DOI: http://dx.doi.org/10.26483/ijarcs.v16i4.7323

ISSN No. 0976-5697

Volume 16, No. 4, July-August 2025

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

A REVIEW ON SMART DEVICES, NETWORKING TECHNOLOGIES AND SECURITY IN NEXT-GENERATION IOT SYSTEMS

Sandeep Gupta
SATI, Vidisha, India

***Abstract*—**The digital environment has been completely transformed by advancements in the Internet of Things (IoT), which have led to the creation of intelligent, interconnected systems that integrate smart devices, advanced networking technologies, and adaptive security frameworks. The main elements propelling next-generation IoT systems are thoroughly reviewed in this paper. It classifies smart devices based on their functionalities and explores their benefits in enhancing automation, energy efficiency, and remote monitoring. Communication between devices may be made low-latency, scalable, and energy-efficient with the help of emerging networking technologies like 5G, Low Power Wide Area Networks (LPWAN), Software-Defined Networking (SDN), and network slicing. It is anticipated that integrating artificial intelligence (AI) into the Internet of Things would revolutionize it, especially in the domains of intelligent decision-making, predictive analytics, and real-time data processing. In this investigation, end-to-end encryption, blockchain-based authentication, and mechanisms for controlling access, such as Role-Based Access Control (RBAC) are examined as ways to protect user privacy and data integrity. According to the paper, AI, smart devices, and advanced networking combine to create autonomous, real-time systems in several domains, such as health care, smart cities, and industry automation. Despite advancements, interoperability, data privacy, and energy limitations remain problems, highlighting the necessity of more research into standardization, low-power cryptography, and AI-enhanced frameworks.

***Keywords*—**Internet of Things (IoT), Smart Devices, Networking Technologies, Edge Computing, Software-Defined Networking (SDN), Role-Based Access Control (RBAC), Zero Trust Architecture (ZTA).

I. INTRODUCTION

The concept of the Internet of Things (IoT) has grown from an idea to disrupt the world of technology to an innovation affecting everyday human interaction with technology [1]. IoT provides real-time connectivity for chosen, interconnected physical devices, sensors, and systems, which facilitates the development of smarter environments and systems in every industry, be it healthcare, agriculture, smart cities, or industrial automation [2]. IoT allows for interaction of physical devices, digital systems and the human environment. The acceleration of IoT into all areas of how lives smart homes, smart healthcare, smart agriculture and the efficiency in smart automation/industrial revolution has increasingly made IoT more intelligent, efficient and scalable. The latest generation of IoT systems represents a shift to improved performance, autonomy, and real-time analytics. But it is the three interconnected and emergent pillars of smart devices, networking technologies and security frameworks that support them that define current and future IoT systems.

At the centre of next-generation IoT systems are smart devices that are the nodes of interaction and generation of raw IoT data. The use of AI-compatible processors, local processing power, and dynamic, adaptive functionality is rapidly making smart hardware, such as wearables, smart home appliances, and industrial sensors, more intelligent. In particular, hardware miniaturization and contextually aware processing make it possible for IoT nodes to operate, even autonomously, further enabling distributed intelligence [3]. The dissemination of myriad different devices also introduces challenges associated with a diversity of devices with interoperability, scalability, and lifecycle management that must be thoroughly examined.

In parallel, networking technologies have seen significant innovation to meet the demands of next-generation IoT systems. Low-power wide-area networks (LPWANs) [4][5], 5G, and software-defined networking (SDN) are enabling energy-efficient, fast, and low-latency connectivity. As IoT network design moves towards more decentralized models, edge and fog computing become increasingly important for latency reduction and data preparation. This section of the review dissects how modern networking frameworks are being tailored to support the massive connectivity and responsiveness needed in IoT deployments.

As IoT systems expand, security and privacy become paramount concerns [6]. The heterogeneous nature of devices, coupled with continuous data generation and transmission, creates a large attack surface susceptible to dangers including denial-of-service (DoS) assaults, data leaks, and device spoofing. Furthermore, the use of conventional security measures is restricted by the limited resources of many IoT devices. This review investigates emerging security frameworks, such as blockchain-based authentication, lightweight encryption and AI-driven threat detection that aim to provide robust protection across IoT layers without compromising performance

A. Structure of the paper

This paper is structured as follows: Section II covers smart devices in next-generation IoT systems. Section III outlines networking technologies for IoT. Section IV addresses security and privacy concerns. Section V presents a literature review, and Section VI concludes with key findings and future work.

