	OAuth 2.0 / JWT, rate limiting [23]
Ransomware	Operational shutdown	Offline backups, immutable audit logs [3]
Privacy breach	Data exposure	End-to-end encryption, data minimisation [9]
Physical tampering	Persistent backdoor	Tamper-evident seals, TPM / PUF [4]

As Table III illustrates, it's not one control that's going to address all of the threats. As mentioned by M. Conti et al., resilience in IoT is achieved by ensuring that an attacker is unable to control the system when an attack on one layer is successful [15].

V. NEW IOT SECURITY TECHNOLOGIES

Traditional security tools that are based on rules and signatures struggle to keep up with attackers who continuously change their tactics. Blockchain technology and AI are among two technology families that have been receiving continuous research focus to enhance the adaptability of IoT security, according to Z. Ali et al. [11].

A. Programming Languages

The ability of ML models to learn from examples instead of having experts write down every possible attack pattern makes it an attractive prospect for IoT security. As per the research of M. Roopak et al., supervised classifiers like random forest, gradient boosted trees and support vector machines have showed excellent performance in network Intrusion Detection (NID) [5]. A. A. Diro and N. Chilamkurti extended this concept to distributed topologies of IoT and found that federated detection models can maintain classification accuracy with reduced communication overhead [6]. H. Sedjelmaci et al. demonstrated a cooperative IDS system that can achieve the detection rate greater than 97% in the presence of an assault simulation for vehicle IoT networks [26].There are serious practical issues. However, Restuccia et al. argue that adversarial inputs can cause a decrease in detection rate without triggering any alarms, and models trained on one network environment often perform poorly on another [18]. The Y. Zhang and T. Li also demonstrated that the explainability problems of black-box models are more prominent in healthcare IoT controlled environments [12].

B. Blockchain for Internet of Things (IoT) and Data Trustworthiness

The models are interesting for the IoT security space as they can be trained on examples and do not need an expert to manually list all possible attack patterns. Supervised classifiers like random forest, gradient-boosted trees and support vector machines have proven to provide good results in network intrusion detection systems as shown by M. Roopak et al. [5]. This was extended to distributed IoT topologies by A.A. Diro and N. Chilamkurti who found that federated detection models enable while reducing the communication overhead maintaining classification accuracy [6]. H. Sedjelmaci et al. presented cooperative IDS system that maintained the detection rate above 97% even when it was under attack simulation [26].There are real-life problems. The F states that even though adversarial examples may not raise an alarm, they may decrease detection rates, and models trained on one network environment often do not perform well on another [18]. The Y. Zhang and T. Li also demonstrated that explainability problems resulting from black-box models are more pronounced in regulated contexts such as healthcare IoT [12]. Scalability remains a constant problem. S. Otoum et al. [28] report that public blockchain can process only tens of transactions per second, whereas millions of IoT devices periodically request access to the blockchain will result in a significantly higher throughput requirement. Higher throughput is achieved by permissioned ledgers like Hyperledger Fabric, although some centralization is reintroduced; sharing and layer-2 aggregation solutions are being developed.

C. AI and Blockchain as Complementary Tools

While AI excels at detecting anomalies and classifying threats as they happen, it doesn't provide much insight into whether the information it processes is compromised. While the main limitation of blockchain would be the lack of immediate identification of active assaults, it does provide a dependable audit trail and decentralized identification management. Z. Ali et al. state that a combination of blockchain for identity and provenance and of AI for real-time detection has a larger attack surface than either approach alone [11]. Table IV presents a comparison of the major security properties of the two.

TABLE IV. COMPARISON OF AI AND BLOCKCHAIN AS IOT SECURITY TOOLS

Criterion	Artificial Intelligence	Blockchain
Core function	Threat detection & classification	Trust anchoring & audit trail
Real-time operation	Yes (with hardware support)	Limited by latency
Data integrity assurance	Indirect (model-dependent)	Strong (cryptographic proof)
Decentralization	Typically centralized training	Inherently decentralized
Scalability	High (with compression)	Constrained (throughput limits)
Explainability	Often a challenge	Transparent by design
Primary weakness	Adversarial robustness	Transaction throughput

While standards for interoperability between the two technology stacks have not yet been developed, as Z. Ali et al. explain [11],

a hybrid design pattern, where the detection is performed at the edge using ML technology and the tracking of security events is done on the blockchain, still seems to be a viable one (Table IV).

VI. FUTURE DIRECTIONS IN IOT

This is because the current deployment and research environment in the field presents a number of gaps that suggest future development needs. Table V lists the main problems and the most promising research directions to overcome the problems.

