



The Evolution of the Internet of Things (IoT) and Smart Networks: From Inception to Intelligent Edge Computing

Elpitiya Badalge Don Sanjaya Samudra^{a*}, Yasas Chamod Chamalka
Liyanapathiranage^b, Marasinghe Achchige Sithum Dineth Prabhashwara^c,
Weihenage Don Pasindu Buddhima^d, Ranathunga Gamaralalage Thiran Ranthila
Ranathunga^e, Maheshika Medhavi Vindya Senanayake^f

^{a,b,d,e,f}Department of Knowledge Engineering and Communication, Faculty of Computing, University of Sri
Jayewardenepura, Nugegoda, 10250, Sri Lanka

^cDepartment of Scientific Computing, Faculty of Computing, University of Sri Jayewardenepura, Nugegoda,
10250, Sri Lanka

^aEmail: sanjayasamudraelpitiya@gmail.com

^bEmail: yasaschamod1234@gmail.com

^cEmail: sithumdineth908@gmail.com

^dEmail: passbudd@gmail.com

^eEmail: thiranranathunga@gmail.com

^fEmail: vindya@sjp.ac.lk

Abstract

Today, the Internet of Things (IoT) is used in different fields like healthcare, agriculture, transportation, etc. Alongside, it investigates the Software-Defined-Networking (SDN), 5G/6G, edge computing, and other novel technologies and their impact on smart networks in terms of the performance, scalability, and operational intelligence of IoT systems. Therefore, this paper presents a timeline of milestones in history, beginning with early-stage Machine-to-Machine (M2M) communication and tracing the evolution to sophisticated edge Artificial Intelligence (AI) and technological growth related to IoT and smart networks. A discussion of the data processing architecture of IoT with sensor technology, challenges faced in modern applications, the analysis of current gaps

in research related to smart developments, emerging trends in IoT, and future directions is also explored in this study.

Keywords: Internet Of Things; Smart Networks; Edge Computing; 5G/6G; Artificial Intelligence; Software Defined Networking

* Corresponding author. Email address: sanjayasamudraelpitiya@gmail.com

1. Introduction

The Internet of Things, more commonly referred to through its ubiquitous acronym IoT, is a revolutionary and innovative technological paradigm that supports the interconnection of devices, rendering them not only connected but an essential part of a far larger and complicated network. A direct consequence of this immense interconnectivity is the new degree of interaction that is possible, most notably amongst the devices themselves and the ambience environment within which they function. While the idea of IoT was originally envisioned as a simple machine-to-machine (M2M) communication system, over time it has developed into a complex and heterogeneous collection of highly developed ecosystems that comprise an enormous range of connected smart devices, networks, and sophisticated artificial systems that have the capability of communicating with each other in a seamless fashion. With over 75 billion connected devices by 2025, the exponential growth of IoT deployment has completely changed how data is gathered, processed, and used across a wide range of applications, from industrial automation to smart cities. Significant issues with scalability, security, energy efficiency, and interoperability have arisen along with this technological evolution; these issues need to be thoroughly examined and analyzed in order to determine their implications for upcoming IoT deployments. This work provides comprehensive details of the IoT ecosystem's evolution for researchers and practitioners.

This study aims to give a detailed and comprehensive account of the historical progression as well as the wide range of technologies that underline IoT and smart networks, with a specific focus on the current shift towards intelligent edge computing, including the prominent developments within the arena of AI, along with identifying research gaps in the current IoT implementations to propose a framework. By synthesizing literature and emerging technologies, this document collates information from networking and protocol sensors, artificial intelligence, and new-age communication technologies to create a complete picture of the IoT ecosystem. Additionally, this review fulfills the important gap in the understanding of the technological convergence of 5G and 6G, edge computing, and artificial intelligence, which significantly transform the IoT, and the intelligent systems driven by them. Contributions of this review document include: (1) Detailed chronological compilation of the development of IoT beginning with M2M and ending with intelligent edge computing, (2) Comprehensive classification and review of competing networking and communication protocol systems, (3) compilation of the most relevant technological hindrances faced in the present day in IoT systems, and (4) a proactive outlining of prospective areas of investigation in sync with the emerging technological innovations and the needs of the IoT industry.

In order to ensure a clear and coherent presentation of this discourse, this paper has been organized as follows: Section 2 gives a descriptive explanation of the historical progression of IoT; Section 3 gives an overview of the range of networking paradigms and communication protocols that enable this degree of connectivity to be possible; Section 4 discusses the architecture relating to the processing of data, as well as the technology relating to sensors; Section 5 discusses the notion of smart networks and the evolution of the range of new technologies relating to this field; lastly, Section 6 gives a detailed overview of the current research work that is being conducted, discussing the issues that are faced as well as describing the range of potential scope for improvements that can be explored in the years to come.