II. SMART DEVICES IN NEXT-GENERATION IOT SYSTEMS

The basis of the next generation the intelligent integration of smart devices that facilitate data collection, processing, and transfer across networked settings, is the foundation of IoT systems. These devices serve as the primary link between the digital and physical realms, providing real-time information and the ability to make decisions on their own. As seen in Figure 1, this section examines the categorization, essential features, and developing patterns of smart devices within the IoT ecosystem.

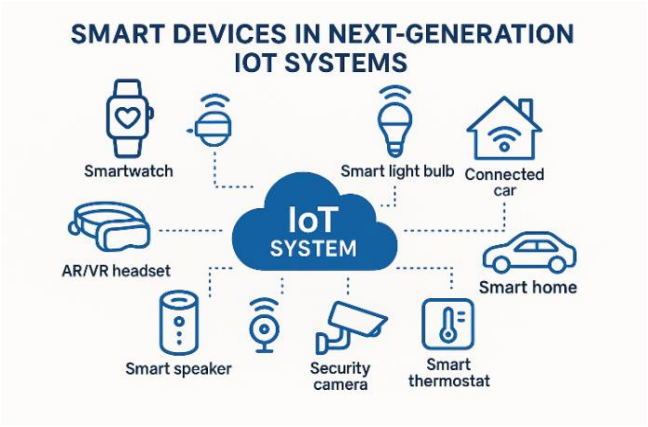

Fig. 1. Smart Devices in Next-Generation IOT Systems

The central IoT system cloud coupled to several smart devices is depicted in Figure 1 as smart devices in the next-generation IOT system. These include a smartwatch, smart light bulb, connected car, smart home, AR/VR headset, smart speaker, security camera, and smart thermostat. Each device is visually represented with icons and labeled accordingly. Dotted lines link each device to the central cloud [7], indicating connectivity within the IoT ecosystem.

A. Smart Devices

Smart devices are electronic devices with some form of computing power, connectivity, and real-time interaction with users and other devices. To gather, process, and transmit data independently, they often have sensors, processors, and communication modules. One component of the IoT ecosystem is smart devices. [8]. They enable more automation, greater efficiency, and better user experience in various areas. Sometimes they are categorized based on how they function or the application domain they belong to. Examples of common categories include, but are not limited to: Medical gadgets, wearable technology, smart home devices, and industrial IoT devices. Even though they all serve different purposes, they all have similar elements of connectivity, intelligence, and responsiveness. Smart devices continue to evolve with improvements in AI, wireless networking, and embedded systems.

B. Smart IoT Device Classification

To extract some higher-level information, ML algorithms must be able to handle and comprehend IoT data. Complex information like "how many people are in the room right now?" or simple statistics like "the average temperature in a room" all require data analysis to extract meaningful insights from the data [9]. It takes varying degrees of hardware resources to process this type of data. The necessary algorithm resources must be compatible with the hardware class of the most widely used IoT devices available on the market, a categorization system for IoT devices was therefore developed. To carry out this type of data analysis and extract the pertinent information, the gadget must be able to fuse (combine) all the data. Four categories may be used to classify it:

- **Low-Level Fusion:** It's also known as signal level fusion. Integrating the raw data inputs produces a fresh piece of information that is more precise than the individual inputs.
- **Medium-Level Fusion:** A feature map is created by fusing an entity's attributes or features, which may then be utilized for different purposes. It is sometimes referred to as feature/attribute level fusion.
- **High-Level Fusion:** It's also known as decision-level fusion or symbol fusion. It uses symbolic representations or assessments as input to provide a conclusion that is more confident and/or global.
- **Multilevel Fusion:** Multilevel fusion happens when input and output can be of any level and data with different levels of abstraction are included in the fusion process.

