International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(3s) 2026 pp. 966-1028
https://doi.org/10.70917/ijcisim-2026-2415
Article

Toward Resilient Smart Cities: A Systematic Comparative Survey of Blockchain-Integrated Deep Learning Architectures for IoT Authentication and Secure Communication

Ahmed Swar[I], **Mohammed Belal**[I], **Soha Ahmed Ehssan Aly**[I]

[I]Computer Science Department, Faculty of Computers and Artificial Intelligence,
Capital University (Formerly Helwan University), Cairo 12317, Egypt
ahmed.swar@fci.helwan.edu.eg, belal@fci.helwan.edu.eg, dr.soha@fci.helwan.edu.eg
Corresponding Author: Ahmed Swar (Email: ahmed.swar@fci.helwan.edu.eg)

Abstract: The growing adoption of Internet of Things (IoT) devices supports the development of smart cities but also brings serious security risks due to device diversity, limited computing resources, and an expanding attack surface. Traditional security tools are falling behind as cyber threats become more advanced, which has led researchers to explore new combinations of technologies. This survey offers a comparative analysis of how blockchain and deep learning (DL) can work together to strengthen IoT security in smart city settings, with particular attention to authentication methods and communication protocols. We look at how blockchain enables decentralized trust, tamper-resistant authentication, and auditable access control through Decentralized Identifiers (DIDs), smart contracts, and lightweight consensus protocols. In parallel, we study how deep learning supports adaptive intrusion detection, risk scoring, and anomaly monitoring using Convolutional Neural Networks (CNNs), Long Short-Term Memory networks (LSTMs), Graph Neural Networks (GNNs), and autoencoders. A central contribution of this work is a six-dimensional comparison framework that rates approaches on scalability, latency, security level, energy efficiency, privacy preservation, and interoperability. Our findings show that hybrid blockchain-DL designs outperform single-technology solutions across most of these dimensions, though open problems remain in cross-domain interoperability, consensus overhead, and adversarial robustness of DL models. We also evaluate eight benchmark IoT security datasets and outline a phased research roadmap covering short-term (2025–2027), medium-term (2027–2029), and long-term (2029–2032) goals. This survey is intended to serve as a practical reference for researchers and engineers working on secure, intelligent IoT systems for future smart cities.

Keywords: Internet of Things (IoT), Blockchain, Deep Learning, Authentication Architectures, Communication Protocols, Smart Cities, IoT Security, Comparative Review, Federated Learning.

1. Introduction

The Internet of Things (IoT) has reshaped computing and sensing over the past two decades, growing from a concept linked to radio frequency identification (RFID) into a worldwide network of billions of connected devices [1, 14]. Nowhere is this more visible than in smart cities, where sensors, actuators, cameras, and edge gateways collaborate to manage traffic, distribute energy, track public health, protect infrastructure, and raise the quality of urban services [2, 12]. The numbers tell a clear story: IoT-connected devices passed 10 billion in 2021, and projections place the figure at 41 billion by 2027, with more than 152,000 new connections coming online every minute [13, 15, 16]. At the same time, this rapid growth has opened up one of the largest attack surfaces in the history of networked systems.

The security consequences are serious. IoT devices range widely in capability, from Class 0 sensors with under 10 KB of RAM to full-featured edge servers, and many are placed in physically exposed, unattended locations with little capacity for firmware updates [59]. This mix of limited resources and physical accessibility creates real problems: studies estimate that roughly 60 percent of deployed IoT devices still lack basic encryption, leaving networks open to botnet takeover, ransomware, and chain-reaction failures in which one compromised node can spread weaknesses across the whole system [9, 10, 11, 159]. The Mirai botnet and its successors showed what this looks like in practice, turning hundreds of thousands of insecure devices into a distributed denial-of-service weapon that took down major internet services. Traditional defenses, including static authentication, perimeter-based access control, and centralized certificate authorities, are simply not built for this class of distributed, mixed-capability threats [26, 27].

Two technologies have emerged as the strongest candidates for addressing these gaps. The first is blockchain, which replaces centralized trust with a decentralized, tamper-proof ledger. A blockchain records timestamped transactions across a peer-to-peer network, maintaining data integrity without depending on any single authority [3, 33, 34]. For IoT security, this opens up several practical capabilities: device authentication through Decentralized Identifiers (DIDs), auditable access control via smart contracts, tamper-resistant event logging, and removal of single points of failure [42, 43]. The technology has matured rapidly; consortium and private blockchains now offer throughput above 1,000 transactions per second with sub-second finality, putting them within reach of real-time IoT demands [44, 46].

The second is deep learning (DL), a branch of machine learning that has changed how security systems detect, classify, and respond to threats. Where traditional intrusion detection relies on fixed rules or known signatures, deep learning models learn patterns directly from raw data, which makes them effective at catching novel attacks, zero-day exploits, and subtle behavioral changes [4, 68]. The range of useful architectures is broad: CNNs handle spatial patterns in network traffic for intrusion detection; LSTM networks and GRUs capture temporal sequences to spot multi-step attacks and support continuous authentication; autoencoders learn normal behavior profiles and flag departures as anomalies; and GNNs analyze the graph structure of device networks to find unusual interactions [5, 6, 69, 70]. Reinforcement learning adds another dimension, allowing models to improve continuously by interacting with the live IoT environment.

What makes the combination of blockchain and deep learning especially useful is that they address different parts of the security problem. Blockchain handles trust: immutable audit trails, decentralized identity, and automated policy enforcement through smart contracts. Deep learning handles intelligence: pattern recognition, anomaly detection, and behavioral profiling [7, 50]. Used together, they produce a security approach that is both verifiable and adaptive. Blockchain ensures that decisions are transparent, traceable, and resistant to tampering, while deep learning ensures that those decisions are informed, context-sensitive, and able to keep pace with changing threats. Several integration patterns have already taken shape, including Zero-Trust frameworks backed by blockchain where DL-based risk scores drive access decisions enforced through smart contracts, Blockchain-enabled Federated Learning (BlockFL) for privacy-preserving collaborative training with built-in defenses against model poisoning, and Explainable AI (XAI) paired with on-chain audit logs for accountable, traceable security decisions [8, 44, 96, 133].

Despite growing research activity at this intersection, the published literature remains scattered. Earlier surveys have covered blockchain for IoT [34, 51, 60, 61], machine learning for intrusion detection [23, 25, 120], federated learning for IoT privacy [97, 100], and blockchain-IoT use in sectors like healthcare [54, 118], transportation [55], smart grids [56, 57], smart agriculture [64], edge-fog-cloud computing [65], business process management [66], and cloud-AI-IoT integration [67]. Yet no existing work has brought together the combined use of blockchain and deep learning for IoT security with a clear focus on authentication architectures and communication protocols in smart city settings. This survey addresses that gap with a detailed comparative analysis of recent work (2023–2025), a structured identification of research gaps, and concrete directions for future effort.

A. Research Questions

This survey is organized around five research questions that cover the main aspects of blockchain-DL integration for IoT security:

• RQ1: What blockchain-based authentication architectures have been proposed for IoT in smart cities, and how do they compare in terms of scalability, latency, and trust model?

• RQ2: How effectively do deep learning techniques address continuous authentication and intrusion detection in resource-constrained IoT environments?

• RQ3: What synergies emerge from integrating blockchain and deep learning, and what are the dominant integration patterns (e.g., Zero-Trust, BlockFL, XAI+ledger)?

• RQ4: How do application-layer (MQTT, CoAP) and LPWAN (LoRaWAN, NB-IoT) protocols impact the feasibility and security of authentication handshakes?

• RQ5: What critical gaps, challenges, and future research directions remain for the convergence of these technologies in smart city deployments?

B. Key Contributions

The main contributions of this survey are:

• Comparative Review: We review recent studies (2023–2025) on the joint use of blockchain and deep learning for IoT security, organized through a taxonomy covering authentication architectures, intrusion detection, data integrity, and access control.

• Six-Dimensional Evaluation Framework: We assess reviewed approaches on scalability, latency, security level, energy efficiency, privacy preservation, and interoperability, with radar chart visualization for direct comparison.

• Protocol Analysis: We present the first integrated examination of how application-layer (MQTT, CoAP, AMQP) and LPWAN (LoRaWAN, NB-IoT) protocols affect the design of blockchain-DL authentication schemes, including newer standards such as OSCORE, EDHOC, and Matter.

• Dataset Evaluation: We compare eight benchmark IoT security datasets (Bot-IoT, TON_IoT, Edge-IIoTset, IoT-23, CICIDS2017, UNSW-NB15, N-BaIoT, and MedBIoT) on device diversity, feature set, attack coverage, and model performance.

• Research Roadmap: We map open research gaps through a coverage heat map and propose a three-phase roadmap covering short-term (2025–2027), medium-term (2027–2029), and long-term (2029–2032) priorities.

C. Survey Methodology

Our literature search was conducted across IEEE Xplore, Scopus, Web of Science, ACM Digital Library, and Google Scholar using combinations of keywords including 'blockchain IoT security', 'deep learning intrusion detection IoT', 'smart city authentication', 'federated learning IoT', and 'decentralized identity IoT'. The primary search window covers publications from 2020 to mid-2025, with emphasis on works from 2023 to 2025; foundational references from earlier periods are included where they establish important theoretical or technical context. Inclusion criteria required that studies (i) address IoT security using blockchain, deep learning, or both, (ii) present novel architectures, frameworks, or empirical evaluations, and (iii) be published in peer-reviewed venues or established preprint archives. We also include relevant IETF RFCs, NIST standards, and 3GPP specifications that define the protocol-level security landscape. This process yielded 177 references, of which over 40 are primary studies analyzed in our comparative tables. Table VI positions this survey relative to existing surveys to highlight our unique contributions.

TABLE VI. Comparison of This Survey with Existing Surveys

Survey	Year	BC	DL	Auth	Proto.	Smart City	Datasets	RQ-Driven	Roadmap
Al-Garadi et al. [23]	2020	✗	✓	Partial	✗	✗	Partial	✗	✗
Attkan & Ranga [34]	2022	✓	✓	✓	✗	✗	✗	✗	✗
Ferrag & Shu [61]	2021	✓	✗	✗	✗	✗	✗	✗	✗
Shammar et al. [49]	2021	✓	✗	Partial	✗	✗	✗	✗	✗
Ali et al. [50]	2024	✓	✓	✗	✗	✗	✗	✗	✗
Chaudhary et al. [63]	2022	✓	✗	✗	✗	✗	✗	✗	✗

Alsheavi et al. [108]	2024	✗	✗	✓	Partial	✗	✗	✗	✗
Dritsas & Trigka [95]	2024	✓	✓	✗	✗	✓	✗	✗	✗
Alotaibe [114]	2023	✗	✗	✓	✗	✗	✗	✗	✗
This Survey	2025	✓	✓	✓	✓	✓	✓	✓	✓

D. Paper Organization

The rest of this paper is structured as follows. Section II covers background material on IoT architecture, security vulnerabilities, core security requirements, smart city context, and the basics of blockchain and deep learning. Section III reviews related work through our proposed taxonomy, including blockchain-based authentication, deep learning for intrusion defense, convergence approaches, communication protocol security, platform-level analysis, and gap identification. Section IV presents comparative analysis results: a main comparison table of reviewed studies, authentication architecture comparison, protocol security evaluation, benchmark dataset analysis, and multi-dimensional framework assessment. Section V discusses open challenges, research problems, and future directions, including a three-phase roadmap. Section VI presents conclusions and revisits the research questions.

2. Background and Preliminaries

This section provides the foundational concepts essential for understanding the subsequent comparative analysis. We introduce the IoT architecture, its inherent vulnerabilities, core security requirements, the smart city context, and the fundamentals of blockchain and deep learning technologies.

A. IoT Architecture and Smart Cities

The Internet of Things (IoT) has revolutionized connectivity by linking billions of internet-enabled devices, enabling intelligent interactions and integrating physical infrastructure with digital systems across multiple industries, including smart factories, healthcare, smart cities, and transportation [12]. Initially developed to support radio frequency identification (RFID) technology, IoT now serves a broad spectrum of applications, from remote monitoring and real-time analytics to autonomous systems and intelligent infrastructure management [14]. The widespread adoption of IoT devices, their diverse functionalities, and the continuous advancement of communication protocols have spurred significant innovation in enabling technologies [17]. In addition, AI and ML techniques have amplified the potential of IoT by deriving valuable insights from diverse sensor data, thereby revolutionizing business operations and urban service delivery [18].

As depicted in Fig. 1, IoT systems are organized into five distinct layers, each serving a critical function. The perception layer includes physical devices such as sensors, actuators, RFID tags, cameras, and smart meters that monitor the environment and transmit data upward. The transport layer facilitates communication between devices and cloud-based platforms through protocols such as WiFi, LoRaWAN, NB-IoT, 5G, and Zigbee. The processing layer, hosted on edge, fog, or cloud platforms, provides storage, computation, scalability, and interoperability. The application layer oversees system functions, user interactions, and process management across domain-specific services. The business/analytics layer generates actionable insights through AI/ML-driven analytics to support decision-making [17, 18].

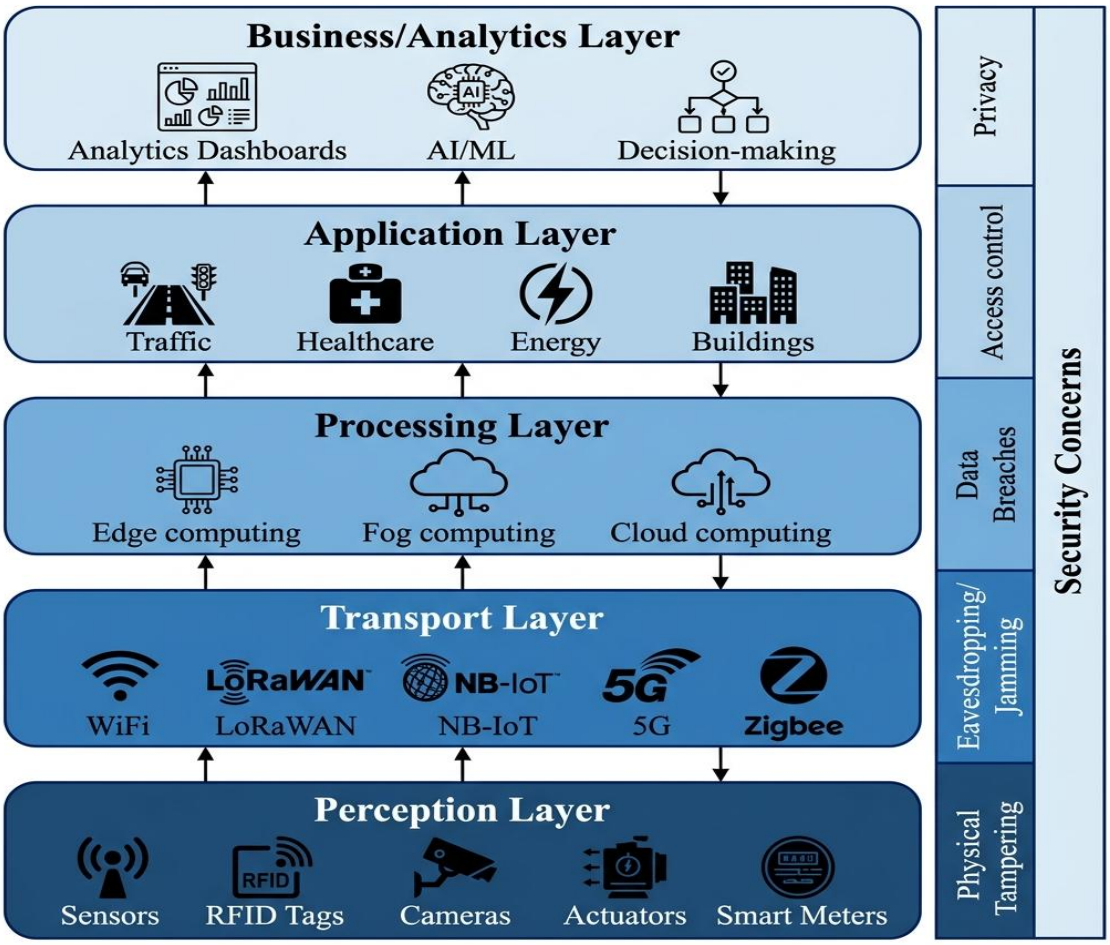

Fig. 1. Five-layer IoT architecture with associated security concerns at each layer.

IoT serves as a foundational enabler of smart city initiatives, integrating networks of sensors, actuators, and edge devices to enhance essential urban services such as intelligent traffic management, energy distribution, public healthcare, environmental monitoring, and public safety [158]. Smart city IoT deployments typically involve heterogeneous device populations ranging from Class 0 devices (severely constrained sensors with less than 10KB RAM) to Class 2+ devices (gateways and edge servers with substantial computing resources). This device heterogeneity creates unique security challenges that cannot be addressed by one-size-fits-all solutions [59].