2. The History and Early Age of IoT

The Internet of Things (IoT) idea came from the base technologies of Machine-to-Machine (M2M) communication, which emerged in the early 1980s when ATMs and telemetry systems employed modems for data transmissions without the need for human action [1]. M2M introduced stand-alone point-to-point connections also was often proprietary exclusive then limited to industrial use cases such as vehicle tracking and SCADA systems [2]. Kevin Ashton formally envisioned "IoT" in 1999, predicting a category of which in RFID tags could automate supply chains through linking tangible things to the internet [3]. This revolution enabled the development of IP-based infrastructures that expanded upon the originally limited M2M networks.

Commercial demands accelerated RFID and Wireless Sensor Networks adoption in the 2000s. Walmart's 2003 RFID tagging mandate cut supply-chain shortcomings by 30%, demonstrating IoT's potential for widespread use [4]. At the same time, academic projects like Smart Dust explored microsensors for ambient environmental monitoring. This research opened the age of ubiquitous detection [5].

By the 2010s, standardization efforts such as IEEE 802.15.4 (Zigbee) and IPv6 solved early interoperability and address exhaustion problems as they enabled IoT for billions of devices [6]. Yet, obstacles remained, including fragmented processes such as Zigbee. Elevated hardware costs continued as initial RFID tags cost more than \$1 per unit. Z-Wave also hindered business adoption [7].

The transition from M2M to IoT was both technology and concept based. M2M was concerned with the transmission of data communications, and the IOT integrated cloud computing, edge analytics and AI to create intelligent networks [8].

Today, the applications for IoT are from smart cities, wearables, to industrial automation while the ethical issues, such as data protection, and the inherited security threat from M2M system have not been fully addressed [9]. With the continued development of edge Computing and 6th generation networks, the boundary between M2M and IoT will be further altered, and number of connected devices will gradually reduce to the fabric of devices [10].

Table 1: ROI of RFID in Retail (2003–2010)

Metric	Pre-RFID	Post-RFID	Improvement
Inventory Accuracy	65%	95%	+30%
Labor Costs	\$2.1M/year	\$1.4M/year	-33%
Stockout Reduction	15%	5%	-10%

3. The Networking Paradigms and Communication Protocols

Internet of things (IoT) has seen a paradigm shift in the networking world with the types of processing that sensor and device data face. Although this transformation enhances the scalability and flexibility of networks, it brings new challenges. Local control is provided by a distributed system in which devices are capable of communicating

and operating independently of any one control point. But this transition complicates interoperability and security. Modern networking paradigms evolve due to advancements in connected devices; however, traditional networking approaches differ fundamentally. Research shows these decentralized IoT networks can enhance resilience by 60% alongside introducing room for more complex security challenges needing to be addressed in novel ways. This standards development cycle has been stimulated by organizations such as the Institute of Electrical and Electronics Engineers (IEEE) in its effort to promote a transition to IPv6, the most current version of Internet Protocol (IP). Advancements in modern IoT applications trigger the proliferation of expansive interconnected devices. These evolving networking paradigms need to be efficient and uphold security, while also addressing the distinct needs posed by contemporary IoT applications.

3.1. The move from centralized to decentralized networks

Centralized networks evolved from traditional client-server systems and have a greater tendency to rely on one central point of control. However, this faced some problems, such as it was too open to cyber-attacks, and cloud-based IoT platforms faced delay and privacy problems when managing a large number of devices. Existing research indicates that up to 95% of connected devices can be simultaneously affected by centralized IoT architecture's single points of failure. This in turn creates bottlenecks limiting the scalability to around 10,000 devices due to the existence of a single central controller.

Decentralized networks came as a response to these issues. It solved them by using distributed architectures like,

- Grid Computing – enabled sharing of resources between virtual organizations, but dynamic authentication is still an issue.
- Blockchains – greater transparency in credential management systems.
- Decentralized machine learning (DML) – Facilitated collaborative training of AI models without any centralized data pooling.

The benefits offered by distributed architecture such as enhanced fault tolerance and scalability account for the deployment of blockchain-based IoT networks. These networks enhance the incident response times by 40% in comparison to the traditional networks. Also, approaches utilizing decentralized machine learning can minimize the need for data transmission by as much as 80%. These practices mainly concentrate on how to become and stay reliable, meeting the needs of the current IoT age [11]. Decentralized structures pose new challenges, including more intricate network management, elevated computational requirements for consensus mechanisms, and more complex algorithms for distributed node routing if peak performance is to be sustained.