C. Benefits of IoT for Smart Devices

In the following benefits, smart home automation is shown to enhance daily living through improved control, energy efficiency, environmental sustainability, and advanced security features are highlighted below:

- **Monitoring and Control:** The next degree of control over household appliances or equipment is provided by smart home automation [10]. can use a mobile device or internet network to not only remotely turn on or off household appliances, but also to fully manage their operation.
- **Optimization of spending:** Energy consumption is enabled or assisted by IoT and smart home systems, which also optimize expenditure. Can quickly determine areas of use and waste, allowing for appropriate consumption or usage adjustments. Smart lights, for instance, automatically switch on and off based on information or values received from sensors or actuators.
- **Environmental impact:** The entire earth benefits from this smart home automation program, not just the homeowners, their neighbors, and the nation. It lowers the carbon footprint while simultaneously decreasing resource and expenditure optimization. Everyone can go green thanks to IoT or smart grid technology, which also lowers carbon emissions and contributes to pollution reduction. The concept of smart home automation is continuously expanding.
- **Enhance security:** Along with being instruments for home protection, smart locks and surveillance cameras also serve as smart monitoring systems that can identify leaks and power surges. To avoid issues, they periodically notify us about harmful pollutant gases using petrol and water sensors.

III. NETWORKING TECHNOLOGIES FOR IOT

The Networking technology is the backbone of IoT systems, allowing data to be easily transferred between smart devices, cooperate, and communicate. Flexible and effective networking solutions are required due to the variety of IoT applications, which range from industry automation and smart homes. This section explores the key communication requirements, protocols, architectures, and future innovations that shape IoT connectivity, with a focus on performance, scalability, and interoperability, as shown in Figure 2.

Fig. 2. Networking Technologies for IOT

Networking technologies for IOT are shown in Figure 2 presents a central cloud labeled "IoT" connected to five key networking technologies [11]. These include Wi-Fi, Bluetooth, Cellular, Low Power Wide Area Network (LPWAN), and Zigbee, each represented with a distinct icon. The visual layout highlights how these technologies link to and support IoT connectivity. It emphasizes the diverse communication options available for different IoT use cases.

A. IoT Communication Requirements

IoT networks are characterized by their unique operational constraints and application-specific demands. The key communication requirements include:

1) Low Power Consumption

IoT devices frequently run for long periods on batteries, necessitating energy-efficient communication mechanisms.

2) Low Latency

Near real-time data transfer is necessary for applications like healthcare and industrial automation to guarantee accurate and responsive functioning.

3) *Scalability*

To maintain performance, Networks need to sustain millions of nodes as the number of connected devices rapidly rises.

B. Communication Protocols and Standards

In IoT ecosystems, communication protocols are crucial for the unhindered flow of data from devices to gateways and cloud platforms [12]. Generally, IoT communication protocols can be classified as short-range, long-range, and IP-based, which serve different purposes in terms of connectivity and effectiveness.

1) Short-range

Short-range communication protocols are typically used in localized environments such as Industrial automation systems, smart homes, and medical facilities [13].

2) Zigbee

The IEEE 802.15.4 standard serves as the foundation for the Zigbee protocol. This protocol for wireless sensor networks (WSNs) is low-cost and low-power. Mesh, tree, and star network topologies are often supported [14]. Operating at 2.4 GHz, the Zigbee protocol offers a data throughput of around 250 kbit/s.

3) Wi-Fi

The IEEE 802.11 standard serves as the foundation for Wi-Fi, which employs wireless frequencies (2.4, 5, and 60 GHz bands) to provide short-range (up to 100 m) high-speed internet access (from 1 Mb/s to 6.75 Gb/s). It is designed for wireless local area networks [15].

4) Bluetooth

Bluetooth is likely the most widely used IEEE 802.15.1 is the foundation of wireless technology. It operates between 2402 and 2480 MHz or between 2400 and 3483.5 MHz. Although there are 79 channels available, each having a frequency of 1 MHz, some nations have limits on the number of channels that may be used. In both wearable and mobile devices, Bluetooth is widely used. The goal of Bluetooth Low Energy, or BLE, is to develop low-power devices that can be powered by a cell battery continually. [16].

5) Long-range Protocols

For applications requiring wide-area coverage with minimal power usage, long-range communication protocols are preferred

6) LoRa WAN

A long-range, low-power protocol called Long Range Wide Area Network (LoRa WAN) was developed for widespread Internet of Things applications, including smart agriculture and urban sensor networks. To maximize communication efficiency, it enables adaptive data rates and operates in unlicensed frequency ranges.

7) Narrowband IoT (NB-IoT)

Narrowband IoT (NB-IoT) is a cellular-based standard developed by 3GPP that offers robust connectivity and deep indoor penetration [17]. It is suitable for applications requiring reliable transmission of small amounts of data over long durations, such as utility metering and environmental monitoring.