However, the expansion of IoT in urban environments introduces significant security challenges. Device heterogeneity, insufficient firmware updates, and weak authentication mechanisms leave many systems vulnerable. Recent studies indicate that nearly 60% of deployed IoT devices still lack basic encryption, rendering them susceptible to botnet infiltration and ransomware attacks [159]. Further exacerbating these threats are architectural weaknesses, including the persistence of legacy operational technology (OT) systems, inadequate network segmentation, and insufficient real-time monitoring capabilities [160]. Privacy and regulatory concerns also present substantial obstacles; public skepticism regarding data collection practices has slowed several high-profile smart city projects [161]. In response, Zero-Trust Architecture (ZTA) principles, including continuous verification, least-privilege access, end-to-end encryption, and micro-segmentation, are increasingly adopted as the security approach for smart city deployments [160].

B. IoT Vulnerabilities and Attack Taxonomy

The security of the Internet of Things remains a critical concern, given the potential risks and safety issues posed by compromised devices. Research indicates that vulnerabilities persist due to protocol limitations, ineffective mitigation strategies, and challenges in real-time monitoring [19, 20]. These attacks commonly focus on different

layers of the IoT framework, often corresponding to the Open Systems Interconnection (OSI) model [20]. The interconnected structure of IoT systems significantly contributes to their susceptibility to malicious attacks [21].

As depicted in Fig. 2, each layer of the IoT architecture is prone to specific categories of threats. At the perception layer, adversaries exploit physical access to perform node tampering, side-channel attacks, RF jamming, malicious code injection, and device cloning. The network/transport layer faces man-in-the-middle (MITM) attacks, replay attacks, Sybil attacks, distributed denial-of-service (DDoS/DoS), eavesdropping, and routing attacks. The processing layer is vulnerable to SQL injection, malware, data breaches, privilege escalation, and API exploitation. The application layer faces cross-site scripting (XSS), phishing, identity spoofing, session hijacking, and ransomware attacks [22, 23, 24].

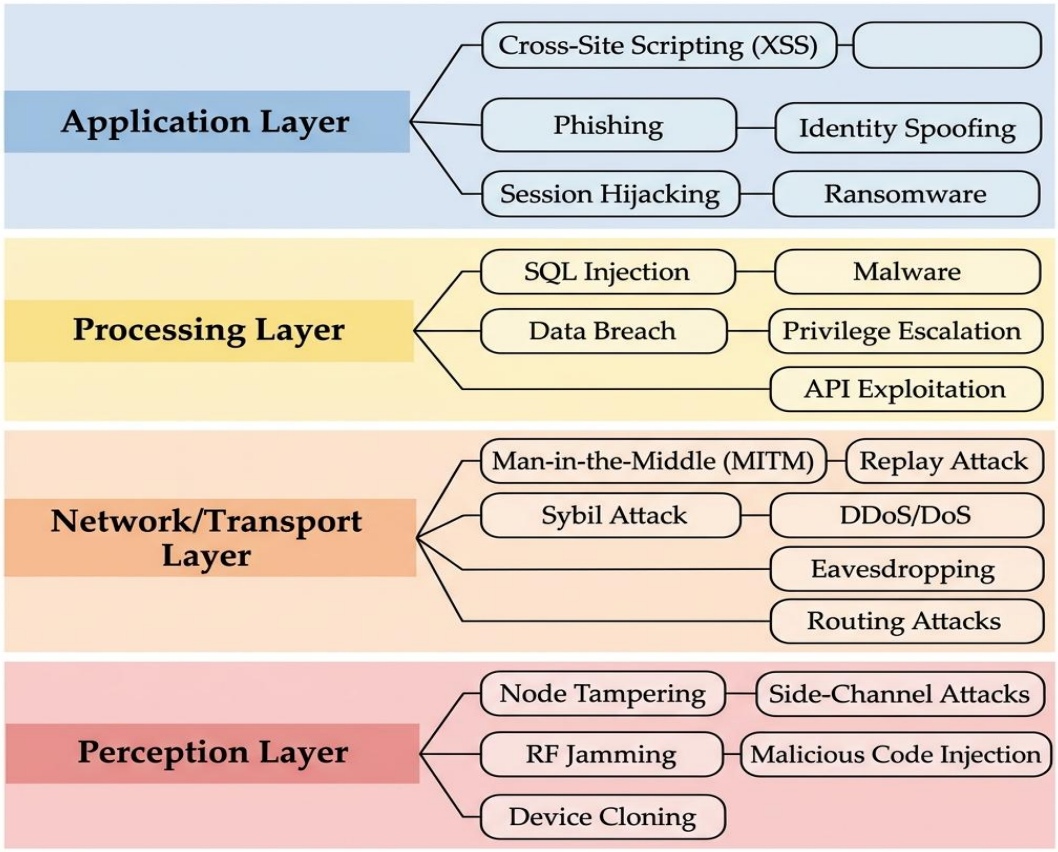

Fig. 2. Comprehensive attack taxonomy across IoT architectural layers.

Most existing IoT applications rely on centralized servers to remotely communicate with and control connected devices. However, the urgency to rapidly launch these applications often results in overlooked security concerns, particularly at hardware and firmware levels. Many IoT devices are not updated regularly, leaving systems increasingly vulnerable over time [25]. Additionally, the lack of standardized security practices across device manufacturers exacerbates the problem, as each vendor implements proprietary and often inadequate security measures. Conventional security measures, such as traditional encryption, static authentication, and perimeter-based access control, are increasingly inadequate in large-scale IoT environments, where emerging technologies introduce new attack methods capable of bypassing traditional defenses [26, 27].

The proliferation of botnets targeting IoT devices has become particularly concerning. The Mirai botnet and its variants demonstrated how compromised IoT devices could be weaponized for large-scale DDoS attacks, disrupting critical internet infrastructure. More recent botnet variants have evolved to target specific IoT protocols and device types, employing sophisticated propagation techniques that evade traditional detection methods [74, 75]. This evolving threat space highlights the need for intelligent, adaptive security solutions that can keep pace with the sophistication and scale of modern attacks.

For the purposes of this survey, we adopt a general threat model consistent with the literature [119, 149]. We consider three classes of adversaries: (i) external attackers who have no legitimate access to the network and attempt to compromise IoT devices through remote exploitation, protocol-level attacks, or botnet recruitment; (ii) insider adversaries who have legitimate access to some network resources and may attempt privilege escalation, data exfiltration, or model poisoning in federated learning scenarios; and (iii) man-in-the-middle adversaries who intercept communication channels to perform eavesdropping, replay, or message modification attacks. Adversary capabilities range from passive observation (traffic analysis, fingerprinting) to active manipulation (device spoofing, firmware tampering, adversarial ML attacks). The trust boundary is defined at the device-edge interface, where authentication and access control mechanisms must verify device identity and data integrity before granting access to edge or cloud resources.

C. IoT Security: Key Requirements and Considerations

Successful security strategies must address six essential attributes, illustrated in Fig. 3, that form the foundation upon which all security mechanisms are designed and evaluated [23]:

Fig. 3. Six key IoT security requirements forming the evaluation foundation.

• Confidentiality: Private and sensitive information must not be exposed or inferred by unauthorized individuals. This is particularly critical in IoT healthcare and smart home applications where personal data flows continuously through device networks [27].

• Integrity: Information should remain unchanged and intact, particularly when transmitted over unsecured or public networks. Blockchain technology directly addresses this requirement through its immutable ledger structure [28].

• Authentication: Data transmission and processing should be verifiable according to established standards. Both device-to-device and user-to-device authentication must be supported, with lightweight protocols for constrained environments [29].

• Authorization: Access to the IoT system and its data must be restricted to authorized users and devices only. Role-based and attribute-based access control mechanisms, potentially enforced through smart contracts, are essential [30].

• Availability: IoT services must be accessible to all authorized users at all times, with system configurations prioritizing resilience against denial-of-service attacks [31].

• Non-repudiation: Ensures users and devices can access records that serve as proof of actions taken, preventing denial of transactions. Blockchain's immutable audit trail provides inherent non-repudiation [32].

These six requirements form the evaluation criteria against which all reviewed authentication architectures and security frameworks are assessed throughout this survey. The challenge lies in satisfying at the same time all requirements within the severe resource constraints of IoT devices, where trade-offs between security strength and computational overhead are inevitable [62, 63].

D. Blockchain Technology Fundamentals

Originally designed to support cryptocurrency applications, blockchain has evolved into an important technology impacting various industries beyond finance. Acting as a decentralized ledger, it securely and transparently records transactions. Its cryptographic principles and distributed structure provide resilience and protect data integrity from manipulation [33]. On a peer-to-peer network, blockchain acts as an open digital ledger that records timestamped transactions in unalterable blocks. Through encryption and the interconnection of each block with the next via cryptographic hashes, it ensures transparency and integrity without centralized control [34].

Blockchains can be categorized into three types: public blockchains (permissionless, accessible to anyone, e.g., Bitcoin [142], Ethereum [144]), private blockchains (permissioned, restricted to authorized participants), and consortium blockchains (semi-permissioned, governed by a group of organizations). For IoT applications, consortium and private blockchains are generally preferred due to their lower computational overhead and higher throughput while maintaining the core security properties of decentralization and immutability [42, 43, 44].

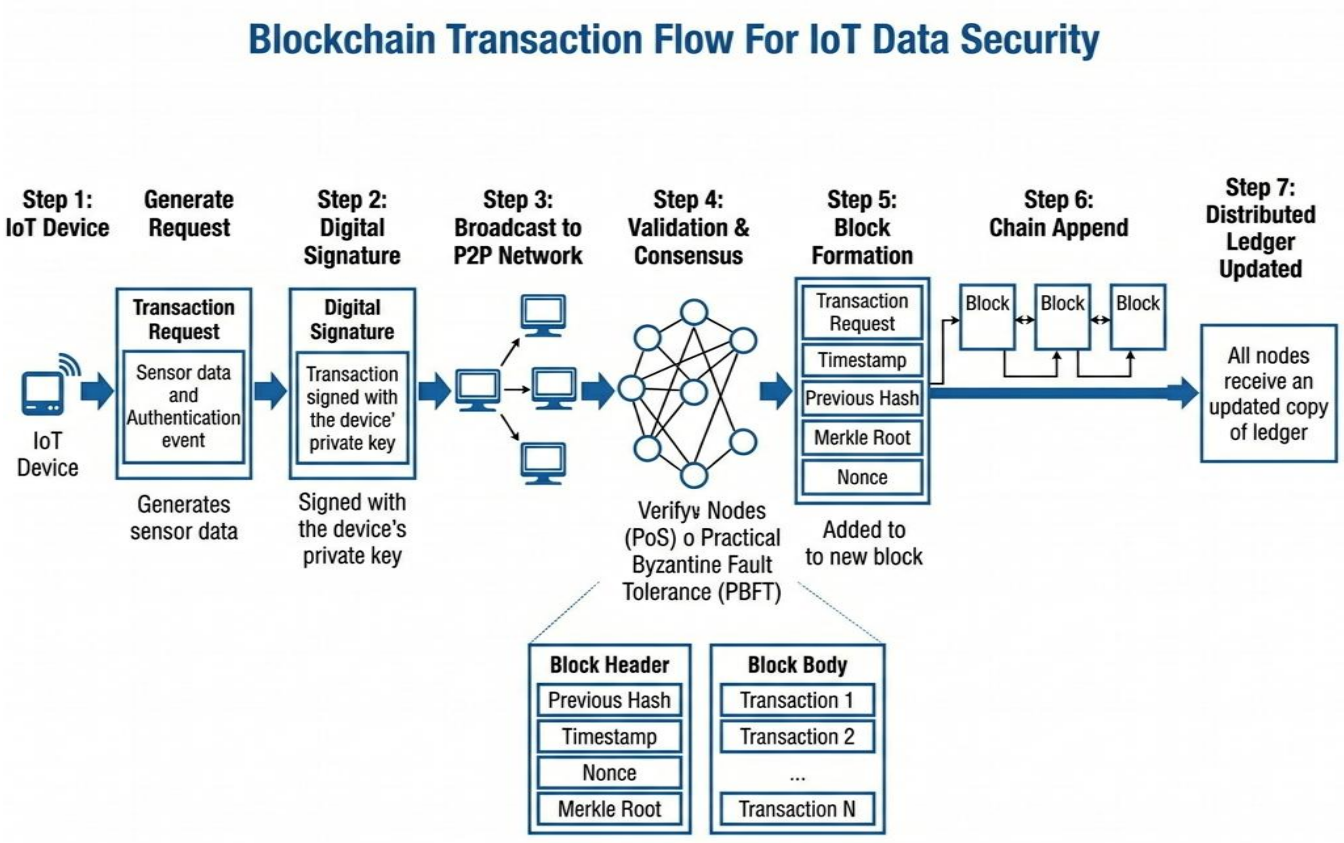

Fig. 4. Blockchain transaction flow for IoT data security, showing the lifecycle from device-generated transactions to immutable ledger storage.

Fig. 5 presents the conceptual integration architecture of blockchain and deep learning for IoT security, illustrating how these complementary technologies jointly address different aspects of the security challenge.

Blockchain provides the trust infrastructure (immutable audit trails, decentralized identity, smart contract enforcement), while deep learning enables adaptive intelligence (pattern recognition, anomaly detection, behavioral analysis). This integration creates a comprehensive security framework that is both trustworthy and adaptive [34, 50].

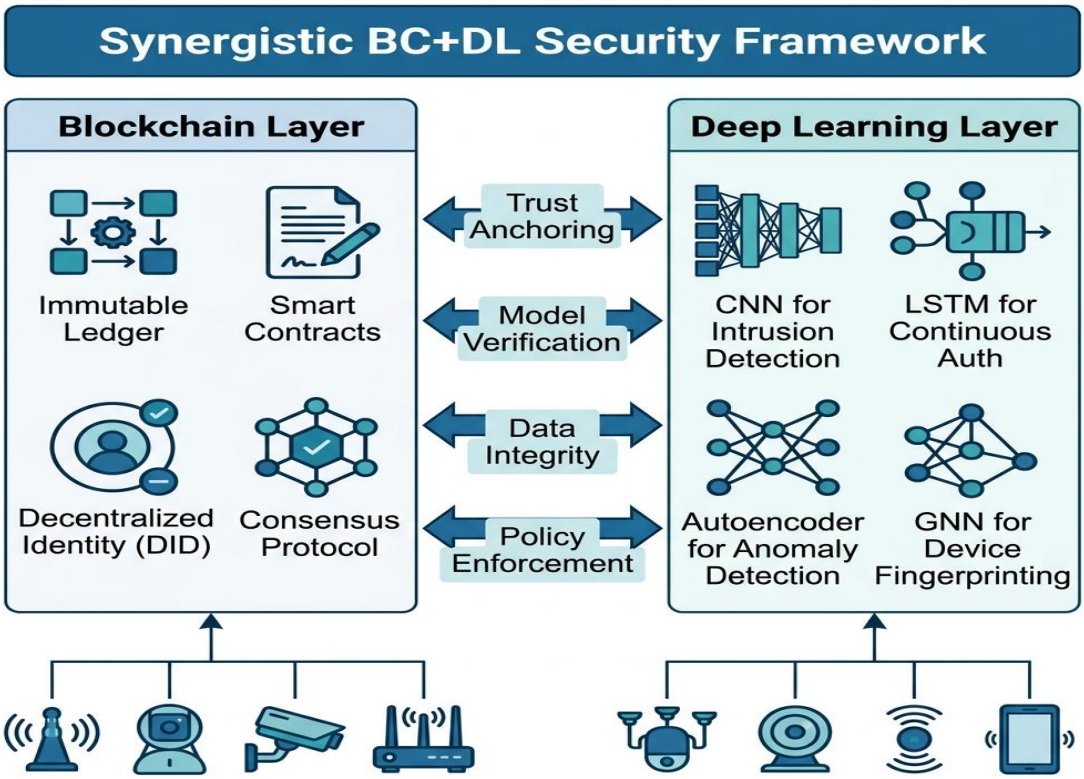

Fig. 5. Blockchain and deep learning integration architecture for IoT security, showing complementary roles and data flow.

Key security features of blockchain for IoT include: (i) Data Integrity and Immutability, ensuring that once recorded, data cannot be altered without network agreement, which is crucial for IoT systems relying on accurate sensor data for decision-making [35]; (ii) Decentralization and Transparency, recording transactions across multiple distributed nodes, thereby reducing dependence on centralized authorities and eliminating single points of failure [36]; (iii) Smart Contracts, self-executing agreements stored on the blockchain that automate security policy enforcement, access control decisions, and compliance verification without human intervention [37, 38, 143]; (iv) Consensus Mechanisms, protocols enabling network participants to agree on transaction validity, with various trade-offs between security, throughput, and energy consumption [39, 40]; (v) Identity Management and Authentication, enabling secure, verifiable identity management through cryptographic key pairs and Decentralized Identifiers (DIDs) [41]; and (vi) Encryption and Privacy, using advanced cryptographic algorithms including zero-knowledge proofs (ZKPs) for selective data exposure while maintaining privacy [41]. Table I compares the major consensus mechanisms and their suitability for IoT deployments.