3.2. IoT protocols (MQTT, CoAP, LoRaWAN, Zigbee)

Selecting the proper communication protocols affects the performance of the whole IoT system, as one protocol may have benefits and drawbacks depending on application needs, network topology, and device limitations. In the comparison study of these protocols, power consumption, latency, and scalability metrics seemed to vary most which are some of the critical metrics of the system performance and cost.

- MQTT is ideal for regions with slow internet but requires an extra security layer like TLS to have in-built encryption. MQTT is the most efficient for the publish-subscribe architecture. Typical message overhead is only 2 bytes which means that it is useful for low bandwidth environments and can handle up to 65,000 clients per broker.
- CoAP performs well on small devices and has excellent signal reliability on mobile robots but performs poorly in larger networks. While CoAP is limited in scalability with networks greater than 1,000 nodes due to congestion control, its RESTful architecture and use of UDP results in 50% lower latency than HTTP-based competitors.
- LoRaWAN use sub gigahertz frequencies which can enable rural deployments.
- Zigbee is appropriate for mesh networks but can face interference problems in dense 2.4GHz environments [12].

Table 2: Communication Protocols

Protocol	Transport Layer	Range	Data Rate	Power Consumption	Primary Use Cases
MQTT	TCP	Network dependent	Up to 256 MB	Moderate	Home automation, Industrial IoT
CoAP	UDP	Network dependent	Optimized for small payloads	Low	Smart cities, Resource-constrained IoT
LoRaWAN	LoRa PHY	2-15 km	0.3-50 kbps	Very Low	Rural connectivity, Asset tracking
Zigbee	IEEE 802.15.4	10-100 m	20-250 kbps	Low	Home automation, Healthcare

3.3. The function of IPv6 in IoT scalability

IPv6 can enable end-to-end connection for large number of devices. Its simplified header can minimize the overhead by nearly 40% compared to IPv4, which makes it a necessity for low-powered devices. By using the 6LoWPAN standard (RFC 4944), we can squash IPv6 packets down small enough to fit on IEEE 802.15.4 networks. The switch to IPv6 is critical for accommodating an estimated 75 billion IoT devices by 2025. While IoT devices are built on IPv4, which only allows 4.3 billion addresses, IPv6 offers a staggering 2^{128} addressing space. This translates to virtually limitless device addressing capabilities. Also, IPv6 supports seamless device onboarding by minimizing configuration delays [13]. According to performance analysis, 6LoWPAN compression offers the capability to shrink the IPv6 header overhead from 40 bytes to 2 bytes for IoT communications. This could enhance energy efficiency by 25% in resource-constrained devices while also improving efficiency in spectrum usage in wireless sensor networks.

3.4. The standardization efforts (IEEE, IETF)

IEEE standards specify Zigbee's physical layer, which has been optimized for 250 kbps data speed and AES-128 encryption. IETF specifies application-layer protocol rules:

1. CoAP (RFC 7252) employs DTLS for secure data transport.
2. MQTT-SN optimizes MQTT for sensor networks by compressing topic IDs.

The actions of the organizations are crucial for achieving unifying interfaces across diverse IoT systems. In particular, IoT devices built on 802.15.4 can support multiple higher-layer protocols which expand the cross-manufacturer device interoperability. And groups like IETF's 6LoWPAN working on IoT stack interoperability along with energy efficiency and spectrum planning [12]. The collaborative approach to standardization has proven to be effective, yielding positive results with protocol efficiency. In particular, the update to CoAP reducing message exchange overhead by 35%, and MQTT-SN achieving 60% compression on topic identifiers are great examples of battery life and network performance improving in large scale deployments.

4. The Data Processing Architecture and Sensor Technology

4.1. The overview

IoT sensors are the bridge between the real world and digital world. The global IoT sensor market has grown heavily with more than \$21.2Billion globally in 2023 and is projected to grow further over \$54 billion by year 2030 owing to rise of real time data collection and smart automation through diverse industries. In the world there is a variety of different types of sensors that can be used for different types of purposes. Modern IoT applications integrate multiple sensor types in their systems; while smart buildings generally use 15-20 different sensors categories, for monitoring and control industrial facilities can involve over 100 sensors per production line.