C. Emerging Trends in IoT Networking

The rapid evolution of the IoT has necessitated significant advancements in networking paradigms to address the growing complexity, scale, and dynamic nature of connected devices. Traditional networking approaches often fall short in accommodating the diverse and constantly evolving needs of IoT applications. As a result, several innovative networking strategies have emerged to enhance IoT networks' intelligence, scalability, and flexibility. These include network slicing, Software-Defined Networking (SDN), and the integration of AI and ML have gained substantial attention as transformative solutions in modern IoT ecosystems.

1) Software-Defined Networking (SDN)

In the Software-Defined Networking (SDN) network design, the forwarding plane and control plane logic are separated. The capacity to utilize software over open interfaces to dynamically administer networks is a novel approach to network programmability known as SDN, alter, and govern network behaviors—rather than depending on proprietary interfaces and closed boxes. The SDN architecture enables centralized control of data route components, regardless of the network technology used to link these devices, which several companies may manufacture [18]. The centralized control preserves a network-wide perspective of the data route components and their relationships, which incorporates all the intelligence. Because of its centralized, current perspective, the controller may easily modify networking operations through the centralized control plane and execute network management tasks.

2) Network Slicing for IoT

Network slicing is a key enabler for the provision of bespoke services now for 5G networks and future IoT networks. Several virtual networks with distinct characteristics may be established on the same physical infrastructure thanks to network slicing. Network slicing has several positive implications for the diverse

applications within IoT, all of which exceed specific bandwidth, latency, and reliability requirements.

3) Integration with AI/ML for Adaptive Networks

AI and ML to IoT networking is an essential milestone in the development of autonomous and dynamic network control. AI/ML algorithms gather and evaluate a deluge of real-time data generated from IoT devices to predict network performance and behavior while also spotting anomalies so network routing can be optimized [19]. These intelligent processing capabilities allow networks to make preemptive processing decisions, which can limit downtime and improve network efficiency.

IV. Security And Privacy In Next-Generation IoT Systems

Security and privacy are key concerns of next-generation IoT systems, as millions of devices are interconnected in a wide variety of applications collecting, processing, and transmitting sensitive data [20]. These systems are poised to face specific challenges due to their limited resources, heterogeneous resource-utilizing architectures, and a large attack surface. Devices, ranging from small sensors to larger hubs, typically are vulnerable to unauthorized access, malware, and physical tampering, while network access and communications can suffer attacks such denial of service, eavesdropping, and spoofing, resulting in denial of access to legitimate users. In addition to securing data sent over a network or stored on a device, user privacy must be created and maintained [21]. IoT devices often collect personal information, contextual information, or both. Therefore, next-generation IoT systems must have built-in multiple layers of security and protocols that include lightweight encryption, authentication, access controls, and privacy-centric elements such as federated learning and differential privacy [22]. Innovative frameworks like blockchain and zero trust architecture complement regulations like the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA), must be used to enhance protection from end-to-end connectivity as well as help to develop and sustain user trust in intelligent connected environments.

A. Encryption

Encryption is essential to secure communication channels and data storage in IoT systems [23]. Elliptic Curve Cryptography (ECC), AES-128, and Present are examples of lightweight encryption algorithms that are frequently employed since many IoT devices have minimal processing power and batteries. These lightweight encryption algorithms provide proper security with low computation requirements. Encryption helps ensure data confidentiality, integrity, and non-repudiation, especially when information travels over unsecured wireless networks and/or is stored in remote cloud servers.

B. Blockchain-Based Security

Blockchain technology can improve IoT security by offering decentralized, transparent, and impenetrable solutions. Blockchain can deliver trusted security in situations of device authentication, access records, firmware integrity verification, and data sharing among untrusted nodes [24][25]. Smart contracts in blockchain platforms allow for the automated enforcement of security policies without a central authority. One possibility for using blockchain technology is to record device interactions in an immutable manner or secure over-the-air (OTA) updates. With these implementations, reduce the dependence and reliance on vulnerable centralized systems.

C. Role-Based Access Control (RBAC)

In IoT contexts, role-based access control, or RBAC, is a basic security paradigm that limits system access according to the responsibilities that people or devices have been allocated. Figure 3 illustrates this concept. The danger of unwanted access is decreased since each position is linked to a distinct set of permissions. In IoT [26], RBAC helps manage access control for thousands of devices by grouping them under role profiles such as “sensor,” “gateway,” or “admin.” [27] This hierarchical model ensures simplified access management and compliance, though it may struggle with dynamic, context-aware policies in real-time systems.