TABLE I. Comparative Analysis of Blockchain Consensus Mechanisms for IoT

Mechanism	Throughput (TPS)	Latency	Energy Consumption	Fault Tolerance	IoT Suitability
Proof of Work (PoW)	7–15	10–60 min	Very High	50% Byzantine	Very Low – Impractical for constrained devices
Proof of Stake (PoS)	100–1,000	2–15 s	Low	51% stake	Moderate – Reduced energy

					but stake requirements
Delegated PoS (DPoS)	1,000–4,000	0.5–2 s	Low	51% delegates	High – Fast finality, suitable for IoT gateways
PBFT	1,000–3,000	1–5 s	Low	33% Byzantine	High – Deterministic finality, permissioned networks
DAG-based (IOTA)	500–1,500	5–30 s	Very Low	Varies	Very High – Feeless, lightweight for M2M transactions
Proof of Authority (PoA)	1,000+	<1 s	Very Low	Varies	High – Ideal for private IoT consortiums

The convergence of blockchain and IoT is characterized by several key trends [43, 52, 53]. These include the adoption of edge computing for real-time processing, the integration of AI for sophisticated decision-making, the deployment of high-speed 5G networks, and the creation of blockchain-enabled communication frameworks for secure data exchange. Federated blockchains such as R3 Corda provide greater scalability and improved transaction privacy [53, 54]. Ricardian contracts enable legally binding electronic records, while Blockchain as a Service (BaaS) streamlines application management [53, 55]. Emerging hybrid blockchain architectures deliver increased security and flexibility by combining the openness of public chains with the performance of private chains [53, 54, 55].

When integrated into IoT systems, blockchain's decentralized architecture offers numerous security advantages: ensuring data integrity through immutable ledgers [2, 48]; secure device identification and authentication through digital certificates and DIDs [14, 48, 58]; decentralized access control that removes single points of failure [2, 14, 48]; supply chain integrity through tamper-proof audit trails [2, 45, 47, 48]; secure over-the-air (OTA) firmware updates through cryptographic authentication [2, 14]; distributed threat intelligence sharing across organizational boundaries [2, 14, 48]; privacy-preserving data sharing through zero-knowledge proofs [2, 14, 48]; and automated security policy enforcement via smart contracts [2, 46, 48]. Blockchain also underpins emerging IoT applications in wireless sensor networks [150], where its immutable ledger provides provenance tracking for sensor data. However, significant challenges remain, particularly regarding the computational and storage requirements of blockchain for resource-constrained IoT environments [49, 63].

E. Deep Learning Fundamentals for IoT Security

As data volume grows, feature selection becomes essential to reduce both dataset size and training complexity. While traditional machine learning methods can achieve high accuracy with well-prepared datasets, deep learning automatically extracts hierarchical features through optimization algorithms, making it highly effective for large-scale, high-dimensional datasets [68]. Deep Learning (DL) models are a subset of machine learning algorithms that utilize artificial neural networks with multiple hidden layers to automatically learn representations from data without manual feature engineering. This capability is particularly valuable for IoT security, where the volume and velocity of network traffic data make manual feature extraction impractical.

Fig. 6 illustrates four key deep learning architectures that have demonstrated particular effectiveness for IoT security applications [68, 69, 70].

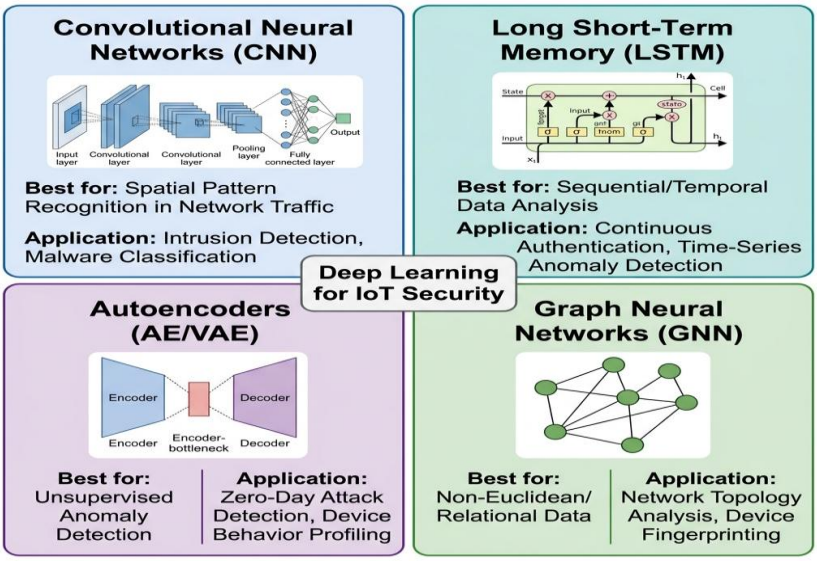

Fig. 6. Four key deep learning methods applied in IoT security: CNN, LSTM, Autoencoder, and GNN.

Convolutional Neural Networks (CNNs) are effective for spatial data processing and widely used in intrusion detection and malware classification. Their ability to extract local features through convolution filters makes them particularly suitable for analyzing fixed-size network packet representations [69]. Long Short-Term Memory (LSTM) networks and Gated Recurrent Units (GRU) handle sequential data through specialized gating mechanisms, making them suitable for time-series analysis, continuous authentication, and anomaly detection in temporal IoT data streams [69, 70]. Autoencoders and Variational Autoencoders (VAEs) excel in unsupervised anomaly detection by learning compact representations of normal behavior and flagging deviations that may indicate security breaches; their unsupervised nature is particularly valuable given the scarcity of labeled attack data in IoT environments [73]. Graph Neural Networks (GNNs) extend deep learning to non-Euclidean data structures, enabling device relationship modeling and network topology analysis, essential capabilities for understanding the complex interconnection patterns in large-scale IoT deployments [70].

In the context of IoT security, these DL architectures are applied across multiple domains. For anomaly detection, models learn normal operational patterns and identify deviations indicating faults or malicious activity. For intrusion detection, CNNs and GRUs analyze network traffic to detect complex attack patterns in real-time, achieving detection rates exceeding 95% on benchmark datasets [69, 70]. For continuous authentication, DL models verify identities through behavioral biometrics including typing behavior, touch dynamics, gait analysis, voice patterns, and energy usage profiles [71]. Device fingerprinting uses DL to identify devices based on unique hardware characteristics including RF emissions, signal strength variations, and packet timing [72]. Table II provides a comparative analysis of these models.

TABLE II. Comparative Analysis of Deep Learning Models for IoT Security Applications

DL Model	Primary Use Case	Accuracy Range	Computational Cost	Edge Deployable	Key Strength
CNN	Intrusion Detection	92–98%	Medium–High	Via MobileNet/pruning	Spatial pattern recognition in packets
LSTM	Continuous Auth.	89–96%	Medium	With quantization/pruning	Temporal sequence modeling
GRU	Anomaly Detection	88–95%	Medium	Yes	Faster training than LSTM, fewer params
Autoencoder	Zero-day Detection	85–93%	Low–Medium	Yes	Unsupervised, no labeled data needed

VAE	Device Profiling	86–94%	Medium	Partial	Generative anomaly scoring
GNN	Device Fingerprinting	90–97%	High	Via split learning	Graph-structured IoT topology analysis
Transformer	Traffic Classification	93–98%	Very High	Via knowledge distillation	Long-range dependency modeling

A critical challenge in deploying DL models for IoT security is the fundamental tension between model complexity and the resource constraints of IoT devices. Model compression techniques, including quantization, pruning, knowledge distillation, and neural architecture search, are essential for making these models practical for edge deployment [80, 81]. The emerging TinyML approach specifically addresses this challenge by developing models that can run within sub-256KB memory footprints, enabling on-device inference at the perception layer [101].

3. Related Work and Literature Review

This section provides a comprehensive review of existing literature on the integration of blockchain and deep learning for IoT security. We organize the reviewed works according to our proposed taxonomy (Fig. 7) and identify key research gaps that motivate this survey. The taxonomy classifies approaches into four primary categories: blockchain-driven authentication, deep learning for intrusion defense, hybrid BC+DL integration, and protocol-level security.

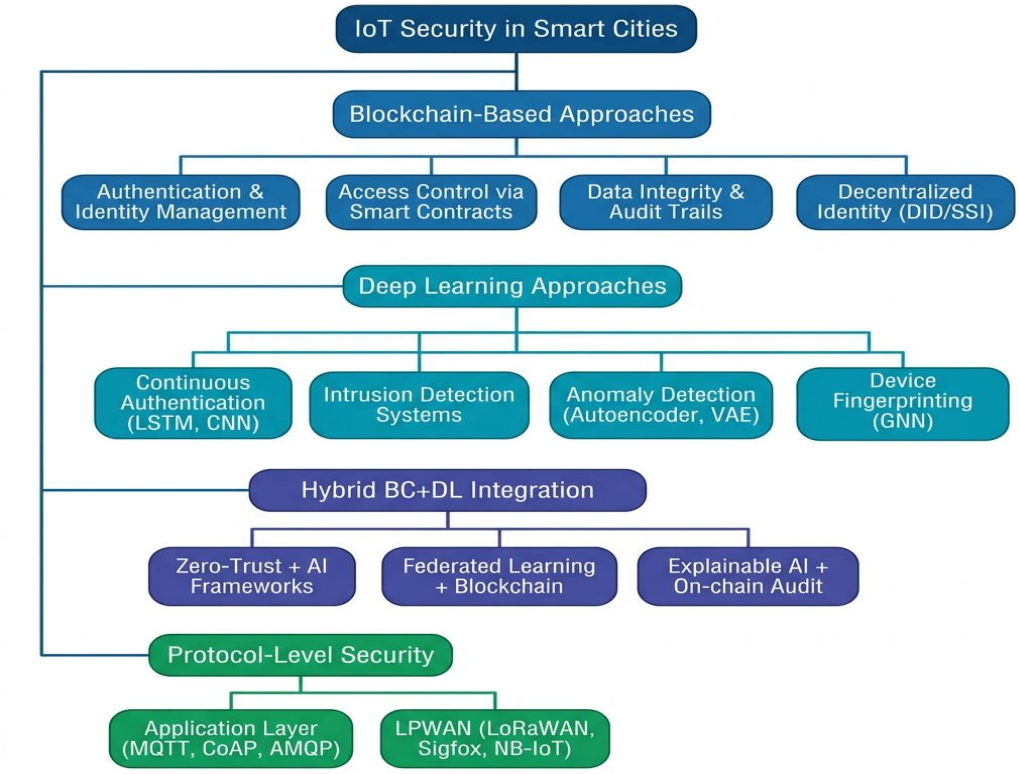

Fig. 7. Proposed taxonomy of IoT security approaches reviewed in this survey.

A. Blockchain-Driven Authentication for IoT and Smart Cities

Recent studies strongly advocate for decentralized architectures to achieve auditable trust and authentication at a smart city scale. Kumar et al. [89] integrated a blockchain-based Authentication and Key Agreement (AKA) mechanism with explainable AI (XAI) to secure consumer IoT devices. Their design highlights how on-chain evidence can complement model decisions and improve the accountability of access control, addressing the critical challenge

of trust transparency in automated security systems. The framework was evaluated on a testbed of 50 IoT devices and demonstrated a 40% reduction in false positive alerts compared to traditional approaches.

Islam et al. [88] proposed a decentralized trust framework that combines blockchain with AI-driven threat detection and a lightweight adaptive Proof-of-Stake (PoS) consensus mechanism. Their approach ensures authentication remains scalable in dense urban deployments by dynamically adjusting consensus parameters based on network load. The framework achieved consensus latency below 3 seconds for networks of up to 1,000 nodes, making it suitable for medium-scale smart city deployments.

In addition, recent work has specifically addressed security at the network edge and in complex data flows. Iftikhar et al. [90] designed a blockchain-assisted, proximity-aware authentication technique for edge networks that reduces latency by using tamper-resistant on-chain logs and geographic proximity verification. Their approach is particularly relevant for multi-operator smart city environments where devices from different administrative domains must establish trust. Pannyagol et al. [91] introduced the DPro_Auth protocol to provide end-to-end authentication and confidentiality for data flows in multi-tenant environments, demonstrating resilience against replay and impersonation attacks through formal verification using ProVerif [128].

Synthesizing these trends, the comprehensive survey by Enaya et al. [92] confirmed that security and data-sharing are the dominant catalysts for integrating blockchain into smart city platforms, while highlighting significant scalability limitations, latency, and energy overheads that complicate deployment on resource-constrained IoT nodes. The authors stress that overcoming these barriers necessitates lightweight cryptography and hierarchical designs distributing workloads across edge, fog, and blockchain layers. This observation is corroborated by Khashan [110], who proposed a trust-based fog-blockchain model specifically designed for scalable authentication in smart cities, offloading authentication processing to fog nodes to reduce blockchain consensus overhead by approximately 60%.

Privacy-preserving cryptographic schemes have gained significant attention. Zero-knowledge proofs (ZKPs) allow devices to authenticate and prove attributes without exposing sensitive data, though most implementations remain at proof-of-concept stage due to computational overhead [111, 112]. Decentralized Identifiers (DIDs) represent another promising direction: Yang et al. [145] proposed BDIDA-IoT, a blockchain-based decentralized identity architecture that eliminates dependency on centralized certificate authorities; Ramirez et al. [146] demonstrated IOTA-based DID management for constrained IoT devices; and Zhang et al. [147] developed a trusted data collection system using DID attestation for smart city telemetry provenance.

B. Deep Learning for Continuous Authentication and Intrusion Defense

The application of deep learning has evolved to provide multi-layered continuous security monitoring across diverse IoT environments. Sahu et al. [93] utilized LSTM networks to model behavioral sequences for continuous user authentication in IoT-enabled healthcare systems. Their approach achieved 94.2% accuracy on continuous authentication tasks, establishing methods later repurposed for creating device-specific behavioral baselines that can detect account takeover attacks within seconds of occurrence.

Hazman et al. [94] developed a DL-based intrusion detection system specifically engineered for IoT connectivity standards, achieving improved detection of protocol-specific attacks in smart city scenarios. Their system demonstrated particular effectiveness against MQTT-specific attacks, achieving a 97.3% detection rate with less than 2% false positive rate. At the system level, Dritsas and Trigka [95] conducted a comprehensive survey finding that in blockchain-IoT ecosystems, machine learning is primarily used to enhance security by intelligently prioritizing alerts and improving efficiency by pre-filtering data before commitment to the distributed ledger, thereby reducing blockchain storage requirements by up to 70%.

Behavioral biometrics [71] enables continuous authentication based on interaction patterns such as typing behavior, touch dynamics, gait analysis, voice patterns, and energy usage profiles. DL models, particularly CNNs and RNNs, learn subtle user-specific patterns for real-time continuous authentication without requiring explicit user input. Device fingerprinting [72] uses DL to identify devices based on unique hardware characteristics including RF emissions, signal strength variations, packet timing, and MAC-layer features, enabling passive device authentication. Anomaly detection [73] using LSTM networks, GRUs, and VAEs models temporal dependencies to detect subtle deviations that may indicate zero-day attacks, botnets, and advanced persistent threats, attacks for which no signature exists in traditional IDS databases.

The CNN-GRU hybrid architecture proposed by Sagu et al. [139] represents a significant advance in IoT threat detection, combining CNN's spatial feature extraction with GRU's temporal modeling to achieve leading performance

on the Bot-IoT and TON_IoT datasets. Chinnasamy et al. [70] further enhanced this approach by incorporating Graph Neural Networks (GNNs) to capture device relationship patterns, enabling contextual intrusion detection that considers network topology. Alsubaei et al. [152] provided a comprehensive taxonomy of DL-based cybersecurity threat detection methods specifically tailored for IoT devices, identifying CNN-LSTM hybrids and attention mechanisms as the most promising architectures for resource-constrained deployment.

C. Convergence of Blockchain and Learning: Zero-Trust and Federated Learning at the Edge

A significant development in the 2023–2025 period is the integration of blockchain and machine learning to enforce a zero-trust security posture. Salim et al. [96] proposed a framework for smart cities using a blockchain-enabled architecture where Deep Reinforcement Learning (DRL) dynamically adjusts access policies and authenticates devices through adaptive gateways. This design directly addresses the need for security that adapts to the fluid trust boundaries between municipal departments, utility providers, and public services. The framework demonstrated a 35% improvement in policy adaptation speed compared to static rule-based approaches.

Concurrently, Federated Learning (FL) has emerged as a cornerstone for privacy-preserving analytics in distributed IoT environments. The comprehensive survey by Al-Huthaifi et al. [97] established that FL can train effective security models while keeping raw data on-device, satisfying GDPR and CCPA privacy requirements. Banabilah et al. [98] provided foundational analysis of FL techniques applicable to smart city scenarios, while Qasmaoui et al. [99] specifically examined FL deployment challenges in urban IoT contexts. Subsequent research [100, 101] focused on making FL feasible for city-scale IoT by optimizing client selection algorithms, model compression techniques, and personalization strategies for heterogeneous device populations.