TABLE V. CURRENT RESEARCH GAPS AND EMERGING SOLUTIONS

Gap Area	Current Limitation	Promising Direction
Intrusion detection	High false-positive rates	Explainable, federated IDS [11], [12]
Device identity	Centralized CAs as failure points	Blockchain-based PKI [23], [24]
Privacy in ML	Raw data leaves device for training	Federated + differential-privacy learning [11]
Cryptography	Standard ciphers too heavy for MCUs	NIST LWC standardized primitives [19]
Adversarial robustness	Models fooled by crafted inputs	Certified-robust training, XAI [12]
Post-quantum readiness	Current public-key schemes vulnerable	CRYSTALS-Kyber, CRYSTALS-Dilithium [13]
Patch management	No scalable automated update mechanism	Signed OTA with blockchain provenance [3]

A. *Federated Learning*

The model address problems of privacy issues, however, requires a lot of network traffic to be concentrated to enable the model to be trained to make it viable. This problem is addressed in federated learning with each device or gateway training its network locally and sending only the gradient vectors to a global training phase without raw traffic on the devices, as presented by Z. Ali et al. [11]. They demonstrated that federated IoT security models have detection rates within a few percentage points of their centrally-trained counterparts and offer strong privacy guarantees, particularly when combined with differential privacy noise injection.

B. *Explainable AI for Security*

Operators need to understand the rationale behind what makes a device suspicious and triggers an automated action to isolate it from the network. Y. Zhang and T. Li have assessed XAI techniques in the context of cybersecurity, such as SHAP, LIME, and attention maps for sequence models, finding that these methods can be used to analyze and validate the logic behind a model and detect spurious correlations before they lead to a false classification [12]. Furthermore, they demonstrated that explainability helps with Adversarial robustness: when the model's robustness against an adversary requires a feature that is easily manipulated, this suggests that the feature should be revisited.

C. *Edge-Native Security*

Latency, bandwidth, and privacy issues arise when all device telemetry is sent to a centralized cloud for analysis. According to F. Restuccia et al., compressed machine learning models that provide sub-second detection latency without requiring a cloud round-trip can be executed by gateways with modest GPU or NPU capabilities [18]. By demonstrating that mode the problems occur when all device telemetry data is relayed to a central cloud for analysis, such as latency, bandwidth, and privacy. F. Restuccia et al. [18] suggest that it is possible to process machine learning algorithms with sub-second detection latency without having to make a round trip to the cloud by running them on gateways with modest GPU or NPU. In [28] S. Otoum et al. showed that deploying compressed models on practical gateway hardware can make such deep-learning sensor-network IDS at the edge viable.

D. *Post-Quantum Cryptography*

RSA and elliptic-curve cryptography would be compromised by quantum computers that could execute Shor's algorithm on a large scale. A. Kumar and B. Bhushan noted that long service lives of industrial IoT deployments mean that the equipment deployed today may still be in place when practical quantum computers are available, and explored NIST's post-quantum standardization process as the most realistic migration strategy [13]. NIST has now standardized CRYSTALS-Kyber for key encapsulation, and CRYSTALS-Lithium and FALCON, which are algorithms designed to resist quantum attacks, for signatures. Even though lattice-based operations are more computationally intensive than elliptic-curve operations, they are being optimized for embedded targets, such as done by T. Nguyen and H. Kim [19]. These new features are integrated into an architecture for future IoT systems as depicted in Fig. 3.

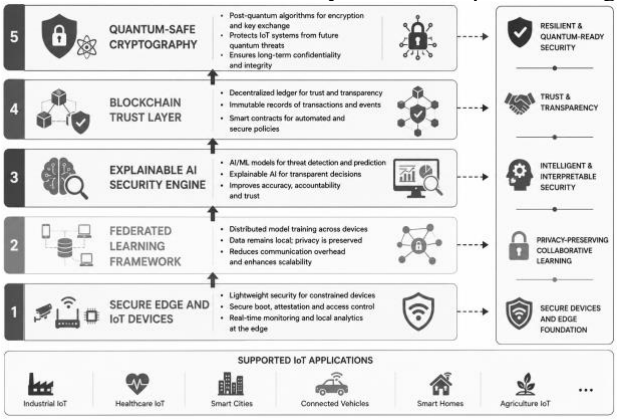

Fig. 3. Proposed architecture for a future secure IoT ecosystem, combining edge-native analytics, federated learning, explainable AI, blockchain-anchored identity, and post-quantum cryptographic primitives [13].