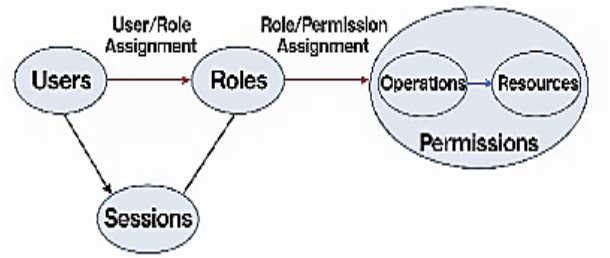

Fig. 3. Role-Based Access Control (RBAC) Model Showing User, Role, Session, and Permission Assignments.

D. Zero Trust Architecture (ZTA)

Zero Trust Architecture is predicated on the idea of “never trust, always verify”. It is especially relevant to open and heterogeneous IoT ecosystems (e.g., environments comprising various computing devices from many different vendors). ZTA requires continuous authentication, authorization, and monitoring of every network communication, regardless of the origin of the communication [28]. Differently from perimeter security approaches [29], ZTA assumes every network element is compromised. Its use with IoT is based upon robust identity management, micro-segmentation, secure gateways, and token-based authentication, which lessen lateral movement through networks.

V. Literature Review

The literature review section explores recent advancements in IoT, highlighting innovations in blockchain-based security, sustainable device development, next-gen communication protocols, 5G integration, ERP-based automation, and strategic IoT threat management, offering insights into building scalable, secure, and efficient IoT systems.

Zhang et al. (2025) suggested an architecture for IoT security based on blockchain that includes a wallet component, Smart Contract Component, Multi-Layer Security Component, and Common Component. This framework, designed for resource-constrained environments and embedded into cellular communication modules, enables multi-end offloading of computational tasks and secure transmission for IoT devices. Experimental results show that the data processing capability of the decentralized network architecture based on this framework is improved by 115.06% compared to traditional methods, thereby enhancing IoT decentralization and increasing the security and independence of IoT devices. This provides a valuable reference for designing next-generation IoT security architectures [30].

Let et al. (2024) recommend implementing an ERP (enterprise resource planning) system and automating campus transportation procedures. Permit administration, legal document maintenance, and digital record storage are all made possible by the ERP system. Furthermore, addressed were the

usage of RFID tags to track vehicle entry and leave and an alert system to notify consumers of upcoming transport services. The advantages of automating campus transportation operations, including better effectiveness, lower costs, and higher-caliber services, are highlighted in this study [31].

Moons et al. (2024) accomplished the traditional random-access scheme's connection density and energy efficiency using innovative grant-free and quick uplink access methods. Findings reveal that optimal random-access schemes can support three times as many devices as grant-free schemes and therefore perform the best in terms of connection density. However, when it comes to energy efficiency, random access performs the worst, with energy consumption up to 12 times higher than grant-free schemes. Fast-uplink access fulfills its expectations as the most promising technique for next-generation IoT communication, supporting a connection density twice as high as grant-free access at similar power consumption [32].

Rahmani et al. (2023) provided viable answers to some of the primary underlying issues in the development of environmentally friendly electronics for the future, with an emphasis on wireless connection, sustainable powering, and eco-friendly manufacturing for IoT devices. Industrial automation, wearable technology, self-driving cars, and smart cities are just a few of the IoT applications that are driving the growth of IoT systems. In recent years, wireless connection options, powering methods, and manufacturing processes have seen a paradigm shift due to the various application-specific system requirements and the quickly expanding number of IoT devices. Discuss how to power IoT devices sustainably by using wireless power transmission and energy harvesting, look at environmentally friendly production techniques for IoT devices of the future and provide biodegradable and environmentally friendly substitutes for existing materials [33].

Kar et al. (2021) have demonstrated that the suggested 5G-IoT architecture may provide scalable next-generation smart systems with ultra-high reliability, sub-millisecond latency, and high throughputs of about 1 Gbps. Next-generation 5G networks are essential for industrial verticals and emerging IoT applications to meet the increasing demands for high throughput and highly dependable low-latency connections. For a variety of applications, including different mobility situations, future IoT services also need to be highly scalable and have an Internet connection. The requirements of IoT applications have not yet been fully satisfied by communication solutions. But 5G can meet these demands and offers essential enabling technologies for the widespread use of IoT. [34].