Ragab et al. [102] demonstrated that advanced AI combined with FL can strengthen cyber-resilience without data centralization, achieving detection rates comparable to centralized approaches while preserving data locality. The coupling of blockchain with FL, commonly termed BlockFL, uses blockchain to provide robust defense against model poisoning and Sybil attacks by authenticating participants and immutably tracking model update provenance [111, 112]. Sharma et al. [133] extended this approach to Industry 5.0 contexts by combining blockchain-based zero-trust networks with federated transfer learning, enabling knowledge transfer across organizational boundaries while maintaining data sovereignty.

Devi et al. [134] developed FL-enabled lightweight IDS specifically designed for wireless sensor networks in smart city environments, demonstrating that federated approaches can achieve detection accuracy within 3% of centralized models while reducing communication overhead by 80%. Gigli et al. [135] introduced zero-trust oracle networks that secure IoT data integrity through blockchain-verified data feeds, providing a foundation for trustworthy smart contract execution based on real-world IoT sensor data. Despite these advances, the scalability of BlockFL for large-scale smart city applications remains challenged by high communication overhead, consensus latency, and the heterogeneity of participating devices [82].

D. Communication Protocols: Security and Performance Implications

Authentication mechanisms are implemented atop application-layer and LPWAN protocols, meaning their underlying behavior directly dictates security and performance characteristics. Tran et al. [103] provided a critical comparison of MQTT, CoAP, AMQP, and HTTP messaging protocols, demonstrating how transport choices and Quality of Service (QoS) levels directly impact reliability and latency, factors critical for efficient authentication handshakes. Their analysis revealed that MQTT with QoS 1 offers the optimal balance between reliability and overhead for IoT authentication scenarios.

Gentile et al. [104] performed granular analysis of MQTT networks, quantifying the throughput and latency overhead introduced by various security features including TLS 1.2, TLS 1.3, and username/password authentication. Their findings concluded that lightweight cryptography and session resumption mechanisms are essential for scalable deployments, and that TLS 1.3 reduces handshake latency by approximately 33% compared to TLS 1.2. Gavriilidis et al. [148] provided complementary empirical evaluation of TLS-enhanced MQTT on constrained IoT devices, quantifying the memory and computational overhead across different device classes.

At the LPWAN tier, security challenges are particularly acute due to limited bandwidth and processing capabilities. For LoRaWAN [105, 106], recent analyses systematically enumerate persistent weaknesses in key management, session handling, and resilience against replay and DoS attacks. These vulnerabilities necessitate architectural mitigations such as join-server hardening, device pre-provisioning, or using blockchain side-channels to anchor device identity [131]. Piechowiak et al. [132] demonstrated ML-guided coverage planning for LoRaWAN

smart metering systems, highlighting the intersection of network optimization and security considerations. Broader IoT security syntheses [107] offer comprehensive catalogs of protocol-specific vulnerabilities across the entire communication stack (MQTT, CoAP, Zigbee, LoRaWAN, Bluetooth LE), providing essential checklists for security designers.

E. Integrated Smart-City Platforms and Security Models

A comprehensive analysis of commercial and open-source IoT platforms reveals a significant gap between standard and emerging security practices. As Monios et al. [113] demonstrate in their thorough review, while mainstream platforms universally support foundational protocols like MQTT/CoAP and TLS-based authentication, their native integration with blockchain or ML-based identity management remains exceptionally rare. This gap creates opportunities for middleware solutions that bridge existing platforms with advanced security capabilities.

Alotaibe [114] explicitly positions robust authentication as the core enabler underpinning all other security functions in IoT systems, arguing that without reliable device and user authentication, all subsequent security measures (encryption, access control, audit logging) are effectively compromised. Alotaibi et al. [115] categorize modern authentication methods into blockchain-based, biometric, and deep learning approaches, finding that most solutions suffer from a critical lack of comprehensive lifecycle management, including credential provisioning, rotation, revocation, and recovery, which limits their practical deployment. Albugmi [153] proposed a hybrid smart IoT detection and prevention framework for smart cities that implements a six-stage end-to-end security stack combining blockchain contracts, DL analytics, and automated alert generation.

Tagliaro et al. [151] conducted vulnerability analysis of smart city backend infrastructure, revealing that many deployed systems expose unprotected MQTT brokers, CoAP endpoints, and REST APIs to the public internet. Their findings underscore the urgent need for the authentication and access control mechanisms reviewed in this survey. Rai et al. [136] provided a blockchain-based approach for securing IoT networks addressing issues across energy management, healthcare, and smart city domains, while Al-Matari et al. [137] conducted a systematic literature review of blockchain applications in healthcare, supply chains, and smart cities, identifying common security patterns and challenges across these verticals.

F. Comparative Surveys and Emerging Trends

Recent surveys have consolidated the IoT authentication space by classifying schemes based on cryptographic primitives, trust models, and deployment constraints. Alsheavi et al. [108] mapped the broader ecosystem, outlining trends including lightweight post-quantum cryptography, formal verification of protocols, and standards-driven approaches. A focused 2024 study by Dargaoui et al. [109] compared recent authentication protocols (2019–2023), highlighting critical gaps in scalability under device mobility and resistance to desynchronization attacks that can permanently lock out legitimate devices.

Future authentication frameworks must evolve to meet challenges posed by 6G and AI-native networking [116, 117], necessitating slice-aware authentication, ultra-low latency re-authentication (sub-millisecond), and seamless integration of AI-driven trust fabrics that can operate across network slices with different security requirements. The convergence of zero-trust principles with 6G network architecture represents a particularly promising direction for future research [160].

Ahsan et al. [138] provided a systematic review of blockchain-secured IoT systems mapped to the NIST cybersecurity framework, categorizing approaches by Identify, Protect, Detect, Respond, and Recover functions. Wang et al. [121] explored ECC-based blockchain identity solutions for constrained IoT devices. Over the past three years, research has solidified blockchain's role as a foundational structural layer for decentralized identity and immutable audit trails in urban IoT systems. Critical research gaps remain: lack of realistic benchmarking environments, resilient FL defenses for intermittent connectivity, comparative trust cost models between blockchain and hardware attestation (DICE, TPMs), and unified credential lifecycle management across heterogeneous protocols [108, 109, 176, 177].

4. Comparative Analysis

This section presents the core comparative analysis of our survey, systematically evaluating reviewed studies across authentication architectures, communication protocol security, blockchain integration patterns, deep learning models, and benchmark datasets. The analysis, synthesized from over forty studies, is structured around our proposed taxonomy and evaluation framework, with results presented through comprehensive tables and multi-dimensional visualizations.

A. Authentication Architecture Comparison

The comparative analysis reveals three dominant approaches in IoT authentication for smart cities: (i) blockchain-only authentication using Decentralized Identifiers (DIDs), smart contracts, and lightweight consensus for tamper-proof identity management; (ii) DL-enhanced continuous authentication using behavioral biometrics, device fingerprinting, and anomaly detection models that adapt to evolving threat patterns; and (iii) hybrid BC+DL frameworks that jointly combine decentralized trust infrastructure with adaptive intelligence for comprehensive security coverage.

Table III presents a comprehensive comparison of 33 key reviewed studies across seven evaluation dimensions. Several important patterns emerge from this analysis. First, blockchain-driven authentication architectures are increasingly adopting lightweight ECC-based cryptography and DID models designed specifically for resource-constrained environments, moving away from heavyweight certificate-based approaches [122, 123]. Second, deep learning models are transitioning from centralized training approaches to federated and split learning approaches that respect data privacy requirements [133, 134]. Third, hybrid frameworks that combine blockchain's immutable trust foundation with DL's adaptive intelligence consistently demonstrate superior performance across our evaluation criteria compared to single-technology approaches [96, 153]. Among the 33 reviewed studies, 11 (33%) employ blockchain-only mechanisms, 9 (27%) rely on DL-only approaches, and 13 (40%) adopt hybrid BC+DL frameworks, confirming that the field is moving decisively toward integrated solutions.

TABLE III. Comprehensive Comparative Analysis of Reviewed Studies (2023–2025)

Author	Scope	Auth Design	BC Role	DL/FL Role	Protocol	Key Findings / Limitations
Kumar [89]	Consumer IoT	AKA + XAI	On-chain evidence	Explainable AI	Agnostic	BC+XAI accountability; limited scale testing
Islam [88]	Smart-city trust	Role-based auth	Decentralized trust	Threat detection	V2I/IoT	Cross-domain trust; PoS consensus overhead
Iftikhar [90]	Edge networks	Consortium-chain	Identity+session	—	Edge-centric	Multi-operator cities; governance complexity
Pannyagol [91]	BC-IoT auth	DPro_Auth	Auth evidence	—	6G Het.	Strong confidentiality; ledger overhead
Enaya [92]	IoT smart cities	Survey	Integrity/sharing	—	Mixed	Wide BC-IoT survey; scalability/governance flags
Salim [96]	City-scale IoT	Zero-Trust+BC	Policy/attestation	DRL	Edge-cloud	ZT at scale; policy latency tuning needed
Wang [121]	Constrained IoT	ECC identity	DID+on-chain	—	Agnostic	ECC-enabled BC identity for devices
Khalique [122]	Sustainable cities	Lightweight ECC	—	—	Constrained	Low-compute auth; needs lifecycle mgmt
Khoury [123]	Constrained IoT	Cert-based CoAP	Light cert anchor	—	CoAP/DTLS	Reduces X.509 overhead significantly
Hsu [124, 125]	MQTT telemetry	Service agent	Msg verification	—	MQTT	BC+MQTT fusion for verifiable pub/sub
Alotaibi [126]	IoT networks	—	—	Distributed ML	MQTT	Distributed ML hardens MQTT deployments

Bangare [127]	IoT general	—	Merkle integrity	—	MQTT	Lightweight MQTT hardening via Merkle trees
Li [128]	Anonymous AKA	ECC-based AKA	—	—	Agnostic	ProVerif-verified; DAC-synchronized AKA
Prazeres [129]	Smart-city IDS	—	—	ML pipeline	Agnostic	Supervised ML-IDS for city IoT deployments
Alsulami [130]	IoT IDS	—	—	ML-IDS	MQTT/CoAP/HTTP	Protocol-aware multi-protocol IDS
Stanco [131]	LPWAN security	Survey	—	—	LPWAN	Comprehensive LPWAN security survey
Piechowiak [132]	Smart metering	—	—	ML coverage	LoRaWAN	ML-guided LoRaWAN coverage planning
Sharma [133]	Industry 5.0	ZTN principles	Model updates	Fed. transfer	Agnostic	BC+federated TL for distributed IoT learning
Devi [134]	WSN cities	—	—	Federated IDS	WSN/IoT	FL lightweight IDS for smart city WSNs
Gigli [135]	Oracle networks	—	Oracle on-chain	—	Agnostic	Zero-trust oracle for IoT data integrity
Rai [136]	Energy/city	Access+privacy	Audit/sharing	—	Agnostic	Cross-domain BC-IoT security framework
Dritsas [95]	Cross-domain	Varies (survey)	Integrity/privacy	ML across layers	Mixed	ML+BC enablers; integration complexity noted
Al-Matari [137]	Supply/health	Varies	Provenance/audit	—	Agnostic	Scalability/energy/privacy gaps identified
Ahsan [138]	IoT general	Access control	Policy+audit	—	Agnostic	NIST-mapped ABAC/capability trends
Sagu [139]	IoT threats	CNN-GRU IDS	—	Deep classifier	Agnostic	Detection boost; concept drift handling needed
Far [140]	DRL+BC cities	Adaptive DRL	Exchange/incentives	DRL routing	Cellular	Efficiency gains; training cost trade-offs
Yang [145]	City data bus	DID-based	On-chain creds	—	Agnostic	DID speeds secure data flow
Ramirez [146]	Constrained IoT	Device identity	IOTA-based DID	—	Agnostic	Decentralized identity via IOTA DAG
Zhang [147]	Trusted collection	DID attestation	Telemetry provenance	—	Agnostic	Tamper-evident smart city data collection
Gavriilidis [148]	City telemetry	TLS auth	—	—	MQTT/TLS	Quantifies TLS overhead on constrained devices

Tagliaro [151]	City backends	—	—	—	MQTT/CoAP	Vulnerable backends identified in production
Alsubaei [152]	IoT threats	—	—	DL taxonomy	Agnostic	DL taxonomy for post-authentication detection
Albugmi [153]	Hybrid BC-IoT	Policy+auth	Contracts+alerts	Analytics loop	Agnostic	Six-stage end-to-end city security stack

The comparative analysis indicates that blockchain-driven authentication and decentralized identity frameworks are maturing, marked by adoption of lightweight cryptography and DID models designed for resource-constrained devices. Deep learning effectively complements these mechanisms by facilitating dynamic trust assessment, intrusion detection, and large-scale anomaly monitoring. At the protocol level, MQTT with TLS 1.3 and CoAP with DTLS 1.3 / OSCORE are emerging as de facto standards; however, scalability and latency under high device density present persistent challenges that require architectural solutions [141, 142, 143].

B. Communication Protocol Security Comparison

Securing IoT ecosystems critically depends on robust communication tailored for resource-constrained devices and lossy networks. The period from 2023 to 2025 has witnessed significant maturation in the IoT security standards space, with several key developments: constrained OAuth 2.0 (ACE) [162] providing lightweight authorization for IoT; Object Security for Constrained RESTful Environments (OSCORE) [162] enabling end-to-end application-layer security independent of transport; Ephemeral Diffie-Hellman Over COSE (EDHOC) [163] reducing key establishment overhead by 90% compared to DTLS handshakes; Remote Attestation Procedures (RATS/EAT) [164, 165] enabling cryptographic device health verification; FIDO Device Onboard (FDO) [166] automating secure device provisioning; and vertical-specific standards such as Matter 1.4 [167], Wi-SUN FAN [168], and LwM2M [169] for domain-specific deployments.

Fig. 8 illustrates the comparative protocol stacks and their security mechanisms, providing a visual overview of how different protocols layer security features at the transport and application levels.

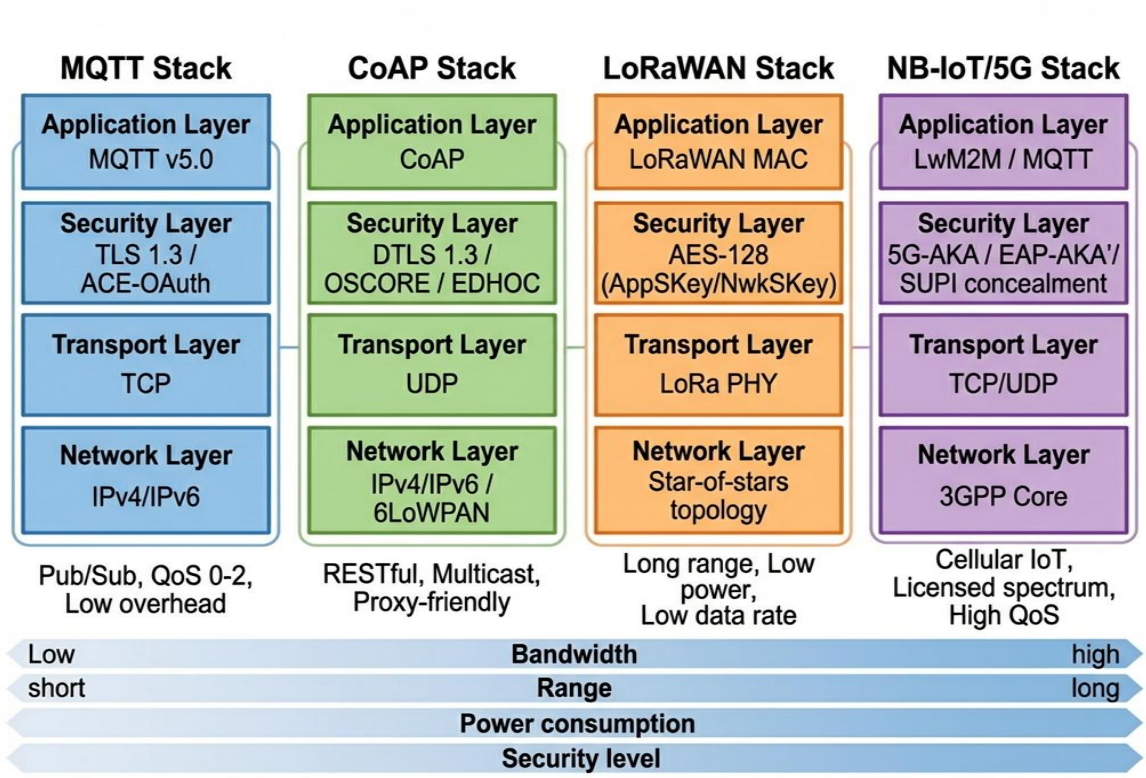

Fig. 8. Comparative IoT communication protocol stacks and their associated security mechanisms.