4.2. The key sensors technologies

There are various key sensor technologies depending upon the user requirements. This section of the paper explains the details of different sensor technologies used in modern developments.

Conventional Sensors are analog in nature such as thermocouples, strain gauges and photodiodes that require signal conditioning and A/D conversion external to the sensor. Most of these sensors offer 12–16-bit resolution and require extra circuitry costing \$15–\$30 per channel. This makes them ideal for projects where precision matters more than cost, delivering temperature readings accurate to $\pm 0.1^{\circ}\text{C}$ and strain measurements precise to just 1 microstrain.

Digital Sensors such as DS18B20 temperature sensors and ADXL345 accelerometers provide digital outputs directly with their own microprocessor and standard protocols (I2C SPI) [14]. By removing the need for external ADCs and including built-in calibration, digital sensors can lower total system costs by 25–35%. They also provide standardized communication interfaces, making it easier to connect them with microcontrollers and IoT gateways.

MEMS (Micro-Electro-Mechanical Systems) is one of the advanced technologies developed, that combines

mechanical and electrical elements on the same chip, and deployed in inertial measurement, environment monitoring, and medical devices [15]. Smart Sensors integrate sensing elements with onboard microprocessors, memory, and wireless communication for self-calibration, adaptive sampling, and local data processing [16].

4.3. The evolution of data processing architecture

As time goes by, the processing of data has become very sophisticated. One of the key transformations is the change from central high order to distributed edge architectures. To address the major issues of latency, bandwidth, and scalability, edge computing has been evolving as an alternative to the traditional centralized computing system.

In Edge Computing, the information computation need of sensor node can be provided immediately, It can not only avoid high cost of network traffic but also increase the system's response time. Before such processed results are sent to higher level systems, edge nodes filter, aggregate and perform some preliminary processing on the data [17].

Fog Computing generalizes the concept of the edge by introducing intermediary computing layers between edge devices and cloud infrastructure to enable local data aggregation and hierarchical processing in large-scale IoT deployments [18].

4.4. Applications and challenges

IoT is a multitudinous phenomenon, where their multiplicity of applications considering the advances in technology. Intelligent agriculture here on this platform, smart cities, or home automation are some of the major cases where IoT is applied to make life easier. Almost all sectors have current IoT implementations, the largest being Manufacturing (23%), Transportation (18%), and Energy/Utilities (15%), which together account for over \$180 billion IoT spending worldwide per year. Nevertheless, the IoT also carries considerable challenges. One of the biggest challenges is that IoT systems can be hacked by security hackers, which can result in data breaches and system crashes. The higher automation that comes with IoT can add to joblessness and lack of physical efforts. Recently released cybersecurity reports claim that IoT devices undergo an average of 5,200 attacks each month. Moreover, considering 98% of IoT device traffic that goes unencrypted, there is a clear need for multi-layered security systems and devices with strong IoT authentication safeguards.

Examples of important application areas are smart cities (traffic monitoring, environmental management), Industrial IoT (predictive maintenance, process optimization), healthcare (continuous patient monitoring), environmental sensing (climate research, pollution tracking) [19]. Looking at these applications with a quantitative approach shows significant improvements in performance. For instance, with IoT assisted traffic control systems, smart cities are experiencing a 20-30% decrease in traffic congestion. Additionally, the industrial sector is taking advantage of IoT with predictive maintenance, reducing unplanned downtime by 25-40%. Lastly, in the healthcare sector, IoT enabled systems are improving patient outcomes by 15-20% through the ability to constantly monitor.

The important issues related to WSNs consist of scalability in large-scale networks, interoperability among heterogeneous devices, security, energy constraint (conscious) and efficiency, and sensitivity in distributed systems [20]. Safety-critical applications need advanced edge-processing, especially owing to real-time processing needs [21].

4.5. The future directions

The next IOT is driven by even more AI, enabled by connectivity through even more advanced technologies like 5G and further, and with more emphasis on security and privacy. The ability to process AI at the edge strategically redefines IoT architecture. Moreover, there are projections that indicate that 75% of data generated by enterprises will be processed outside of the data centers by 2025, thus needing a reconfiguration of distributed intelligence and self-governing frameworks.

Some of the emerging trends are the integration of AI at sensor level for local learning and pattern recognition, 5G connectivity for ultra-low-latency and ultra density, and the provision for autonomous sensor networks having self-organizing and self-healing capabilities [22]. Federated learning methods provide a cross-cutting solution for collaborative learning without centralized data sharing, while quantum sensing techniques can bring unprecedented measurement sensitivity for future uses [23].