Park and Ahn (2021) IoT-related mishaps and DDoS assaults are being recorded, and the area of cyber threat detection is growing. As a result, this study has looked at the degree of IoT standardization as well as developments in IoT technology commercialization and expansion. Based on the IoT reality that this technique investigated, research and analysis on the essential elements for IoT security management were then conducted, and an IoT security control plan was ultimately supplied. Using the basic strategy framework of "Pre-response-accident response-post-response," the Internet of Things environment was divided into three groups: IoT networks and communication, IoT devices, and IoT platforms and services. The appropriate strategic course for security control was then established for each of these groupings [35].

Table I presents a summary of the literature review, A Review on Smart Devices, Networking Technologies and Security in Next-Generation IoT Systems, highlighting each study's focus, strategy, important discoveries, difficulties, and suggested future paths.

TABLE I. COMPARATIVE ANALYSIS FOR LITERATURE STUDIES BASED ON SMART DEVICES, NETWORKING TECHNOLOGIES AND SECURITY IN NEXT-GENERATION IOT SYSTEMS

Reference	Study On	Approach	Key Findings	Challenges	Future Direction
Zhang et al. (2025)	IoT Security Framework	Blockchain-based framework with Wallet, Smart Contract, and Multi-Layer Security components	Improved data processing by 115.06%, enhanced security, autonomy, and decentralization of IoT	Resource-constrained environments	Design of scalable, secure, decentralized IoT architectures
L et al. (2024)	Smart Campus Transportation	Automated ERP system with RFID and alert features	Increased efficiency, reduced costs, better service quality	Integration of IoT with existing systems	Full automation and monitoring of campus logistics
Moons et al. (2024)	IoT Access Technologies	Comparison of random-access, grant-free, and fast-uplink access schemes	Random access has higher density but lowest energy efficiency; fast uplink offers best performance balance	High energy consumption in conventional access schemes	Optimize access methods for both density and energy efficiency
Rahmani et al. (2023)	Sustainable IoT Devices	Review of eco-manufacturing, sustainable powering, and connectivity	Biodegradable materials and energy harvesting are viable; paradigm shift in IoT design	Scalability of sustainable manufacturing	Development of fully eco-friendly IoT systems
Kar et al. (2021)	5G-enabled IoT Systems	5G-IoT architecture with ultra-low latency and high reliability	1 Gbps throughput, sub-ms latency, scalable systems	Existing networks inadequate for IoT needs	Expand 5G deployment for comprehensive IoT integration

Park and Ahn (2021)	IoT Security Control Strategy	Pre-response, accident-response, and post-response spanning device, network, and platform levels comprise the strategic framework	Clear security control directions for each IoT layer; standardization analysis	Lack of standardizatio n, frequent DDoS threats	Refined IoT security frameworks and proactive threat detection

VI. Conclusion And Future Work

The convergence of smart devices, intelligent networking technologies, and adaptive security frameworks drives the rapid advancement of next-generation IoT systems. These foundational elements are crucial in building responsive, scalable, and secure IoT environments that cater to the growing demands of modern applications. This review provides an in-depth understanding of how these components interact to shape the future of IoT ecosystems. The integration of intelligent hardware, low-latency communication protocols, and AI-driven network management is redefining the state of automation and connection in industries including smart cities, healthcare, and agriculture. The shift toward edge computing, decentralized architectures, and adaptive security measures, including blockchain and zero trust, underscores the need for scalable and secure IoT infrastructures. These innovations support the development of smarter, autonomous systems that offer real-time insights and improved user experiences while addressing challenges like interoperability, energy efficiency, and data privacy.

Future research should focus on context-aware, self-learning IoT systems using edge AI and federated learning, and develop unified standards for interoperability. Further work is needed on integrating AI/ML for predictive security, lightweight cryptographic protocols, and context-aware access controls. Research into sustainable energy models and AI-driven lifecycle management is also essential for ensuring long-term reliability and eco-efficiency.

References

[1] Z. H. Ali, H. A. Ali, and M. Badawy, "Internet of Things (IoT): Definitions, Challenges, and Recent Research Directions," *Int. J. Comput. Appl.*, vol. 128, pp. 975–8887, 2015.