TABLE IV. Communication Protocol Security Comparison Matrix

Protocol	Transport	Auth Method	Encryption	Overhead	Latency	BC Compatible
MQTT v5+TLS 1.3	TCP	ACE-OAuth, X.509	TLS 1.3	Medium	Low	Yes (token binding)
CoAP+OSCORE	UDP	EDHOC+OSCORE	COSE/AES-CCM	Very Low	Very Low	Yes (via EAT)
CoAP+DTLS 1.3	UDP	PSK/certificate	DTLS 1.3	Low	Low	Yes
LoRaWAN 1.1	LoRa PHY	AES-128 (AppSKey/NwkSKey)	AES-128 CTR	Very Low	High	Limited (off-chain)
NB-IoT (5G)	3GPP Core	5G-AKA / EAP-AKA'	SUPI concealment	Medium	Low–Med	Via gateway
AMQP 1.0	TCP	SASL / TLS	TLS 1.2–1.3	High	Low	Yes
Matter 1.4	Thread/WiFi	SPAKE2+ / CASE	AES-CCM-128	Low	Low	Via DCL
HTTP/3 (QUIC)	UDP/QUIC	TLS 1.3 built-in	TLS 1.3	Medium	Very Low	Yes

Key findings from the protocol analysis include: (1) application-layer security (OSCORE) is often better suited than transport-layer security (DTLS) for multi-hop, proxy-rich IoT networks because it preserves end-to-end security through intermediaries; (2) EDHOC [163] significantly reduces key establishment overhead compared to DTLS, requiring only 3 messages totaling approximately 200 bytes versus DTLS's 6+ messages exceeding 2KB, making it viable for Class-0 devices; (3) post-quantum cryptography preparedness is advancing with NIST's ML-KEM [171], ML-DSA [172], and SLH-DSA [173] standards, though their integration into constrained IoT devices remains a significant engineering challenge; (4) cellular IoT security continues maturing through 3GPP TS 33.501 [170] with refinements to 5G-AKA and SUPI concealment; and (5) credential lifecycle management, including provisioning, rotation, revocation, and recovery, remains a significant open challenge across all protocol families [176, 177].

C. Benchmark Dataset Evaluation

Robust and representative datasets are a critical prerequisite for rigorous evaluation of IoT security frameworks. The quality and diversity of evaluation datasets directly impacts the validity of reported results and the generalizability of proposed solutions. Table V presents an extended comparative analysis of eight widely adopted benchmark datasets, evaluating them across device diversity, feature richness, attack coverage, duration, scale, generation methodology, and benchmark performance metrics.

TABLE V. Extended Comparative Analysis of IoT Security Benchmark Datasets

Dataset	Devices	Features	Attack Types	Duration	Samples	Method	F1-Max	AUC-Max
Bot-IoT [74]	6	46	4 categories	9 days	72M	Synthetic	0.98	0.99
TON_IoT [75]	9	43	9 categories	3 weeks	22M	Hybrid	0.95	0.97
Edge-IIoTset [76]	25	61	13 categories	2 months	22M	Physical testbed	0.91	0.94
IoT-23 [77]	3	25	7 categories	20 hours	23M	Malware capture	0.89	0.92
CICIDS2017 [154]	N/A	80	14 categories	5 days	2.8M	Synthetic	0.97	0.98
UNSW-NB15 [155]	N/A	49	9 categories	16 hours	2.5M	Hybrid	0.93	0.96

N-BaIoT [157]	9	115	2 categories	Continuous	65M	Real malware	0.96	0.98
MedBIoT [156]	3	100	3 categories	Continuous	17M	Medical IoT	0.94	0.96

Among synthetic benchmarks, Bot-IoT [74] stands out for its exceptional scale (72M+ samples) and high benchmark performance (F1: 0.98, AUC: 0.99), making it ideal for evaluating scalable detection models. TON_IoT [75] employs a hybrid methodology combining simulated and real traffic across nine diverse IoT devices, achieving balanced accuracy (F1: 0.95). Edge-IIoTset [76] offers the highest feature diversity from a physical testbed of 25 industrial IoT devices, providing the most realistic evaluation environment for industrial applications. General-purpose network intrusion datasets such as CICIDS2017 [154] and UNSW-NB15 [155] remain valuable for training and benchmarking on contemporary attack patterns, while domain-specific datasets like N-BaIoT [157] for botnet detection and MedBIoT [156] for medical IoT are indispensable for targeted security research in their respective verticals.

The selection of appropriate datasets involves fundamental trade-offs between scale, realism, and attack diversity. For evaluating blockchain-deep learning frameworks, datasets combining high device heterogeneity, realistic behavioral patterns, and comprehensive attack variety are essential but currently lacking. Critical gaps remain: 92% of available datasets include 5 or fewer device categories, severely limiting evaluation of solutions designed for heterogeneous smart city deployments; only 6% provide continuous monitoring traces essential for evaluating behavioral authentication; and current datasets collectively address only 32% of MITRE ATT&CK for IoT tactics, leaving significant blind spots in evaluation coverage.

D. Multi-Dimensional Framework Comparison

To provide a complete evaluation of the reviewed security approaches, we introduce a multi-dimensional comparison framework assessing five approaches across six critical dimensions: scalability, latency, security level, energy efficiency, privacy preservation, and interoperability. These dimensions were selected based on their prominence in the reviewed literature and their direct relevance to smart city deployment requirements.

As visualized in the radar chart in Fig. 9, hybrid BC+DL frameworks demonstrate the most balanced performance profile, achieving competitive or superior scores across all six dimensions. Traditional PKI/TLS provides moderate baseline performance across most dimensions but falls short in interoperability and adaptive security capabilities. Blockchain-only approaches excel in security level and auditability but suffer from scalability constraints and high energy consumption due to consensus overhead. Deep-learning-only solutions offer high scalability and low latency but face fundamental limitations in privacy preservation (due to centralized data processing) and trust establishment (due to lack of immutable audit trails).

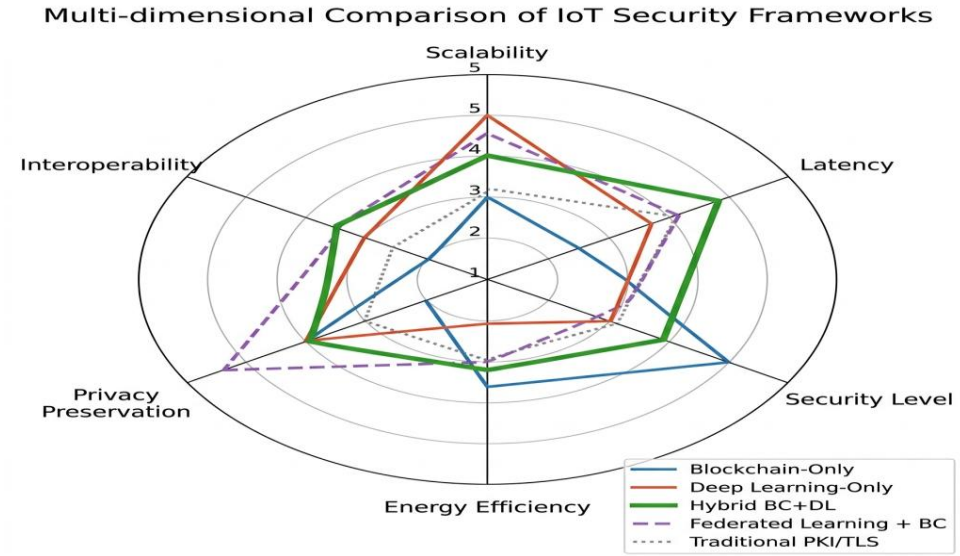

Fig. 9. Multi-dimensional comparison of five IoT security framework approaches across six evaluation criteria.

Federated Learning combined with blockchain achieves the highest privacy preservation scores while maintaining competitive security levels, making it the most promising approach for privacy-sensitive smart city applications such as healthcare IoT and smart home environments. However, the communication overhead of federated aggregation combined with blockchain consensus creates challenges for real-time applications requiring sub-second response times [82, 97].

A critical observation from this multi-dimensional analysis is that no single approach achieves optimal scores across all dimensions, confirming the need for context-aware security architectures that can dynamically select and combine approaches based on application requirements, device capabilities, and threat context. This finding directly motivates the research roadmap proposed in Section VI.

TABLE VII. Multi-Dimensional Framework Scoring Data (Scale: 1–10)

Dimension	Traditional PKI/TLS	BC-Only	DL-Only	FL+BC	Hybrid BC+DL
Scalability	7	4	8	6	7
Latency	7	5	8	5	7
Security Level	6	9	7	8	9
Energy Efficiency	7	3	6	5	6
Privacy Preservation	5	6	4	9	8
Interoperability	4	3	5	5	7

The scoring methodology draws from quantitative metrics reported in reviewed studies (latency measurements, throughput benchmarks, energy consumption profiles) supplemented by qualitative assessment of architectural properties (decentralization degree, protocol support breadth, privacy mechanism strength). Scores represent consensus estimates across the reviewed literature rather than measurements from a single testbed, and should be interpreted as relative comparisons rather than absolute ratings. Formal verification of these frameworks through standardized cryptographic proofs [174, 175] remains an important direction for establishing rigorous security guarantees.

5. Discussion

This section discusses the critical challenges that impede practical deployment of integrated blockchain-deep learning solutions in real-world smart city environments, followed by a forward-looking research roadmap. The discussion synthesizes findings from our comparative analysis and identifies the most significant barriers to widespread adoption alongside actionable research directions.

A. Scalability and Performance Bottlenecks

Blockchain consensus mechanisms introduce latency and computational overhead that are often incompatible with real-time IoT requirements. Proof-of-Work (PoW) remains entirely impractical for constrained devices due to its enormous energy consumption and slow block finality times (10–60 minutes), while even lightweight alternatives face limitations at city scale [78, 79]. PBFT achieves deterministic finality but its $O(n^2)$ message complexity limits practical deployment to networks of fewer than 100 consensus nodes. DPoS offers higher throughput but introduces centralization concerns through its limited delegate set. DAG-based approaches such as IOTA's Tangle eliminate mining entirely but face challenges in achieving consensus under low transaction volumes.

Deep learning models encounter parallel scalability barriers in heterogeneous IoT ecosystems. The computational demands of training and inference for deep neural networks conflict with the strict latency requirements of safety-critical IoT applications, creating a fundamental tension that existing frameworks have yet to resolve satisfactorily [80, 81]. In federated learning scenarios, the heterogeneity of participating devices leads to straggler effects where the slowest devices bottleneck the entire training process. Additionally, the storage requirements of blockchain grow linearly with transaction volume, creating long-term sustainability concerns for IoT deployments generating millions of daily transactions. Pruning strategies, state channels, rollups, and off-chain computation layers offer partial solutions but introduce their own complexity, trust assumptions, and potential security vulnerabilities [82].

B. Computational and Resource Constraints

IoT devices typically operate with sub-100MHz microcontrollers (e.g., ARM Cortex-M0+), less than 256KB RAM, and strict energy budgets requiring less than 1mW average power for multi-year battery operation. These severe constraints render conventional deep learning architectures infeasible for direct on-device deployment. Model compression techniques offer partial solutions but involve significant accuracy trade-offs: 8-bit quantization can reduce model size by approximately 75% but at the cost of 8–12% increased false negatives; pruning 60% of neurons saves roughly 40% energy while decreasing detection rates by up to 15% [80, 81].

Split computing approaches, where model layers are distributed between device and edge server, offer a promising middle ground but introduce latency from network round-trips and raise privacy concerns about intermediate feature transmission. The emerging TinyML approach specifically addresses deployment on sub-MB devices through neural architecture search (NAS) and knowledge distillation, but current TinyML models achieve significantly lower accuracy than their full-sized counterparts [101]. Hardware acceleration through dedicated neural processing units (NPUs) and FPGA-based implementations may ultimately bridge this gap, but widespread availability in IoT-grade devices remains years away. The Siamese neural network approach proposed by Fusco et al. [81] demonstrates promising results for TinyML-based IDS with minimal memory footprints, but generalization across diverse attack types remains challenging.

C. Data Privacy, Regulatory Compliance, and Adversarial Robustness

The application of deep learning in IoT environments raises critical data privacy risks due to the centralized processing of sensitive sensor data, which may conflict with regulatory frameworks such as GDPR (EU), CCPA (California), and emerging IoT-specific regulations in various jurisdictions [83]. While federated learning addresses some privacy concerns by keeping raw data on-device, recent research has demonstrated that gradient leakage attacks and membership inference attacks can still reconstruct sensitive training data from shared model updates, seriously challenging the privacy guarantees of standard FL implementations.

Adversarial attacks represent a fundamental and evolving challenge to DL-based security systems. Carefully crafted perturbations can deceive intrusion detection models with high confidence, creating a critical security paradox: systems designed to identify threats become themselves susceptible to targeted manipulation [84, 85]. The transferability of adversarial examples is particularly concerning in IoT contexts, where a single adversarial strategy crafted against one model can be effective against multiple deployed models across a network [86]. Current defense mechanisms, including adversarial training, defensive distillation, certified defenses, and continual adversarial defense [87], introduce 3–5x energy overhead and 15–20% accuracy degradation on clean inputs, creating an unacceptable trade-off for energy-constrained IoT devices. In addition, the emergence of generative AI tools has lowered the barrier for crafting sophisticated adversarial inputs, potentially enabling scalable attacks against deployed IoT security systems.

D. Interoperability and Standardization Gaps

The fragmentation of IoT ecosystems, with distinct security protocols, trust models, device capabilities, and administrative domains across vertical sectors, presents a major obstacle to cross-domain deployments in smart cities. A smart city typically integrates systems from transportation, energy, healthcare, public safety, and environmental monitoring, each with its own technology stack and security requirements. While emerging standards such as ACE-OAuth [162], Entity Attestation Tokens (EAT) [165], EDHOC/OSCORE [163], and RATS [164] offer potential unifying security layers, significant work remains in developing standardized profiles, conformance testing suites, and interoperability frameworks that bridge Matter/Thread, Wi-SUN FAN, 5G, and LoRaWAN domains [167, 168].

The lack of standardized APIs for blockchain integration with IoT platforms further complicates adoption. Each blockchain platform (Ethereum, Hyperledger Fabric, IOTA, Algorand) exposes different interfaces, smart contract languages, consensus configurations, and data models, making it difficult to develop portable security solutions. The absence of standardized trust anchoring mechanisms between blockchain-based identity and traditional PKI infrastructure creates interoperability barriers for organizations transitioning from legacy systems. Industry consortiums such as the Industrial Internet Consortium (IIC) and the Connectivity Standards Alliance (CSA) have begun addressing this gap through cross-platform security profiles, but widespread adoption of unified standards remains several years away [176, 177].

E. Dataset Limitations and Benchmarking Challenges

The evaluation of IoT security frameworks is significantly hampered by fundamental dataset limitations that undermine the validity of reported results. Our analysis reveals several critical gaps in the current benchmarking space: 92% of public datasets include 5 or fewer device categories, severely limiting the evaluation of solutions designed for heterogeneous smart city deployments with dozens of device types; only 6% provide continuous monitoring traces exceeding 30 days, which are essential for evaluating behavioral authentication systems and detecting slow-evolving threats; the average 3.7-year latency between the emergence of new attack types and their inclusion in benchmark datasets creates a persistent threat recency gap; and current datasets collectively address only 32% of MITRE ATT&CK for IoT tactics, leaving significant blind spots in evaluation coverage [74, 75, 76, 77].

Fig. 10 visualizes the research coverage gaps across key topics and methodologies, revealing significant under-explored areas that represent opportunities for future research. The heat map highlights particularly sparse coverage in areas such as post-quantum IoT authentication, adversarial robustness evaluation, cross-domain identity federation, and protocol-level authentication benchmarking.