As Table V summarizes and as Fig. 3 illustrates, none of these methods is well-developed enough for off-the-shelf use today, but each has a gap that existing controls cannot fill. Work on interoperability, getting these elements to work as a cohesive field rather than each as a separate research path, would be useful to the field.

VII. CONCLUSION

The reality of IoT is constrained hardware, heterogeneous protocols, distributed deployment, and sophisticated attackers, and IoT security is a challenge because of this. This review has shown the evolution of the field from cryptographic hardening to more intelligent and adaptive solutions and identified the current gaps. Distributed deployment, heterogeneous protocols, limited hardware, and proficient adversaries combine to make IoT security extremely challenging. This overview has demonstrated the progression and evolution of the field from basic cryptographic strengthening to more sophisticated and flexible techniques and the areas which remain to be improved.

Device-level flaws, such as default passwords, unsigned firmware, and a lack of update mechanisms, continue to be the most abused entry points. In terms of scope and sophistication of protocol and network-layer attacks, and the deployment of cloud-based methods, API and access-control vulnerabilities have been added that are not protected by traditional network perimeters. The compliance dimension caused by data privacy and regulatory risk can only be fixed with technical controls.

The best defenses have one thing in common: They are not single control defenses. All of these components work together, rather than separately, and each can cover a different aspect of the attack surface. These solutions each cover a different part of the attack surface e and are most effective when used in combination rather than individually.

The technology of blockchain and AI are changing the face of IoT security in a complementary manner. Blockchain provides tamper evident identity and audit capabilities that the large-scale device estate requires. ML-based detection can identify new forms of attacks that are not covered by signature-based detection. The industry is still trying to work out the implementation costs of both technologies and neither is a complete solution.

As IoT deployments grow in the future, post-quantum cryptography, edge-native security processing, federated learning, and explainable AI (XAI) all address questions that will be more pressing. The future path forward is clear: IoT security needs to be more open, flexible and decentralized, but the road ahead is long, and there is much research to be done. Research efforts are beginning to fill in those pieces, but the basic issue that needs to be addressed is how to transition from lab to industrial.

CONFLICTS OF INTEREST

The authors declare no conflicts of interest to report regarding the present study.

AUTHOR CONTRIBUTIONS

Conceptualization, D.K. and P.K.; methodology, D.K.; software, D.K. and P.K.; validation, D.K.; writing—original draft preparation, D.K.; writing—review and editing, P.K.

FUNDING STATEMENT

This research received no external funding.

INSTITUTIONAL REVIEW BOARD STATEMENT

Not applicable.

INFORMED CONSENT STATEMENT

Not applicable.

DATA AVAILABILITY STATEMENT

Data is available on reasonable request.

REFERENCES

[1] Y. Lu and L. D. Xu, “Internet of Things (IoT) cybersecurity research: A review of current research topics,” IEEE Internet Things J., vol. 6, no. 2, pp. 2103–2115, Apr. 2019.

[2] J. Granjal, E. Monteiro, and J. Sá Silva, “Security for the Internet of Things: A survey of existing protocols and open research issues,” IEEE Commun. Surveys Tuts., vol. 17, no. 3, pp. 1294–1312, Thirdquarter 2015.

[3] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, “Blockchain for IoT security and privacy: The case study of a smart home,” in Proc. IEEE PERCOM Workshops, Kona, HI, USA, Mar. 2017, pp. 618–623.

[4] M. Ammar, G. Russello, and B. Crispo, “Internet of Things: A survey on the security of IoT frameworks,” J. Inf. Secur. Appl., vol. 38, pp. 8–27, Feb. 2018.

[5] M. Roopak, G. Y. Tian, and J. Chambers, “Deep learning models for cyber security in IoT networks,” in Proc. IEEE CCNC, Las Vegas, NV, USA, Jan. 2019, pp. 452–457.

[6] A. A. Diro and N. Chilamkurti, “Distributed attack detection scheme using deep learning approach for Internet of Things,” Future Gener. Comput. Syst., vol. 82, pp. 761–768, May 2018.

[7] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum, and N. Ghani, “Demystifying IoT security: An exhaustive survey on IoT vulnerabilities and a first empirical look on Internet-scale IoT exploitations,” IEEE Commun. Surveys Tuts., vol. 21, no. 3, pp. 2702–2733, Thirdquarter 2019.

[8] R. Roman, J. Zhou, and J. Lopez, “On the features and challenges of security and privacy in distributed Internet of Things,” Comput. Netw., vol. 57, no. 10, pp. 2266–2279, Jul. 2013.