[2] U. Khalil, O. A. Malik, M. Uddin, and C.-L. Chen, "A Comparative Analysis on Blockchain versus Centralized Authentication Architectures for IoT-Enabled Smart Devices in Smart Cities: A Comprehensive Review, Recent Advances, and Future Research Directions," *Sensors*, vol. 22, no. 14, Jul. 2022, doi: 10.3390/s22145168.

[3] S. C. Mukhopadhyay, S. K. S. Tyagi, N. K. Suryadevara, V. Piuri, F. Scotti, and S. Zeadally, "Artificial Intelligence-Based Sensors for Next Generation IoT Applications: A Review," *IEEE Sens. J.*, vol. 21, no. 22, Nov. 2021, doi: 10.1109/JSEN.2021.3055618.

[4] Y. Chen, Y. A. Sambo, O. Onireti, and M. A. Imran, "A Survey on LPWAN-5G Integration: Main Challenges and Potential Solutions," *IEEE Access*, vol. 10, 2022, doi: 10.1109/ACCESS.2022.3160193.

[5] R. Patel, "Security Challenges In Industrial Communication Networks: A Survey On Ethernet/Ip, Controlnet, And Devicenet," *Int. J. Recent Technol. Sci. Manag.*, vol. 7, no. 8, pp. 54–63, 2022, doi: 10.10206/IJRTSM.20251717.

[6] Gopi, "Zero Trust Security Architectures for Large-Scale Cloud Workloads," *Int. J. Res. Anal. Rev.*, vol. 5, no. 2, pp. 960–965, 2018.

[7] M. Menghnani, "Modern Full Stack Development Practices for Scalable and Maintainable Cloud-Native Applications," vol. 10, no. 2, 2025, doi: doi.org/10.5281/zenodo.14959407.

[8] D. Buil-Gil *et al.*, "The digital harms of smart home devices: A systematic literature review," *Comput. Human Behav.*, vol. 145, Aug. 2023, doi: 10.1016/j.chb.2023.107770.

[9] A. R. Neto, B. Soares, F. Barbalho, and L. Santos, "Classifying Smart IoT Devices for Running Machine Learning Algorithms," 2018, doi: 10.5753/semish 2018.3429.

[10] M. A. Y. Shaikh and M. S. H. Shaikh, "Internet of Things (IoT): Smart Living and Lifestyle," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 2, no. 9, pp. 379–383, Jun. 2022, doi: 10.48175/IJARSCT-5358.

[11] D. Patel, "Zero Trust and DevSecOps in Cloud-Native Environments with Security Frameworks and Best Practices," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 3, no. 3, pp. 454–464, Jan. 2023, doi: 10.48175/IJARSCT-11900D.

[12] S. Garg, "Predictive Analytics and Auto Remediation using Artificial Intelligence and Machine learning in Cloud Computing Operations," *Int. J. Innov. Res. Eng. Multidiscip. Phys. Sci.*, vol. 7, no. 2, 2019.

[13] B. Baker, J. Woods, M. J. Reed, and M. Afford, "A Survey of Short-Range Wireless Communication for Ultra-Low-Power Embedded Systems," *J. Low Power Electron. Appl.*, vol. 14, no. 2, p. 27, May 2024, doi: 10.3390/jlpea14020027.

[14] T. M. Ghazal *et al.*, "IoT for Smart Cities: Machine Learning Approaches in Smart Healthcare A Review," *Futur. Internet*, vol. 13, no. 8, p. 218, Aug. 2021, doi: 10.3390/fi13080218.

[15] P. P. Ray, "A survey on Internet of Things architectures," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 30, no. 3, pp. 291–319, Jul. 2018, doi: 10.1016/j.jksuci.2016.10.003.

[16] D. Mocrii, Y. Chen, and P. Musilek, "IoT-based smart homes: A review of system architecture, software, communications, privacy and security," *Internet of Things*, vol. 1–2, pp. 81–98, Sep. 2018, doi: 10.1016/j.iot.2018.08.009.

[17] S. Chacko and M. D. Job, "Security mechanisms and Vulnerabilities in LPWAN," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 396, Aug. 2018, doi: 10.1088/1757-899X/396/1/012027.

[18] A. Hakiri, A. Gokhale, P. Berthou, D. Schmidt, and T. Gayraud, "Software-Defined Networking: Challenges

and research opportunities for Future Internet," *Comput. Networks*, vol. 75, 2014, doi: 10.1016/j.comnet.2014.10.015.