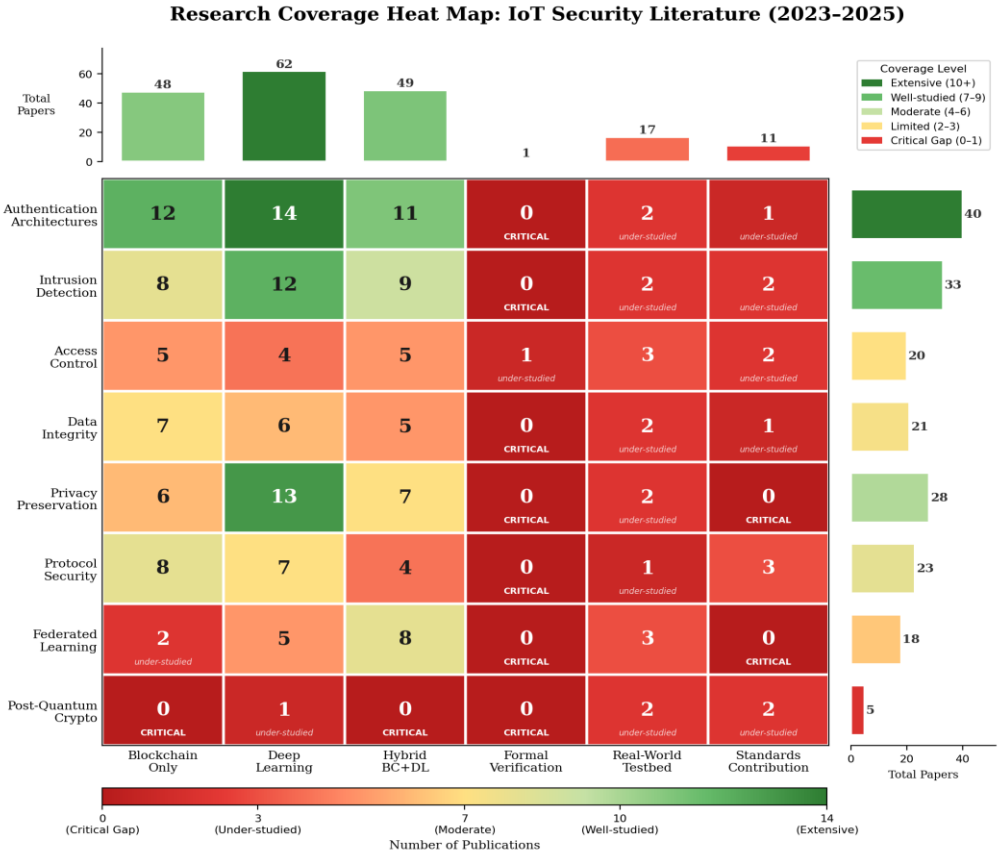

Fig. 10. Research coverage heat map: IoT security literature (2023–2025) showing topic vs. methodology coverage density.

In addition, the lack of standardized evaluation methodologies across studies makes direct comparison of reported results extremely difficult. Differences in train/test split ratios, feature selection approaches, preprocessing pipelines, and hardware platforms can lead to significantly different performance measurements for the same underlying algorithm, undermining reproducibility and scientific rigor in the field.

TABLE VIII. Summary of Open Challenges and Proposed Research Directions

Challenge Area	Current State	Key Gap	Proposed Direction	Timeline
Consensus Overhead	PoW impractical; DPoS/PBFT limited to <100 nodes	Sub-second finality at 10K+ nodes	DAG/PoA with IoT-specific optimization	2025–2027
Resource Constraints	TinyML emerging; 8–15% accuracy loss	NPU availability in IoT-grade devices	NAS + knowledge distillation + HW accel.	2025–2027
Privacy / Adversarial	FL partial; gradient leakage demonstrated	Defense overhead 3–5x energy cost	Lightweight certified defenses	2027–2029
Interoperability	Fragmented standards across verticals	No cross-domain trust bridge	Unified middleware + EAT/RATS profiles	2027–2029
Dataset Gaps	92% datasets have <=5 device types	32% MITRE ATT&CK coverage only	Community-driven open benchmarks	2025–2027
Post-Quantum	NIST standards finalized (2024)	No constrained-device implementation	HW-accelerated ML-KEM/ML-DSA	2027–2029

F. Future Research Directions and Roadmap

Based on our comprehensive analysis of the current space, identified challenges, and emerging technological trends, we propose a phased research roadmap (Fig. 11) delineating priorities across three time horizons. This roadmap aims to guide the research community toward practical, scalable, and secure IoT solutions for smart cities, organized by technological readiness and deployment feasibility.

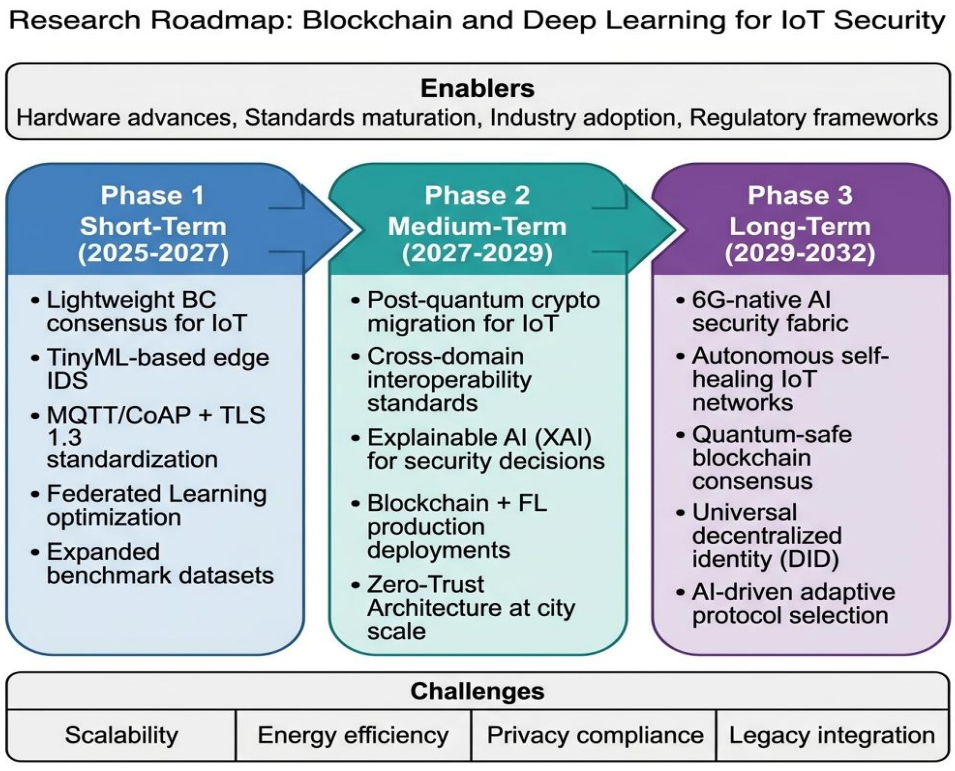

Fig. 11. Phased research roadmap for blockchain and deep learning in IoT security (2025–2032).

1) Short-Term Priorities (2025–2027):

Immediate research priorities should focus on optimizing existing technologies for practical deployment and addressing the most critical gaps identified in this survey:

• Development and benchmarking of lightweight consensus protocols (DAG-based, Proof-of-Authority, Proof-of-Elapsed-Time) specifically optimized for IoT gateway environments with sub-second finality requirements and energy budgets below 100mW [39, 40].

• Advancement of TinyML-based edge intrusion detection systems achieving sub-256KB memory footprints through neural architecture search, knowledge distillation, and mixed-precision quantization, targeting detection accuracy within 5% of full-scale models [81, 101].

• Standardization and reference implementation of MQTT/CoAP security extensions including OSCORE, EDHOC, and ACE-OAuth, with conformance testing suites and interoperability certification programs for IoT device manufacturers [162, 163].

• Optimization of federated learning for intermittent IoT connectivity through asynchronous aggregation protocols, communication-efficient gradient compression (Top-k, random sparsification), and robust aggregation algorithms resilient to Byzantine participants [100, 102].

• Creation of community-driven, open-source benchmark datasets with diverse device categories (20+ types), continuous monitoring traces (90+ days), comprehensive MITRE ATT&CK coverage, and standardized evaluation protocols enabling reproducible comparisons [74, 75, 76].

2) Medium-Term Agenda (2027–2029):

Medium-term research should address fundamental architectural challenges and prepare for emerging technological shifts:

• Post-quantum cryptography migration for IoT protocols, integrating NIST-standardized ML-KEM [171] and ML-DSA [172] algorithms into constrained device firmware with hardware acceleration support, while maintaining backward compatibility with classical cryptographic schemes during the transition period.

• Development of cross-domain interoperability standards and middleware that bridges Matter/Thread, Wi-SUN FAN, 5G, and LoRaWAN security domains under a unified trust framework with standardized credential format translation, trust delegation, and cross-domain audit logging [167, 168, 170].

• Integration of Explainable AI (XAI) techniques with immutable on-chain audit trails, enabling transparent and accountable security decision-making that satisfies regulatory requirements for algorithmic transparency and provides human-interpretable justifications for automated access control decisions [89].

• Production-scale BlockFL deployments in smart city pilot programs with rigorous evaluation of Byzantine-resilient aggregation, model convergence under real-world IoT conditions (device heterogeneity, intermittent connectivity, data imbalance), and quantification of privacy-utility trade-offs [111, 112, 133].

• Implementation and evaluation of Zero-Trust Architecture at city-wide scale, incorporating continuous device attestation via RATS/EAT, dynamic microsegmentation, AI-driven policy engines with formal verification, and automated compliance monitoring [96, 160, 164].

3) Long-Term Vision (2029–2032):

Long-term research should pursue important approaches that could reshape IoT security:

• 6G-native AI security fabric with slice-aware authentication supporting sub-millisecond re-authentication latency, ultra-reliable communication with 99.99999% availability guarantees, and seamless AI-driven trust fabrics that operate autonomously across network slices with heterogeneous security requirements [116, 117].

• Autonomous self-healing IoT networks with AI-driven threat response that can detect, isolate, mitigate, and recover from security incidents without human intervention, using multi-agent reinforcement learning for coordinated defense and self-reconfiguring security policy adaptation [140].

• Quantum-safe blockchain consensus mechanisms that maintain practical efficiency (sub-second finality, low energy consumption) while providing post-quantum security guarantees for critical infrastructure, potentially using quantum-resistant signature schemes and lattice-based cryptographic primitives [171, 172, 173].

• Universal decentralized identity (DID) frameworks enabling seamless cross-platform, cross-domain, and cross-jurisdiction device authentication and authorization with built-in privacy controls, credential portability, and automated lifecycle management [145, 146, 147].

• AI-driven adaptive protocol selection systems that dynamically choose optimal security configurations based on real-time assessment of device capabilities, network conditions, threat intelligence, and regulatory requirements, enabling context-aware security that automatically adapts to changing operational environments.

6. Conclusions

This survey has presented a comprehensive comparative analysis of integrated blockchain and deep learning architectures for secure authentication and communication in smart city IoT ecosystems. We reviewed a broad corpus of studies published between 2023 and 2025, supplemented by foundational references totaling 177 cited works, and organized them within a novel taxonomy spanning blockchain-based authentication, deep learning for intrusion defense, hybrid BC+DL integration, and protocol-level security.

Addressing our research questions, the key findings are summarized as follows:

• RQ1 (Blockchain Authentication Architectures): Blockchain-based authentication architectures are rapidly maturing through the adoption of lightweight ECC cryptography, Decentralized Identifiers (DIDs), fog-blockchain hybrid models, and consortium chains with PBFT/DPoS consensus. These approaches demonstrate particular promise for smart city scale, though credential lifecycle management (provisioning, rotation, revocation, recovery) remains an inadequately addressed challenge [89, 90, 110, 122, 145].

• RQ2 (Deep Learning for Authentication/IDS): Deep learning effectively enables continuous authentication and real-time intrusion detection, with CNN-GRU hybrid architectures and federated learning approaches achieving F1 scores exceeding 0.95 on benchmark datasets. TinyML and split computing techniques are making on-device deployment increasingly feasible for Class-1 and Class-2 IoT devices, though Class-0 devices still require edge offloading [93, 94, 101, 139].

• RQ3 (BC+DL Integration Patterns): The dominant integration patterns include Zero-Trust+blockchain frameworks for adaptive policy enforcement, BlockFL for privacy-preserving collaborative learning, and XAI+on-chain audit trails for accountable security decisions. Hybrid BC+DL frameworks consistently demonstrate the most balanced multi-dimensional performance across our six evaluation criteria [96, 133, 153].

• RQ4 (Protocol Impact): MQTT with TLS 1.3 and CoAP with OSCORE/EDHOC are emerging as the de facto standards for secure IoT communication. Application-layer security (OSCORE) is often superior to transport-layer security (DTLS) for multi-hop proxy-rich networks, while LPWAN protocols (LoRaWAN, NB-IoT) require architectural mitigations including off-chain identity anchoring for secure authentication [103, 104, 148, 162, 163].

• RQ5 (Gaps and Future Directions): Critical gaps persist in five areas: (i) cross-domain interoperability and standardization; (ii) realistic benchmarking with diverse devices and continuous traces; (iii) adversarial robustness of DL models under energy constraints; (iv) post-quantum cryptography readiness for constrained devices; and (v) unified credential lifecycle management across heterogeneous protocol families [108, 109, 171, 176].

The multi-dimensional comparative analysis reveals that no single approach adequately addresses all six evaluation dimensions (scalability, latency, security, energy efficiency, privacy, interoperability), highlighting the fundamental need for co-designed architectures that combine the complementary strengths of blockchain (immutability, decentralized trust, auditability) and deep learning (adaptability, pattern recognition, automation). The proposed phased research roadmap provides actionable guidance organized across three time horizons (2025–2027, 2027–2029, 2029–2032) for advancing the field toward resilient, scalable, and intelligent IoT security for next-generation smart cities.

A. Limitations of This Survey

This survey is subject to several limitations that should be acknowledged. First, our search was limited to English-language publications, potentially excluding relevant work published in other languages, particularly Chinese, Korean, and Japanese research that is increasingly influential in IoT security. Second, the temporal scope (2020–2025

with emphasis on 2023–2025) may omit foundational works from earlier periods that established important theoretical frameworks. Third, our dataset evaluation is constrained to publicly available benchmarks; proprietary industrial datasets from telecommunications operators and smart city deployments may exhibit different characteristics and challenges. Fourth, some emerging technologies, such as quantum computing applications for IoT, neuromorphic computing for edge intelligence, and digital twin-based security simulation, receive limited coverage due to their nascent state. Finally, the rapid pace of standardization in IoT security means that some protocol specifications referenced herein may have been updated between the time of writing and publication. Despite these limitations, we believe this survey provides a comprehensive, timely, and actionable reference for researchers and practitioners in this rapidly evolving field.

REFERENCES

1. L.A.C. Ahakonye, C.I. Nwakanma, J.M. Lee, D.S. Kim. "Ensemble Trees Bootstrap Aggregation for Detection and Characterization of IoT-SCADA Network Traffic", IEEE Transactions on Industrial Informatics, 20, pp. 5217–5228, 2023. https://doi.org/10.1109/TII.2023.3331531
2. R. Alajlan, N. Alhumam, M. Frikha. "Cybersecurity for Blockchain-Based IoT Systems: A Review", Applied Sciences, 13, 7432, 2023. https://doi.org/10.3390/app13137432
3. S. Mahmood, M. Chadhar, S. Firmin. "Cybersecurity Challenges in Blockchain Technology: A Scoping Review", Human Behavior and Emerging Technologies, 2022, 7384000, 2022. https://doi.org/10.1155/2022/7384000
4. M. Abdullahi, Y. Baashar, H. Alhussian, A. Alwadain, N. Aziz, L.F. Capretz, S.J. Abdulkadir. "Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review", Electronics, 11, 198, 2022. https://doi.org/10.3390/electronics11020198
5. L.A.C. Ahakonye, G.C. Amaizu, C.I. Nwakanma, J.M. Lee, D.S. Kim. "Classification and Characterization of Encoded Traffic in SCADA Network Using Hybrid Deep Learning", Journal of Communications and Networks, 26, pp. 65–79, 2024. https://doi.org/10.23919/JCN.2024.000001
6. K. Albulayhi, A.A. Smadi, F.T. Sheldon, R.K. Abercrombie. "IoT Intrusion Detection Taxonomy, Reference Architecture, and Analyses", Sensors, 21, 6432, 2021. https://doi.org/10.3390/s21196432
7. S.S. Mathew, K. Hayawi, N.A. Dawit, I. Taleb, Z. Trabelsi. "Integration of Blockchain and Collaborative Intrusion Detection for Secure Data Transactions in Industrial IoT: A Survey", Cluster Computing, 25, pp. 4129–4149, 2022. https://doi.org/10.1007/s10586-022-03619-5
8. C. Dhasarathan, et al. "COVID-19 Health Data Analysis and Personal Data Preserving: A Homomorphic Privacy Enforcement Approach", Computer Communications, 199, pp. 87–97, 2023. https://doi.org/10.1016/j.comcom.2022.12.004
9. M. Bellaj, et al. "An Integrated Framework for Blockchain-Inspired Intrusion Detection Systems for IoT: A Survey", IEEE Access, 12, 2024. https://doi.org/10.1109/ACCESS.2024.3417478
10. G. Bendiab, et al. "Autonomous Vehicles Security: Challenges and Solutions Using Blockchain and AI", IEEE Transactions on Intelligent Transportation Systems, 24, pp. 3614–3637, 2023. https://doi.org/10.1109/TITS.2023.3236274
11. K. Sultan, et al. "IoT Security Issues via Blockchain: A Review from the Perspective of Devices, Architecture, and Communication", Journal of IoT, 1, pp. 4–30, 2019. https://doi.org/10.32604/jiot.2019.06615
12. P. Scully. "Top 10 IoT Applications in 2020", IoT Analytics, 2020. Available at: https://iot-analytics.com (Accessed on: 15 June 2025).
13. K. Elgazzar, H. Khalil, T. Alghamdi, A. Badr, G. Abdelkader, A. Elewah, R. Buyya. "Revisiting the Internet of Things: New Trends, Opportunities and Grand Challenges", Frontiers in the Internet of Things, 1, 1073780, 2022. https://doi.org/10.3389/friot.2022.1073780
14. T. Alam. "Blockchain-Based Internet of Things: Review, Current Trends, Applications, and Future Challenges", Computers, 12, 6, 2023. https://doi.org/10.3390/computers12010006
15. McKinsey & Company. "The Internet of Things: Catching Up to an Accelerating Opportunity", McKinsey Report, Nov. 2021.
16. D. Evans. "The Internet of Things: How the Next Evolution of the Internet is Changing Everything", Cisco White Paper, 2011.
17. A. Bouguettaya, et al. "An Internet of Things Service Roadmap", Communications of the ACM, 64, pp. 86–95, 2021. https://doi.org/10.1145/3464960
18. J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, W. Zhao. "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy", IEEE Internet of Things Journal, 4, pp. 1125–1142, 2017. https://doi.org/10.1109/JIOT.2017.2683200
19. S. Ghosh, S. Sampalli. "A Survey of Security in SCADA Networks: Current Issues and Future Challenges", IEEE Access, 7, pp. 135812–135831, 2019. https://doi.org/10.1109/ACCESS.2019.2926441
20. H. Hindy, et al. "A Taxonomy of Network Threats and the Effect of Current Datasets on Intrusion Detection Systems", IEEE Access, 8, pp. 104650–104675, 2020. https://doi.org/10.1109/ACCESS.2020.2999577

