Contents lists available at GrowingScience

International Journal of Data and Network Science

homepage: www.GrowingScience.com/ijds

Current developments, applications, challenges and future trends in internet of things: A survey

Maha Helal[a*]

[a]*College of Computing & Informatics, Saudi Electronic University, Riyadh 11673, Saudi Arabia*

C H R O N I C L E

Article history:
Received: July 6, 2024
Received in revised format: August 28, 2024
Accepted: September 18, 2024
Available online: September 18, 2024

Keywords:
Internet of Things
Wireless networks
Advanced technologies
Privacy
Security
Protocols

A B S T R A C T

The rapid digitalization in recent years has opened up many technological possibilities, gradually transforming various sectors and society as a whole. This digital shift has enabled advancements in a number of fields, leading to improved resource efficiency, systems and processes. The Internet of Things (IoT) refers to a system of interconnected devices that share information that exchange information with one another via the internet. IoT devices are now everywhere, found in applications ranging from unmanned aerial vehicles to smart home environments, from the Industrial Internet of Things to the Internet of Medical Things. The core concept of IoT revolves around establishing a seamless and intelligent communication ecosystem, facilitating interactions between devices over the internet. This is anticipated to create new opportunities for enhancing services in various societal sectors, such as transportation, farming and smart cities. However, IoT-based networks face limitations and challenges that hinder the realization of their full potential. This paper outlines these challenges and proposes solutions, emphasizing the importance of collaboration and innovation. The paper also anticipates future trends in IoT, particularly the integration of 5G connectivity, cloud computing and AI, and identifies areas for future research to address current challenges and explore new applications.

1. Introduction

Our lives are becoming increasingly digitalized, as new technologies are continuously invented and adopted. While there are some drawbacks to this technological progress, there is optimism about the upcoming digital revolution due to technologies becoming more affordable, convergent and innovative. The Internet of Things (IoT) is influencing both the present and future generations of the internet (Atzori et al., 2010). The main goal of IoT is to improve communication abilities between connected devices in different networks. This includes improving security aspects and mobility, making it available at any time and to everyone in various locations, as well as the development of new intelligent applications and services. The concept of IoT quickly developed into a crucial ecosystem, involving data, people, processes, objects and the internet are interconnected. Applications of IoT technology span various domains, including smart homes and education (Perera et al., 2014), healthcare (Islam et al., 2015), smart farming and agriculture (Talavera et al., 2017), smart industries (Javed et al., 2018), safety and intelligent transportation (Xu et al., 2014) and smart cities (Zhu et al., 2015), as well as the military (Fernández-Caramés & Fraga-Lamas, 2018a) and the financial sectors (Hassija et al., 2019). Such applications leverage IoT technology to improve the standard of living for individuals (Khairnar & Birari, 2018). The different applications leverage computing technologies, such as edge, fog, cloudlet and cloud computing, to store, process and analyse data. In IoT, data are crucial for decision-making and are often highly private and sensitive (Kuchuk & Malokhvii, 2024). IoT has the potential to revolutionize our lives and work environments, making them smarter and more

* Corresponding author.
E-mail address mhelal@seu.edu.sa (M. Helal)

ISSN 2561-8156 (Online) - ISSN 2561-8148 (Print)

doi: 10.5267/j.ijdns.2024.9.008

interconnected and responsive to our needs. Alongside its significant benefits, however, IoT presents challenges related to security, privacy, interoperability and data management that must be carefully addressed to ensure its widespread and secure adoption (Jatoi et al., 2023). IoT has emerged as a groundbreaking concept, effortlessly linking physical devices to enable communication, data collection and data exchange. Research has been undertaken to trace the origins of IoT, assess the main areas of study and address the challenges it will encounter. The progression of IoT technology is strongly connected to the support of associated theories and methodologies, leading to growing interest from both scholars and practitioners in its development. It is, therefore, an opportune moment to review and reflect on the progress and development of IoT. This paper offers a comprehensive review of the current trends in IoT literature, which includes the intersection of various emerging applications and interdisciplinary technologies. It seeks to advance the future of IoT development and research.

The structure of the paper is as follows. Section 2 offers an overview of IoT and Section 3 presents the technologies used in IoT-based networks. Sections 4 and 5 discuss IoT architecture and applications, respectively. Section 6 outlines the main challenges posed by IoT. Section 7 highlights research trends and opportunities and Section 8 concludes the paper.