[9] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, “Security, privacy and trust in Internet of Things: The road ahead,” Comput. Netw., vol. 76, pp. 146–164, Jan. 2015.

[10] A. Jolfaei and A. Kant, “Practical implications of blockchain and Internet of Things integration,” J. Ambient Intell. Humaniz. Comput., vol. 12, no. 1, pp. 1123–1135, Jan. 2021.

[11] Z. Ali, S. Shaukat, A. Masood, and H. U. Khan, “A survey of federated learning for edge computing: Research problems and solutions,” High-Confidence Comput., vol. 1, no. 1, Art. no. 100008, Dec. 2021.

[12] Y. Zhang and T. Li, “Explainable artificial intelligence applications in cyber security: State-of-the-art and challenges,” IEEE Access, vol. 10, pp. 109974–109993, 2022.

[13] A. Kumar and B. Bhushan, “Post-quantum cryptography for IoT: Challenges and future directions,” Int. J. Inf. Comput. Secure., vol. 18, no. 1–2, pp. 1–25, 2022.

[14] J. Samaila, M. Sequeiros, A. Freitas, M. Correia, and P. Inácio, “Security challenges and recommendations for IoT systems: A survey,” in Proc. IoTBDS, Porto, Portugal, Mar. 2018, pp. 257–264.

[15] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, “Internet of Things security and forensics: Challenges and opportunities,” Future Gener. Comput. Syst., vol. 78, pp. 544–546, Jan. 2018.

[16] P. P. Ray, “A survey on Internet of Things architectures,” J. King Saud Univ. Comput. Inf. Sci., vol. 30, no. 3, pp. 291–319, Jul. 2018.

[17] M. Abomhara and G. M. Køien, “Security and privacy in the Internet of Things: Current status and open issues,” in Proc. PRISMS, Aalborg, Denmark, May 2014, pp. 1–8.

[18] F. Restuccia, S. D’Oro, and T. Melodia, “Securing the Internet of Things in the age of machine learning and software-defined networking,” IEEE Internet Things J., vol. 5, no. 6, pp. 4829–4842, Dec. 2018.

[19] T. Nguyen and H. Kim, “Lightweight cryptography for the Internet of Things: A state-of-the-art survey,” IEEE Access, vol. 9, pp. 89404–89435, 2021.

[20] K. Sharma and B. B. Gupta, “Multilevel trust-based intelligence scheme for securing Internet of Things (IoT) against security attacks using cryptographic authentication,” J. Ambient Intell. Humaniz. Comput., vol. 11, no. 3, pp. 879–897, Mar. 2020.

[21] Addas, Abdullah, Muhammad Nasir Khan, and Fawad Naseer. "Waste management 2.0 leveraging internet of things for an efficient and eco-friendly smart city solution." *Plos one* 19, no. 7, e0307608, 2024.

[22] Naseer, Fawad, Muhammad Nasir Khan, Muhammad Tahir, Abdullah Addas, and SM Haider Aejaz. "Integrating deep learning techniques for personalized learning pathways in higher education." *Heliyon* 10, no. 11 2024.

[23] Naseer, Fawad, Muhammad Nasir Khan, Abdullah Addas, Qasim Awais, and Nafees Ayub. "Game mechanics and artificial intelligence personalization: A framework for adaptive learning systems." *Education Sciences* 15, no. 3, 301, 2025.

[24] Naseer, Fawad, Abdullah Addas, Muhammad Tahir, Muhammad Nasir Khan, and Noreen Sattar. "Integrating generative adversarial networks with IoT for adaptive AI-powered personalized elderly care in smart homes." *Frontiers in Artificial Intelligence* 8, 1520592, 2025.

[25] Y. Meidan et al., “N-BaIoT—Network-based detection of IoT botnet attacks using deep autoencoders,” IEEE Pervasive Comput., vol. 17, no. 3, pp. 12–22, Jul.–Sep. 2018.

[26] H. Sedjelmaci, S. M. Senouci, and T. Taleb, “An accurate and efficient collaborative intrusion detection framework to secure vehicular networks,” IEEE Trans. Intell. Transp. Syst., vol. 16, no. 3, pp. 1183–1192, Jun. 2015.

[27] Y. Li, “Deep reinforcement learning: An overview,” arXiv:1701.07274 [cs.LG], Jan. 2017.

[28] S. Otoum, B. Kantarci, and H. Mouftah, “On the feasibility of deep learning in sensor network intrusion detection,” IEEE Netw. Lett., vol. 1, no. 2, pp. 68–71, Jun. 2019.