21. M. Serror, et al. "Challenges and Opportunities in Securing the Industrial Internet of Things", IEEE Transactions on Industrial Informatics, 17, pp. 2985–2996, 2020. https://doi.org/10.1109/TII.2020.3023507
22. J.P.A. Yaacoub, et al. "Cyber-Physical Systems Security: Limitations, Issues and Future Trends", Microprocessors and Microsystems, 77, 103201, 2020. https://doi.org/10.1016/j.micpro.2020.103201
23. M.A. Al-Garadi, A. Mohamed, A.K. Al-Ali, X. Du, I. Ali, M. Guizani. "A Survey of Machine Learning and Deep Learning Methods for IoT Security", IEEE Communications Surveys & Tutorials, 22, pp. 1646–1685, 2020. https://doi.org/10.1109/COMST.2020.2988293
24. B.B. Gupta, M. Quamara. "An Overview of Internet of Things (IoT): Architectural Aspects, Challenges, and Protocols", Concurrency and Computation: Practice and Experience, 32, e4946, 2020. https://doi.org/10.1002/cpe.4946
25. U. Farooq, et al. "Machine Learning and the Internet of Things Security: Solutions and Open Challenges", Journal of Parallel and Distributed Computing, 162, pp. 89–104, 2022. https://doi.org/10.1016/j.jpdc.2022.01.003
26. N. Chaabouni, et al. "Network Intrusion Detection for IoT Security Based on Learning Techniques", IEEE Communications Surveys & Tutorials, 21, pp. 2671–2701, 2019. https://doi.org/10.1109/COMST.2019.2896380
27. C. Camara, P. Peris-Lopez, J.E. Tapiador. "Security and Privacy Issues in Implantable Medical Devices: A Comprehensive Survey", Journal of Biomedical Informatics, 55, pp. 272–289, 2015. https://doi.org/10.1016/j.jbi.2015.04.007
28. B. Liu, et al. "Blockchain Based Data Integrity Service Framework for IoT Data". In Proceedings of the IEEE International Conference on Web Services (ICWS), Honolulu, HI, USA, pp. 468–475, 2017. https://doi.org/10.1109/ICWS.2017.54
29. R. Das, et al. "A Deep Learning Approach to IoT Authentication". In Proceedings of the IEEE International Conference on Communications (ICC), Kansas City, MO, USA, pp. 1–6, 2018. https://doi.org/10.1109/ICC.2018.8422832
30. K.I. Ahmed, et al. "Machine Learning for Authentication and Authorization in IoT: Taxonomy, Challenges and Future Directions", Sensors, 21, 5122, 2021. https://doi.org/10.3390/s21155122
31. S.J. Pokorni. "Reliability and Availability of the Internet of Things", Vojnotehnicki Glasnik, 67, pp. 588–600, 2019. https://doi.org/10.5937/vojtehg67-21363
32. F. Chen, et al. "TrustBuilder: A Non-Repudiation Scheme for IoT Cloud Applications", Computers & Security, 116, 102664, 2022. https://doi.org/10.1016/j.cose.2022.102664
33. W. Prinz, et al. "Blockchain Technology and International Data Spaces". In Designing Data Spaces, Springer, Cham, Switzerland, 2022. https://doi.org/10.1007/978-3-030-93975-5_12
34. A. Attkan, V. Ranga. "Cyber-Physical Security for IoT Networks: A Comprehensive Review on Traditional, Blockchain and AI-Based Solutions", Complex & Intelligent Systems, 8, pp. 3559–3591, 2022. https://doi.org/10.1007/s40747-022-00667-z
35. W. Li, et al. "An Overview of Blockchain Technology: Applications, Challenges and Future Trends". In Proceedings of the IEEE ICEIEC, pp. 31–39, 2021. https://doi.org/10.1109/ICEIEC49280.2021.9422667
36. K. Christidis, M. Devetsikiotis. "Blockchains and Smart Contracts for the Internet of Things", IEEE Access, 4, pp. 2292–2303, 2016. https://doi.org/10.1109/ACCESS.2016.2566339
37. S. Wang, et al. "Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends", IEEE Transactions on Systems, Man, and Cybernetics: Systems, 49, pp. 2266–2277, 2019. https://doi.org/10.1109/TSMC.2019.2895123
38. Z. Zheng, et al. "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends". In Proceedings of the IEEE BigData Congress, pp. 557–564, 2017. https://doi.org/10.1109/BigDataCongress.2017.85
39. M.S. Solanki. "Overview of Blockchain Technology: Consensus, Architecture and Future Trends", IJIRCST, 9, pp. 47–51, 2021.
40. P. Dixit, et al. "An Overview of Blockchain Technology: Architecture, Consensus Algorithm". In Blockchain Technology and IoT, Apple Academic Press, Palm Bay, FL, USA, 2020.
41. A. Dorri, S.S. Kanhere, R. Jurdak. "Blockchain for IoT Security and Privacy: The Case Study of a Smart Home". In Proceedings of the IEEE PerCom Workshops, Kona, HI, USA, pp. 618–623, 2017. https://doi.org/10.1109/PERCOMW.2017.7917634
42. M.S. Ali, et al. "Applications of Blockchains in the Internet of Things: A Comprehensive Survey", IEEE Communications Surveys & Tutorials, 21, pp. 1676–1717, 2018. https://doi.org/10.1109/COMST.2018.2886932
43. M.A. Khan, K. Salah. "IoT Security: Review, Blockchain Solutions, and Open Challenges", Future Generation Computer Systems, 82, pp. 395–411, 2018. https://doi.org/10.1016/j.future.2017.11.022
44. I. Makhdoom, et al. "Blockchain's Adoption in IoT: The Challenges and a Way Forward", Journal of Network and Computer Applications, 125, pp. 251–279, 2019. https://doi.org/10.1016/j.jnca.2018.10.019
45. T.M. Fernandez, et al. "Review of IoT Applications in Agro-Industrial and Environmental Fields", Computers and Electronics in Agriculture, 142, pp. 283–297, 2017. https://doi.org/10.1016/j.compag.2017.09.015
46. A. Panarello, et al. "Blockchain and IoT Integration: A Systematic Survey", Sensors, 18, 2575, 2018. https://doi.org/10.3390/s18082575
47. N. Kshetri. "Can Blockchain Strengthen the Internet of Things?", IT Professional, 19, pp. 68–72, 2017. https://doi.org/10.1109/MITP.2017.3051335
48. Y.I. Alzoubi, et al. "IoT and Blockchain Integration: Security, Privacy, Technical, and Design Challenges", Future Internet, 14, 216, 2022. https://doi.org/10.3390/fi14070216

49. E.A. Shammar, et al. "A Survey of IoT and Blockchain Integration: Security Perspective", IEEE Access, 9, pp. 156114–156150, 2021. https://doi.org/10.1109/ACCESS.2021.3129697
50. S. Ali, et al. "Blockchain and Federated-Learning-Based Intrusion Detection for Edge-Enabled IIoT Networks: A Survey", Ad Hoc Networks, 152, 103320, 2024. https://doi.org/10.1016/j.adhoc.2023.103320
51. H.N. Dai, Z. Zheng, Y. Zhang. "Blockchain for Internet of Things: A Survey", IEEE Internet of Things Journal, 6, pp. 8076–8094, 2019. https://doi.org/10.1109/JIOT.2019.2920987
52. M.A. Ferrag, et al. "Blockchain Technologies for the Internet of Things: Research Issues and Challenges", IEEE Internet of Things Journal, 6, pp. 2188–2204, 2018. https://doi.org/10.1109/JIOT.2018.2882794
53. A. Reyna, et al. "On Blockchain and Its Integration with IoT. Challenges and Opportunities", Future Generation Computer Systems, 88, pp. 173–190, 2018. https://doi.org/10.1016/j.future.2018.05.046
54. T.M. Ghazal, et al. "IoT for Smart Cities: Machine Learning Approaches in Smart Healthcare: A Review", Future Internet, 13, 218, 2021. https://doi.org/10.3390/fi13080218
55. R. Jabbar, et al. "Blockchain Technology for Intelligent Transportation Systems: A Systematic Literature Review", IEEE Access, 10, pp. 20995–21031, 2022. https://doi.org/10.1109/ACCESS.2022.3149958
56. M.B. Mollah, et al. "Blockchain for Future Smart Grid: A Comprehensive Survey", IEEE Internet of Things Journal, 8, pp. 18–43, 2020. https://doi.org/10.1109/JIOT.2020.2993601
57. P.K. Sharma, et al. "Blockchain Based Smart Contracts for Internet of Things Security", IEEE Internet of Things Journal, 7, pp. 10753–10763, 2020.
58. F. Casino, et al. "A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues", Telematics and Informatics, 36, pp. 55–81, 2019. https://doi.org/10.1016/j.tele.2018.11.006
59. A. Al-Fuqaha, et al. "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications", IEEE Communications Surveys & Tutorials, 17, pp. 2347–2376, 2015. https://doi.org/10.1109/COMST.2015.2444095
60. B. Alotaibi. "Utilizing Blockchain to Overcome Cyber Security Concerns in the Internet of Things: A Review", IEEE Sensors Journal, 19, pp. 10953–10971, 2019. https://doi.org/10.1109/JSEN.2019.2935035
61. M.A. Ferrag, L. Shu. "The Performance Evaluation of Blockchain-Based Security Mechanisms for Internet of Things", IEEE Internet of Things Journal, 8, pp. 17236–17260, 2021. https://doi.org/10.1109/JIOT.2021.3078072
62. M. El-Hajj, et al. "A Survey of Internet of Things (IoT) Authentication Schemes", Sensors, 19, 1141, 2019. https://doi.org/10.3390/s19051141
63. P. Chaudhary, et al. "A Survey on Blockchain and IoT Integration from Security Perspective", IEEE Access, 10, pp. 90334–90363, 2022. https://doi.org/10.1109/ACCESS.2022.3198578
64. H. Yang, et al. "A Survey on Smart Agriculture: Development Modes, Technologies, and Security and Privacy Challenges", IEEE/CAA Journal of Automatica Sinica, 8, pp. 273–302, 2021. https://doi.org/10.1109/JAS.2020.1003536
65. A. Kumar, et al. "A Comprehensive Survey on the Edge, Fog, and Cloud Computing", Peer-to-Peer Networking and Applications, 14, pp. 1–40, 2021.
66. W. Viriyasitavat, et al. "Blockchain-Based Business Process Management (BPM) for Service Composition", Journal of Intelligent Manufacturing, 31, pp. 1737–1748, 2020. https://doi.org/10.1007/s10845-018-1422-y
67. S.S. Gill, et al. "Transformative Effects of IoT, Blockchain and Artificial Intelligence on Cloud Computing: Evolution, Vision, Trends and Open Challenges", Internet of Things, 8, 100118, 2019. https://doi.org/10.1016/j.iot.2019.100118
68. S. Walling, S. Lodh. "An Extensive Review of Machine Learning and Deep Learning Techniques on Network Intrusion Detection Systems for IoT Networks", Transactions on Emerging Telecommunications Technologies, 36, e70064, 2025. https://doi.org/10.1002/ett.70064
69. P. Sinha, et al. "A High Performance Hybrid LSTM CNN Secure Architecture for IoT Environments", Scientific Reports, 15, 9684, 2025. https://doi.org/10.1038/s41598-025-93898-0
70. R. Chinnasamy, et al. "Contextual IoT Intrusion Detection: CNN-GRU Enhanced by Graph Neural Networks for Smart City Security", Cureus, 2025. https://doi.org/10.7759/cureus.80752
71. Ayasha, S. Athilakshmi. "Behavioural Decentralized Biometrics-Based Trust Score Authentication for IoT". In Smart Systems, Springer, Singapore, 2025. https://doi.org/10.1007/978-981-97-7371-8_2
72. C. Sheng, et al. "Network Traffic Fingerprinting for Industrial IoT Device Identification: A Survey", IEEE Transactions on Industrial Informatics, 2025. https://doi.org/10.1109/TII.2025.3533653
73. D. Baswaraj, et al. "A Hybrid Deep Learning Framework for IoT Security Enhancement and Anomaly Detection". In Proceedings of the IEEE ICICACS, pp. 1–6, 2025. https://doi.org/10.1109/ICICACS62495.2025.10823124
74. N. Koroniotis, et al. "Towards the Development of Realistic Botnet Dataset in the IoT for Network Forensics: Bot-IoT Dataset", Future Generation Computer Systems, 100, pp. 779–796, 2019. https://doi.org/10.1016/j.future.2019.05.041
75. A. Alsaedi, et al. "TON_IoT Telemetry Dataset: A New Generation Dataset of IoT and IIoT for Data-Driven Intrusion Detection Systems", IEEE Access, 8, pp. 165130–165150, 2020. https://doi.org/10.1109/ACCESS.2020.3022862
76. M.A. Ferrag, et al. "Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning", IEEE Access, 10, pp. 40281–40306, 2022. https://doi.org/10.1109/ACCESS.2022.3165809
77. S. Garcia, et al. "An Empirical Comparison of Botnet Detection Methods", Computers & Security, 45, pp. 100–123, 2014. https://doi.org/10.1016/j.cose.2014.05.011
78. M. Zhu, S. Gupta. "To Prune, or Not to Prune: Exploring the Efficacy of Pruning for Model Compression", arXiv, arXiv:1710.01878, 2017.