[19] M. Merenda, C. Porcaro, and D. Iero, "Edge Machine Learning for AI-Enabled IoT Devices: A Review," *Sensors*, vol. 20, no. 9, Apr. 2020, doi: 10.3390/s20092533.

[20] S. Pandya, "Innovative blockchain solutions for enhanced security and verifiability of academic credentials," *Int. J. Sci. Res. Arch.*, vol. 6, no. 1, pp. 347–357, Jun. 2022, doi: 10.30574/ijsra.2022.6.1.0225.

[21] L. P. Rachakonda, M. Siddula, and V. Sathya, "A comprehensive study on IoT privacy and security challenges with focus on spectrum sharing in Next-Generation networks (5G/6G/beyond)," *High-Confidence Comput.*, vol. 4, no. 2, p. 100220, 2025, doi: 10.1016/j.hcc.2024.100220.

[22] V. Shah, "Scalable Data Center Networking: Evaluating VXLAN EVPN as A Next-Generation Overlay Solution," *Asian J. Comput. Sci. Eng.*, vol. 8, no. 04, 2023, doi: https://doi.org/10.22377/ajcse.v8i04.237.

[23] I. Kuzminykh, M. Yevdokymenko, and V. Sokolov, "Encryption Algorithms in IoT: Security vs Lifetime," *SSRN Electron. J.*, 2023, doi: 10.2139/ssrn.4636161.

[24] I. I. Al Barazanchi and W. Hashim, "Enhancing IoT Device Security through Blockchain Technology: A Decentralized Approach," *SHIFRA*, vol. 2023, pp. 10–16, Feb. 2023, doi: 10.70470/SHIFRA/2023/002.

[25] H. Kali, "The Future Of Hr Cybersecurity: Ai-Enabled Anomaly Detection In Workday Security," *Int. J. Recent Technol. Sci. Manag.*, vol. 8, no. 6, pp. 80–88, 2023.

[26] J. Mishra, "Design and Development of IoT-Enabled Smart Medicine Box for Medication Management System," 2025

[27] M. Blessing, "Role-Based Access Control (RBAC) for IoT Devices: Enhancing Security in a Connected World," 2024.

[28] F. Federici, D. Martintoni, and V. Senni, "A Zero-Trust Architecture for Remote Access in Industrial IoT Infrastructures," *Electronics*, vol. 12, no. 3, Jan. 2023, doi: 10.3390/electronics12030566.

[29] N. Prajapati, "Federated Learning for Privacy-Preserving Cybersecurity : A Review on Secure Threat Detection," pp. 520–528, 2025, doi: 10.48175/IJARSCT-25168.

[30] L. Zhang, L. Hang, K. Zu, Y. Wang, and K. Yang, "Constructing Next-Generation IoT Security: Embedded Smart Contracts and Multi-Layer Security Protection," *IEEE Internet Things J.*, p. 1, 2025, doi: 10.1109/JIOT.2025.3541256.

[31] P. L, P. K, K. P, and G. V, "IoT-based Next Generation Campus Management System for Transport and Entry Tracking," in *2024 8th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, IEEE, Oct. 2024, pp. 204–211. doi: 10.1109/I-SMAC61858.2024.10714705.

[32] L. Moons, S. Nasser, A. Sabovic, R. K. Singh, and J. Famaey, "Evaluating Fast and Grant-Free Uplink Access in Next-Generation Cellular IoT Networks," in *2024 3rd International Conference on 6G Networking (6GNet)*, 2024, pp. 19–24. doi: 10.1109/6GNet63182.2024.10765754.

[33] H. Rahmani *et al.*, "Next-Generation IoT Devices: Sustainable Eco-Friendly Manufacturing, Energy Harvesting, and Wireless Connectivity," *IEEE J. Microwaves*, vol. 3, no. 1, pp. 237–255, 2023, doi: 10.1109/JMW.2022.3228683.

[34] S. Kar, P. Mishra, and K.-C. Wang, "5G-IoT Architecture for Next Generation Smart Systems," in *2021 IEEE 4th 5G World Forum (5GWF)*, 2021, pp. 241–246. doi: 10.1109/5GWF52925.2021.00049.

[35] W. Park and G. Ahn, "A Study on the Next Generation Security Control Model for Cyber Threat Detection in the Internet of Things (IoT) Environment," in *2021 21st ACIS International Winter Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD-Winter)*, 2021, pp. 213–217. doi: 10.1109/SNPDWinter52325.2021.00053.