5. The Emergence and Impact of Smart Networks

In the present era of the Internet of Things (IoT), Smart networks are evolving the methods devices, and users are communicating and interacting. Yang in 2020 in a review that discusses the recent progress in artificial intelligence (AI), edge computing, software defined networking (SDN) and communication techniques of 5G/6G wireless to show how it has a combined impact in the development of intelligent, agile and scalable networks. Summary of effects and significance of the above technologies The impact of the above technologies when viewed in context to the smart network and its representative elements playing a role in the cascading effects. The forecast of huge penetration of the IoT solutions soon gains momentum and there is a necessity of coming up with intelligent frameworks. With more implementations of IoT framework being adopted, the demand for industrial intelligence-based adaptive mechanisms is increasing. The set architectures are obsolete, they can't keep up with the growing volume of data which require prosthetics, and their variety and speed are constantly increasing along with the connections of manifolds of different devices and systems together. New networking technologies such as Software-Defined Networking (SDN), advanced mobile communication networks (5G/6G), edge computing, and Artificial Intelligence (AI) are proving to be decisive factors for facilitating efficient, real-time, adaptive, and progressive communication [24].

SDN employs the control plane and data plane separation to realize the centralized and programmable network control in the network in a software way. Flexibility enhances the ability to modify the network behavior dynamically based on traffic and device interactions. For IoT, SDN can offer dynamic addition or removal of devices and network path at runtime, which is required to cope with the heterogeneous communication requirements of massive device ecosystems [25].

The move from 5G to 6G represents an order of value for improvement in what networks can perform. 5G networks have a very high bandwidth compared to 4G, ultra-low latency (less than 1 millisecond) and a range of one million devices per square kilometer [26]. These are features that make 5G ideal for the IoT in cities where people are concentrated in smart cities, in cars with autonomous vehicles and in industry with industrial automation.

The 6G will capture more advantages regarding speed and reliability, with satellite-terrestrial systems utilized to boost mile coverage and intelligent resource management around the world [27].

In edge computing, what needs to be done is perform near the data rather than sending that data to the cloud. This is very critical and crucial when considering an example like this, in teleoperation for data for surgery and factory automation, where every millisecond is very precious for the purpose and this could solve the problem. Edge computing could locally filter and make a response, which can be more timely response and can alleviate the burden of cloud network [28].

AI is rendering the networks intelligent through technologies like predictive analytics, anomaly detection, and decision making. AI of SDN can even avoid congestion by diverting traffic in advance of a problem [29]. It is beneficial for 5G/6G systems in terms of greater dynamic resource provisioning as well as spectrum utilization. The edge AI pushes towards greater community independence when making selections, the devices that connect and network systems simply act independently without any human involvement [30].

The Rise of SDN co-rides with 5G/6G, edge computing and AI together constitute a New Generation of Smart Networks. That renders these systems the most flexible, the most powerful and the most "tunable." However there remain issues to resolve regarding interoperability, security, energy efficiency, standardization and many more. More work needs to be carried out to tackle the challenges of FASONS [31].

If utilized to construct SDN, 5G/6G infrastructure, edge computing and AI intelligent network, the structure of digital infrastructure would change. Their combination has the potential to combine efficient and effective communication and information systems that can even automatically adapt to the new IoT environments. They will have a great impact on health care, manufacturing, and other fields, which are associated with the human-machine interface [32].