79. W. Wang, et al. "Compression of Deep Learning Models for Natural Language Processing", arXiv, arXiv:2205.10745, 2022.
80. B. Lin, et al. "Efficient GPU Kernels for N:M-Sparse Weights in Deep Learning", Proceedings of Machine Learning and Systems, 5, pp. 513–525, 2023.
81. P. Fusco, et al. "TinyML-Based Intrusion Detection System for IoT-Edge Domain Using Siamese Neural Network". In Proceedings of the AINA, pp. 389–402, 2025. https://doi.org/10.1007/978-3-031-77738-7_32
82. M.A. Naeem, et al. "The Impact of Federated Learning on Improving IoT-Based Networks in Smart Cities: A Systematic Review", Electronics, 13, 3653, 2024. https://doi.org/10.3390/electronics13183653
83. N. Waheed, et al. "Security and Privacy in IoT Using Machine Learning and Blockchain: Threats and Countermeasures", ACM Computing Surveys, 53, pp. 1–37, 2020. https://doi.org/10.1145/3417987
84. I. Goodfellow, et al. "Generative Adversarial Networks", Communications of the ACM, 63, pp. 139–144, 2020. https://doi.org/10.1145/3422622
85. Y. Tu, et al. "Towards Adversarial Control Loops in Sensor Attacks", arXiv, arXiv:2203.07670, 2022.
86. A. Grini, et al. "Constrained Network Adversarial Attacks: Validity, Robustness, and Transferability", arXiv, arXiv:2505.01328, 2025.
87. Q. Wang, et al. "Continual Adversarial Defense", arXiv, arXiv:2312.09481, 2023.
88. R. Islam, et al. "Decentralized Trust Framework for Smart Cities: A Blockchain-Enabled Model with AI-Driven Threat Detection", Scientific Reports, 15, 23454, 2025. https://doi.org/10.1038/s41598-025-05665-4
89. R. Kumar, et al. "Blockchain-Based Authentication and Explainable AI for Securing Consumer Internet of Things", IEEE Transactions on Consumer Electronics, 70, pp. 1145–1154, 2023. https://doi.org/10.1109/TCE.2023.3320632
90. A. Iftikhar, et al. "A Blockchain Based Secure Authentication Technique for Edge-Based Smart City Networks", Journal of Network and Computer Applications, 233, 104052, 2025. https://doi.org/10.1016/j.jnca.2024.104052
91. B.B. Pannyagol, S.L. Deshpande. "Ensure Authentication and Confidentiality in Blockchain-Based IoT Communication System", Computers & Electrical Engineering, 124, 110303, 2025. https://doi.org/10.1016/j.compeleceng.2025.110303
92. A. Enaya, et al. "Survey of Blockchain-Based Applications for IoT in Smart Cities", Applied Sciences, 15, 4562, 2025. https://doi.org/10.3390/app15084562
93. A.K. Sahu, et al. "Deep Learning-Based Continuous Authentication for IoT-Enabled Healthcare", Computers & Electrical Engineering, 99, 107817, 2022. https://doi.org/10.1016/j.compeleceng.2022.107817
94. C. Hazman, et al. "Enhanced Intrusion Detection System with Deep Learning for IoT-Based Smart Cities Security", Tsinghua Science and Technology, 29, pp. 929–947, 2024. https://doi.org/10.26599/TST.2023.9010071
95. E. Dritsas, M. Trigka. "Machine Learning for Blockchain and IoT Systems in Smart Cities: A Survey", Future Internet, 16, 324, 2024. https://doi.org/10.3390/fi16090324
96. Salim, et al. "Zero-Trust Blockchain-Enabled Architecture for Scalable and Secure IoT Networks", Future Generation Computer Systems, 108093, 2025. https://doi.org/10.1016/j.future.2025.108093
97. R. Al-Huthaifi, et al. "Federated Learning in Smart Cities: Privacy and Security Survey", Information Sciences, 632, pp. 833–857, 2023. https://doi.org/10.1016/j.ins.2023.03.033
98. S. Banabilah, et al. "Federated Learning Review: Fundamentals, Enabling Technologies, and Future Applications", Information Processing & Management, 59, 103061, 2022. https://doi.org/10.1016/j.ipm.2022.103061
99. Y. Qasmaoui, et al. "Federated Learning for Smart Cities: A Comprehensive Survey", arXiv, arXiv:2410.08233, 2024.
100. E. Dritsas, M. Trigka. "Federated Learning for IoT: Techniques, Challenges, and Applications", Journal of Sensor and Actuator Networks, 14, 9, 2025. https://doi.org/10.3390/jsan14010009
101. M.N. Ramadan, et al. "Federated Learning and TinyML on IoT Edge Devices", ICT Express, 2025. https://doi.org/10.1016/j.icte.2025.02.004
102. M. Ragab, et al. "Advanced AI with Federated Learning for Privacy-Preserving Cyberthreat Detection in IoT Cloud Convergence", Scientific Reports, 15, 4470, 2025. https://doi.org/10.1038/s41598-025-89015-2
103. K.T.M. Tran, et al. "Analysis and Performance Comparison of IoT Message Transfer Protocols", International Journal of Networking and Distributed Computing, 12, pp. 131–143, 2024. https://doi.org/10.2991/978-94-6463-174-6_6
104. A.F. Gentile, et al. "Network Performance Analysis of MQTT Security Protocols", Applied Sciences, 14, 7461, 2024. https://doi.org/10.3390/app14177461
105. F. Hessel, et al. "LoRaWAN Security: An Evolvable Survey on Vulnerabilities, Attacks, and Their Systematic Mitigation", ACM Transactions on Sensor Networks, 18, pp. 1–55, 2023. https://doi.org/10.1145/3524285
106. M. Giacobbe, et al. "Key Challenges in LoRaWAN-Based Edge-Cloud for Smart Cities", 2025.
107. E. Dritsas, M. Trigka. "A Survey on Cybersecurity Threats, Vulnerabilities, and Countermeasures in IoT", Future Internet, 17, 30, 2025. https://doi.org/10.3390/fi17010030
108. A.N. Alsheavi, et al. "IoT Authentication Protocols: Classification, Trend and Opportunities", IEEE Transactions on Sustainable Computing, 2024. https://doi.org/10.1109/TSUSC.2024.3389101
109. S. Dargaoui, et al. "Internet of Things Authentication Protocols: Comparative Study", CMC-Computers, Materials & Continua, 79, 2024. https://doi.org/10.32604/cmc.2024.048596
110. O.A. Khashan. "Trust-Based Fog-Blockchain Model for Scalable Authentication in Smart Cities", Computer Networks, 264, 111278, 2025. https://doi.org/10.1016/j.comnet.2025.111278
111. Y. Jiang, et al. "Blockchained Federated Learning for Internet of Things: A Comprehensive Survey", ACM Computing Surveys, 56, pp. 1–37, 2024. https://doi.org/10.1145/3659099

112. W. Ning, et al. "Blockchain-Based Federated Learning: A Survey and New Perspectives", Applied Sciences, 14, 3350, 2024. https://doi.org/10.3390/app14093350
113. N. Monios, et al. "A Thorough Review of Commercial and Open-Source IoT Platforms for Smart Cities", Electronics, 13, 1465, 2024. https://doi.org/10.3390/electronics13081465
114. B. Alotaibe. "A Review of Authentication in the Internet of Things", Computer Science Review, 48, 100560, 2023. https://doi.org/10.1016/j.cosrev.2023.100560
115. A. Alotaibi, et al. "A Review of Authentication Techniques for IoT Devices in Smart Cities: Mechanisms, Advantages, and Challenges", Sensors, 25, 1649, 2025. https://doi.org/10.3390/s25051649
116. W. Saad, et al. "A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems", IEEE Network, 34, pp. 134–142, 2019. https://doi.org/10.1109/MNET.001.1900287
117. S. Dang, et al. "What Should 6G Be?", Nature Electronics, 3, pp. 20–29, 2020. https://doi.org/10.1038/s41928-019-0355-6
118. N.S. Patil, et al. "Blockchain-Based Patient-Centric Health Record Management for Enhanced Privacy in IoMT", Technology and Health Care, 2025. https://doi.org/10.1177/09287329251323009
119. Z. Sun, et al. "Internet of Things Security and Privacy: Design Methods and Optimization", Springer, Cham, Switzerland, 2022.
120. F. Sabahi, A. Movaghar. "Intrusion Detection: A Survey". In Proceedings of the 3rd International Conference on Systems and Networks Communications, 2008.
121. W. Wang, et al. "ECC-Based Blockchain Identity Authentication for IoT Devices", IEEE Access, 2024.
122. A. Khalique, et al. "Lightweight Authentication for IoT Devices in Sustainable Smart Cities", Scientific Reports, 15, 25410, 2025. https://doi.org/10.1038/s41598-025-09975-3
123. D. Khoury, et al. "CoAP/DTLS Protocols in IoT Based on Blockchain Light Certificate", Internet of Things, 6, 2025. https://doi.org/10.1016/j.iot.2025.101541
124. T.C. Hsu. "Designing a Secure Service Agent for IoT Systems Through Blockchain and MQTT Protocol Fusion", Applied Sciences, 14, 2975, 2024. https://doi.org/10.3390/app14072975
125. T.C. Hsu. "Blockchain-Based MQTT Message Verification and Trust Scoring for IoT Ecosystems", Future Internet, 17, 24, 2025. https://doi.org/10.3390/fi17010024
126. B. Alotaibi. "Enhancing MQTT Security with Distributed Machine Learning Framework for IoT Networks", IEEE Access, 2024. https://doi.org/10.1109/ACCESS.2024.3522082
127. M.L. Bangare. "Securing MQTT-Based IoT Using Blockchain Framework with Merkle Data Integrity", Peer-to-Peer Networking and Applications, 18, 38, 2025. https://doi.org/10.1007/s12083-024-01829-1
128. X. Li, et al. "An Anonymous IoT Authentication and Key Agreement Scheme with Auxiliary Signals for DAC Synchronization", IEEE Internet of Things Journal, 2025. https://doi.org/10.1109/JIOT.2025.3530825
129. L. Prazeres, et al. "IoT-Based Smart City Intrusion Detection Systems Using Supervised Machine Learning Classifiers". In Proceedings of the IEEE CISTI, 2024. https://doi.org/10.23919/CISTI62500.2024.10690564
130. R. Alsulami, et al. "IoT Protocol-Enabled Intrusion Detection System Based on Machine Learning", Engineering, Technology & Applied Science Research, 13, pp. 12373–12380, 2023. https://doi.org/10.48084/etasr.6463
131. G. Stanco, et al. "A Comprehensive Survey on Security of Low-Power Wide-Area Network-Based IoT Networks", ICT Express, 10, pp. 519–552, 2024. https://doi.org/10.1016/j.icte.2024.02.005
132. M. Piechowiak, et al. "Smart Metering System Using Machine Learning and LoRaWAN for Efficient Coverage Planning", Scientific Reports, 14, 24143, 2024. https://doi.org/10.1038/s41598-024-73921-6
133. A. Sharma, et al. "Blockchain-Based Zero Trust Networks with Federated Transfer Learning for Internet of Things Environments", PLoS ONE, 20, e0323241, 2025. https://doi.org/10.1371/journal.pone.0323241
134. M. Devi, et al. "Federated Learning-Enabled Lightweight Intrusion Detection System for Secure Wireless Sensor Networks in Smart City Environments", Intelligent Systems with Applications, 25, 200553, 2025. https://doi.org/10.1016/j.iswa.2025.200553
135. S. Gigli, et al. "Zero-Trust Oracle Networks: Securing IoT Data Integrity via Blockchain", IEEE Internet of Things Journal, 2025. https://doi.org/10.1109/JIOT.2025.3528281
136. H. Rai, et al. "A Blockchain-Based Approach for Securing IoT Networks: Issues and Challenges", Discover Internet of Things, 5, 10, 2025. https://doi.org/10.1007/s43926-025-00099-0
137. O.M. Al-Matari, et al. "Blockchain Applications in Healthcare, Supply Chains, and Smart Cities: A Systematic Literature Review", Discover Blockchain, 2, 10, 2024. https://doi.org/10.1007/s44381-024-00004-8
138. M. Ahsan, et al. "Securing the Internet of Things with Blockchain: A Systematic Review and NIST-Based Framework", Information, 16, 470, 2025. https://doi.org/10.3390/info16060470
139. A. Sagu, et al. "Advances in Internet of Things Security: A GRU-CNN Deep Learning Model for Network Intrusion Detection", Scientific Reports, 15, 16485, 2025. https://doi.org/10.1038/s41598-025-98870-6
140. A.Z. Far, et al. "AI for Secured Information Systems in Smart Cities: Collaborative IoT-Edge with Deep Reinforcement Learning and Blockchain", arXiv, arXiv:2409.16444, 2024.
141. Z. Yang, et al. "A Blockchain-Based Framework for Smart City Data Privacy: Decentralized Access Control and Policy Management", IEEE Access, 2024.
142. S. Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008. Available at: https://bitcoin.org/bitcoin.pdf (Accessed on: 15 June 2025).

143. N. Szabo. "Smart Contracts: Building Blocks for Digital Markets", 1996.
144. V. Buterin. "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform", White Paper, 2014. Available at: https://ethereum.org/whitepaper (Accessed on: 15 June 2025).
145. Z. Yang, et al. "BDIDA-IoT: A Blockchain-Based Decentralized Identity Architecture for Internet of Things", Applied Sciences, 14, 1807, 2024. https://doi.org/10.3390/app14051807
146. D.F. Ramirez, et al. "Decentralized Device Identity Management for Internet of Things Using IOTA Blockchain", Heliyon, 11, e42598, 2025. https://doi.org/10.1016/j.heliyon.2025.e42598
147. Y. Zhang, et al. "Trusted Data Collection System for Smart Cities with Decentralized Identifiers and Blockchain". In Proceedings of the IEEE IoT, 2024. https://doi.org/10.1109/IoT62082.2024.00019
148. N.O. Gavriilidis, et al. "Empirical Evaluation of TLS-Enhanced MQTT on Constrained IoT Devices", Applied Sciences, 15, 8398, 2025. https://doi.org/10.3390/app15158398
149. J. Cao, et al. "A Survey on Security Aspects for 3GPP 5G Networks", IEEE Communications Surveys & Tutorials, 22, pp. 170–195, 2019. https://doi.org/10.1109/COMST.2019.2951818
150. L. Yi, et al. "A Review of Blockchain Technology Applications in Wireless Sensor Networks", Sensors, 23, 2300, 2023. https://doi.org/10.3390/s23042300
151. D.A. Tagliaro, et al. "Vulnerability Analysis of Smart City Backend Infrastructure". In Proceedings of the IEEE/ACM CAIN, 2025. https://doi.org/10.1109/CAIN64350.2025.00028
152. F.S. Alsubaei, et al. "A Survey of Deep-Learning-Based Detection of Cybersecurity Threats for IoT Devices", Computers, 14, 175, 2025. https://doi.org/10.3390/computers14050175
153. A. Albugmi. "Hybrid Smart IoT Detection and Prevention Framework for Smart Cities Using Blockchain Technology", IJAAS, 12, pp. 107–115, 2025. https://doi.org/10.21833/ijaas.2025.01.013
154. I. Sharafaldin, A.H. Lashkari, A.A. Ghorbani. "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization". In Proceedings of the ICISSP, 2018. https://doi.org/10.5220/0006639801080116
155. N. Moustafa, J. Slay. "UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems". In Proceedings of the MilCIS, pp. 1–6, 2015. https://doi.org/10.1109/MilCIS.2015.7348942
156. A. Guerra-Manzanares, et al. "MedBIoT: Generation of an IoT Botnet Dataset in a Medium-Sized IoT Network". In Proceedings of the ICISSP, pp. 207–218, 2020. https://doi.org/10.5220/0009187802070218
157. Y. Meidan, et al. "N-BaIoT: Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders", IEEE Pervasive Computing, 17, pp. 12–22, 2018. https://doi.org/10.1109/MPRV.2018.03367731
158. K. Ishaq, S.S. Farooq. "Exploring the Internet of Things in Smart Cities: Practices, Challenges and Way Forward", arXiv, arXiv:2309.12344, 2023.
159. COE Security. "Safeguarding 27 Billion IoT Devices in 2025", COE Security Blog, 2025. Available at: https://www.coe.com.sa (Accessed on: 15 June 2025).
160. S. Kulkarni, et al. "Using the Zero Trust Five-Step Implementation Process with Smart Environments", Future Internet, 17, 313, 2025. https://doi.org/10.3390/fi17070313
161. M.N.O. Sadiku, et al. "Smart Cities: A Primer", International Journal of Advanced Research in Computer Science and Software Engineering, 7, 2017.
162. F. Palombini, et al. "OSCORE Profile of the Authentication and Authorization for Constrained Environments (ACE) Framework", IETF RFC 9203, 2022. https://doi.org/10.17487/RFC9203
163. G. Selander, et al. "Ephemeral Diffie-Hellman Over COSE (EDHOC)", IETF RFC 9528, 2024. https://doi.org/10.17487/RFC9528
164. H. Birkholz, et al. "Remote ATtestation procedureS (RATS) Architecture", IETF RFC 9334, 2023. https://doi.org/10.17487/RFC9334
165. L. Lundblade, et al. "The Entity Attestation Token (EAT)", IETF RFC 9711, 2024. https://doi.org/10.17487/RFC9711
166. FIDO Alliance. "FIDO Device Onboard Specification v1.1", 2022. Available at: https://fidoalliance.org/specs/FDO/ (Accessed on: 15 June 2025).
167. Connectivity Standards Alliance. "Matter Specification v1.4", 2024. Available at: https://csa-iot.org (Accessed on: 15 June 2025).
168. Wi-SUN Alliance. "Field Area Network (FAN) Technical Profile Specification 1.1 v2.0", 2024.
169. OMA SpecWorks. "Lightweight M2M (LwM2M) v1.2", 2022. Available at: https://www.openmobilealliance.org (Accessed on: 15 June 2025).
170. 3GPP. "Security Architecture and Procedures for 5G System", 3GPP TS 33.501 v18.6.0, 2024. Available at: https://www.3gpp.org (Accessed on: 15 June 2025).
171. National Institute of Standards and Technology (NIST). "ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism Standard)", NIST FIPS 203, 2024. https://doi.org/10.6028/NIST.FIPS.203
172. National Institute of Standards and Technology (NIST). "ML-DSA (Module-Lattice-Based Digital Signature Standard)", NIST FIPS 204, 2024. https://doi.org/10.6028/NIST.FIPS.204
173. National Institute of Standards and Technology (NIST). "SLH-DSA (Stateless Hash-Based Digital Signature Standard)", NIST FIPS 205, 2024. https://doi.org/10.6028/NIST.FIPS.205
174. J.P. Aumasson. "Too Much Crypto", Cryptology ePrint Archive, 2019/1492, 2019.
175. G. Barthe, et al. "EasyCrypt: A Tutorial". In Foundations of Security Analysis and Design VII, Springer, Berlin, Germany, 2013.

176. E. Rescorla. "The Transport Layer Security (TLS) Protocol Version 1.3", IETF RFC 8446, 2018. https://doi.org/10.17487/RFC8446
177. R. Barnes, et al. "Automatic Certificate Management Environment (ACME)", IETF RFC 8555, 2019. https://doi.org/10.17487/RFC8555