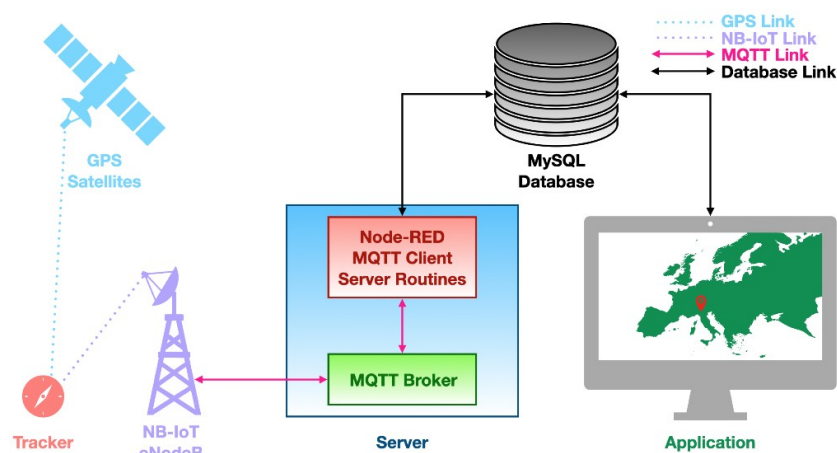


Figure 1: AI Use in Network Operations

6. Current Trends, Challenges, and Future Directions in Research

6.1. *Current research trends*

6.1.1. AI-enabled IoT

AI and IoT and the disruption of industries Both AI and IoT are changing the face of industries around the world, enabling rapid data analysis and better decision making. This shift naturally leads to faster response times and consequently improves the operational performance of systems in practical applications. AI-based sensors in smart home and healthcare environments are able to monitor the vital signs of patients and to timely inform the medical personnel of any irregularity. Processing data at the edge eliminates the reliance on remote servers, which reduces the likelihood of errors. Further, the combination results not only in conservation of bandwidth since there is local information processing close to the device which diminishes the cost of data access but also reduces network traffic. Data privacy is also a concern and keeping sensitive data locally prevents exposure to cybercrime. Such systems provide personal services, where AI analyzes users', individual requirements based on real-time data feeds. Also, processing data at edge protects device batteries and reduces load on network infrastructure, contributing to overall lower running costs. Advanced AI methods are employed in these systems, for example, deep neural networks and convolutional neural networks. [33].

6.1.2. 5G and 6G integrated sensing and communication.

With the development of the 5th and 6th generation networks, coupled with the Internet of Things (IoT), real-time data transmission has been greatly improved. 5G and 6G networks enable devices and sensors to be able to not just connect but communicate data quicker, on lower latency connections, and with more reliability. The new devices are important for auto-driving, tele-medicine and other applications for high-speed data transmission. Combined with the penetration of the internet of things (IoT), 5G and 6G improve the connectivity of a world with the high dependency relationship, to accelerate and stabilize the communications among machines and machines, and between man and machines, and so the industrial and interpersonal aspects of life and working are revolutionized [34].

6.1.3. Modern agriculture

The agricultural sector has changed dramatically with the introduction of IoT (Internet of Things), allowing devices and sensors to be interconnected and share information in real time. Precision agriculture, smart irrigation, animal monitoring and supply chain are just some of the sectors completely reinvented with the help of IoT technologies. Precision agriculture uses sensors that measure soil moisture and temperature and crop health to help growers make decisions when to irrigate, fertilize, and rotate crops. Smart irrigation controllers automatically tailor watering schedules to weather, soil conditions, and plant types, saving both water and money. These are technologies that are helping make farming more efficient, more sustainable, and more profitable, boosting yields, cutting waste, and saving natural resources [35].

6.2. Challenges

6.2.1. Zero Trust Architecture (ZTA) implementation in IoT

Increased attacks by hackers on Internet of Things (IoT) devices have mainly increased networks, and lack of security. These devices are particularly appealing to cyberhackers because they do not contain advanced features such as continuous authentication and strong access control schemes. Against these vulnerabilities, Zero Trust Architecture is deployed with the assumption that devices and users can be security threats and therefore any access should be authenticated with a specific mechanism fairly. Secondly, access restrictions are enforced based on the principle of least privilege, so that devices are only allowed to communicate with the required parts of the system. To realize a proper implementation of Zero Trust Architecture, it is important to keep on monitoring users and devices activities in order to identify potential cyber threats at their initial stage. However, concerns about scalability, resource allocation, and operations of devices are not addressed well as yet, indicating the necessity to resolve them with the continuing growth of the IoT ecosystems further enhanced through the deeper penetration of IoT devices in everyday life and various industries [36].

6.2.2. Energy: battery-free sensors

Small batteries or energy-harvesting systems are used in IoT devices, which have a constrained energy budget. To support efficiency, engineers construct both the hardware and the software to leverage ultra-low-power chips or energy-efficient sensors. Software includes power saving algorithms for longer battery life and provides better device optimization. But, the constraints of limited power resources, high communication cost, scalability, computational overload, and lack of standardization pose great challenges to design general solutions. Finding a tradeoff between local processing and energy efficiency is still an open issue. The heterogeneity of standards in devices and communication protocols also hinders the design of more comprehensive power saving mechanisms. Addressing these issues is particularly critical in deploying sustainable IoT solutions capable of effective operations in diverse scenarios [37].

6.2.3. Ethics: ownership of data (GDPR compliance)

IoT devices can collect humongous amounts of personal data without offering proper acknowledgment to individuals about this process. It is imperative that individuals are provided with the right and the option to alter and even delete such data whenever it is felt necessary or appropriate.

The General Data Protection Regulation, or GDPR, lays high priority on the need for open and transparent disclosure of the collection and usage of the data. It is necessary for the users to be aware of the different means through which their data is being handled, stored securely, and transferred from one platform to another. Most IoT devices contain AI-powered algorithms. Ethics call for privacy in AI processing. GDPR limits excessive data gathering [38].

7. Conclusion

The emergence of the Internet of Things (IoT) began with machine-to-machine (M2M) communication but has evolved greatly to involve advanced AI-based edge computing systems. Such evolution involves significant events like the usage of IPv6, decentralized networking, and 5G/6G. Although new protocols (such as MQTT and LoRaWAN), sensor technologies (like MEMS and smart sensors), and edge intelligence have directed to some scaling and lagging issues, severe challenges related to security, collaboration, and the ethical use of AI over time. Our research indicates that there are considerable advancements such as the 70-80% reduction in bandwidth through edge computing as well as smart sensors' 90% improvement in energy efficiency. However, there are still issues with the standardized security frameworks, seamless interfacing with heterogeneous devices, and large-scale deployment models that are designed to be more sustainable.

The in-depth analysis of the structures of networking shows us that the process between centralized and decentralized changes the design concepts of IoT systems entirely. Decentralized networks, while enhancing resilience, tend to make security management and uniform protocol more challenging. Positive trends such as 6G networks and blockchain-based trust models will require collaboration across fields to realize energy efficiency, data privacy, and standardization. With the integration of other new developments such as anomaly detection with AI-empowered sensors, 5G networks that can support 1 million devices in under 1 kilometer, and federated learning reducing communication overhead, the following phase of IoT evolution will transform the networks edge with intelligence and autonomy.

As IoT becomes general in smart cities, healthcare, and manufacturing, future research must investigate new concepts and their societal implications to ensure that the next generation of IoT advances is robust and beneficial to humans and the environment as well. The results of the review are important to everyone, as they give a unique IoT history, its present technological complexity, and future priorities in connected smart systems for the next 10 years of research. It highlights the need for IoT ecosystem experts, as there are reinforcing 6G communication systems and quantum sensing, as well as neuromorphic computing, future deployment. It further states that cross-field work is needed to solve the many IoT scale problems of drone fleet management, national cybersecurity, and frameworks for smart cities. But ensures that the described reasoning of the need for global intelligent connectivity is attained.

References

- [1] J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645-1660, 2013.
- [2] V. Holler, J. Tsiatsis, C. Mulligan, S. Karnouskos and . D. Boyle, *Machine-to-Machine (M2M) Communication: Architecture, Performance and Applications*, Cambridge, U.K.: Cambridge University Press, 2014.
- [3] K. Ashton, "That 'Internet of Things' thing," *RFID Journal*, Jun 2009.
- [4] R. Want, "An introduction to RFID technology," *IEEE Pervasive Computing*, vol. 5, no. 1, pp. 25-33, 2006.
- [5] J. M. Kahn, R. H. Katz and K. S. J. Pister, "Next century challenges: Mobile networking for 'Smart Dust'," in

ACM MobiCom, Seattle, WA, USA, 1999.

- [6] IEEE, *IEEE Standard for Low-Rate Wireless Networks*, IEEE, 2011.
- [7] O. Vermesan et al., "Internet of Things strategic research roadmap," 2011.
- [8] M. E. Porter and J. E. Heppelmann, "How smart, connected products are transforming competition," *Harvard Business Review*, vol. 92, no. 11, pp. 64-88, Nov 2014.
- [9] R. H. Weber, "Internet of Things: Privacy issues revisited," *Computer Law & Security Review*, vol. 26, no. 1, pp. 23-30, Jan 2010.
- [10] W. Shi, J. Cao, Q. Zhang, Y. Li and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637-646, Oct 2016.
- [11] I. Foster, C. Kesselman and S. Tuecke, "The Anatomy of the Grid: Enabling Scalable Virtual Organizations," *International Journal of High Performance Computing Applications*, vol. 15, no. 3, pp. 200-222, Aug 2001.
- [12] H. Elayan, M. Aloqaily and M. Guizani, "Sustainability of Healthcare Data Analysis IoT-Based Systems Using Deep Federated Learning," *IEEE Internet of Things Journal*, vol. 9, no. 10, pp. 7338-7352, May 2022.
- [13] P. Herbke, T. Cory and M. Migliardi, "Decentralized Credential Status Management: A Paradigm Shift in Digital Trust," in *BRAINS (Blockchain Research & Applications for Innovative Networks and Services)*, Berlin, 2024.
- [14] S. Li, L. D. Xu and S. Zhao, "The Internet of Things: A survey," *Information Systems Frontiers*, vol. 17, no. 2, pp. 243-259, Apr 2015.
- [15] J. A. Stankovic, "Research directions for the Internet of Things," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 3-9, Feb 2014.
- [16] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347-2376, 2015.
- [17] W. Shi, J. Cao, Q. Zhang, Y. Li and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet of Things Journal*, vol. 3, no. 5, pp. 637-646, Oct 2016.
- [18] F. Bonomi, R. Milito, J. Zhu and S. Addepalli, "Fog computing and its role in the Internet of Things," in *1st ACM Mobile Cloud Computing Workshop (MCC)*, Helsinki, Finland, 2012.
- [19] A. Zanella, N. Bui, A. Castellani, L. Vangelista and M. Zorzi, "Internet of Things for smart cities," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 22-32, Feb 2014.
- [20] R. Roman, J. Zhou and J. Lopez, "On the features and challenges of security and privacy in distributed Internet of Things," *Computer Networks*, vol. 57, no. 10, pp. 2266-2279, Jul 2013.
- [21] N. Hassan, S. Gillani, E. Ahmed, I. Yaqoob and M. Imran, "The role of edge computing in Internet of Things," *IEEE Communications Magazine*, vol. 56, no. 11, pp. 110-115, Nov 2018.
- [22] X. Wang, Y. Han, V. C. Leung, D. Niyato, X. Yan and X. Chen, "Convergence of edge computing and deep learning: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 869-904, 2020.

- [23] T. Taleb, K. Samdanis, B. Mada, H. Flinck, S. Dutta and D. Sabella, "On multi-access edge computing: A survey of the emerging 5G network edge cloud architecture and orchestration," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 3, pp. 1657-1681, 2017.
- [24] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347-2376, 2015.
- [25] J. Hu, W. Bao, X. Wang and S. Leng, "Software Defined Networking with P4: Principles and Practices," *IEEE Network*, vol. 33, no. 5, pp. 98-104, Sept./Oct. 2019.
- [26] M. Agiwal, A. Roy and N. Saxena, "Next Generation 5G Wireless Networks: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 1617-1655, 2016.
- [27] W. Saad, M. Bennis and M. Chen, "A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems," *IEEE Network*, vol. 34, no. 3, pp. 134-142, May/Jun 2020.
- [28] F. Bonomi, R. Milito, J. Zhu and S. Addepalli, "Fog Computing and Its Role in the Internet of Things," in *ACM MCC Workshop on Mobile Cloud Computing*, 2012.
- [29] M. Chen et al., "Artificial Intelligence in Wireless Communications," *IEEE Wireless Communications*, vol. 27, no. 3, pp. 6-7, Jun 2020.
- [30] S. Wang et al., "Convergence of Edge Computing and Deep Learning: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 869-904, 2020.
- [31] R. Minerva, A. Biru and D. Rotondi, "Towards a Definition of the Internet of Things (IoT)," 2015.
- [32] Z. M. Fadlullah et al., "State-of-the-Art Deep Learning: Evolving Machine Intelligence Toward Tomorrow's Intelligent Network Traffic Control Systems," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2432-2455, 2017.
- [33] S. Yang et al., "Federated learning in the Internet of Things: A comprehensive survey," *Computers*, vol. 13, no. 3, pp. 1-25, 2024.
- [34] A. A. Nasir et al., "Integrated sensing and communications for IoT: Synergies with key 6G technology enablers," 2023.
- [35] O. Friha, M. A. Ferrag, L. Shu, L. Maglaras and X. Wang, "Internet of Things for the Future of Smart Agriculture: A Comprehensive Survey of Emerging Technologies," *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 4, pp. 718-752, Apr 2021.
- [36] C. Liu, R. Tan, Y. Wu, Y. Feng, Z. Jin, F. Zhang, Y. Liu and Q. Liu, "Dissecting Zero Trust: Research Landscape and Its Implementation in IoT," *Cybersecurity*, vol. 7, no. 20, May 2024.
- [37] T. V. Manohar and T. Dharini, "Energy Efficiency in IoT: Challenges, Techniques, and Future Directions," *IJIRT*, vol. 168, no. 552, pp. 1-10, 2024.
- [38] S. Wachter, "The GDPR and the Internet of Things: A Three-Step Transparency Model," *Law, Innovation and Technology*, vol. 10, no. 2, pp. 1-32, 2018.