2. IoT Background

2.1. Concept and Vision

The internet is now essential for the transmission of information (Bălău & Utz, 2017). However, the technology is evolving beyond the mere sharing of information to encompass data collection, data analysis and remote control via the internet, resulting in the emergence of IoT. IoT allows the collection, control, analysis and sharing of real-time data between physical, connected devices in such networks (Lin et al., 2017; Liu et al., 2020) with the aim of enhancing quality of life (Miori & Russo, 2017). The combination of 'internet' and 'things' signifies an innovative leap in information and communication technology (ICT): 'internet' emphasizes a vision focused on the internet within IoT, and 'things' accentuates a focus on the objects themselves. These visions are thus integrated into a unified framework in which diverse objects or things are interconnected (Bandyopadhyay & Sen, 2011). IoT is fundamentally a network that links various components, such as computers, machines, and users with unique IDs. This network allows data transmission without requiring direct interaction between humans or between humans and computers. This development marks a significant milestone in the information technology field and a step towards a modern technological revolution (Wanasinghe et al., 2020). IoT can also be defined as "things that are associated over the Internet" (Khanna & Kaur, 2020, p. 1687). This remarkable technology has impacts on our everyday lives (Rose, 2014). For example, it allows for the control of a broad array of devices, from household appliances such as refrigerators and air conditioners to entertainment systems such as TVs and even vehicles that can suggest the quickest and safest routes, all managed through smartphones as well as smartwatches (Haslett & Brown, 2018). IoT also influences various domains, such as healthcare, smart homes, agriculture, industrial automation (Industry 4.0), transportation systems, urban development, infrastructure monitoring, trade, environmental surveillance, and smart water management and power grids (Al-Fuqaha et al., 2015). IoT encompasses interconnected systems, sensors, automotive antennas and other components (Motlagh et al., 2016). With its capacity to generate and analyse large volumes of data, IoT plays a significant role in driving projects that are focused on big data analytics (Marjani et al., 2017), particularly by providing real-time data (Akbar et al., 2018). IoT is a dynamic infrastructure that uses sensing and network communication technology to establish connectivity everywhere, among people, machines and objects. Over the past several decades, the digital revolution has led to the development of this transformative technological framework. IoT facilitates seamless data exchange, marking a significant shift in the technological landscape (Miorandi et al., 2012). The total number of devices in IoT networks was forecast to reach 83 billion by 2024, which would see a significant rise from 35 billion in 2020. For example, the Industrial IoT (IIoT) sector alone, covering manufacturing, trade and farming, was projected to represent more than 70% of all IoT connections by the year 2024, with an expected 180% increase in IIoT units over the next four years (Rothmuller & Barker, 2020). It was also expected that the number of devices linked to the internet would reach 75.44 billion (Zhou et al., 2019), and the financial impact of IoT technology was expected to range from $2.7 trillion to $6.2 trillion by 2025 (da Cruz et al., 2018), underscoring the profound societal impact of IoT technology. These devices were also projected to generate approximately 80 zettabytes of data (GlobalDots, 2019).

The McKinsey Global Institute and the National Intelligence Council forecast that by 2025 commonplace items, such as food packaging, furniture and paper documents, would be integrated into the internet as nodes. This forecast highlighted the transformative potential of integrating technologies that interacted with the human environment. The merging of information technology and embedded technology was anticipated to propel the evolution of smart objects, which are pivotal to the vision of IoT (Asghar et al., 2015).

Indeed, IoT appears poised to become a pivotal technology. Smart and interconnected objects are envisaged as being able to gather enormous amounts of valuable data, facilitating informed decision-making, lowering expenses through automation in industrial and residential environments, tracking objects and materials, tracking assets and environmental conditions, and facilitating further efficient and advanced medical interventions.

2.2. History and Evolution

The evolution of the internet to the IoT has gone through several phases. The first, known as the pre-internet phase, allowed communication over fixed telephone lines and through the Short Message Service (SMS). Subsequently, mobile telephony devices upgraded the communication platform. The second phase enabled the transmission of large messages, such as emails with attachments, offering information and entertainment as primary functionalities. Furthermore, phase three, referred to as the internet of services, emphasized electronic applications, such as e-commerce and e-productivity tools. Phase four, the internet of people, saw the rise of social media platforms and many other media, such as Facebook, Orkut, Skype and YouTube. Previously independent devices are currently being interconnected through the internet and include machine-to-machine (M2M), person-to-machine, and person-to-person systems. This integration of data, processes, humans and things characterizes the Internet of Everything (IoE) (Evans, 2012a, 2012b). IoE is based on four foundational elements: people, data, processes and things. Unlike IoT, which focuses primarily on 'things', IoE extends to include business and industrial processes to enrich people's lives. IoT, IoE and Internet of Nano Things (IoNT) represent novel paradigms for integrating the internet into personal, professional and societal contexts (Miraz et al., 2015). They have the capability to gather and evaluate data in real time from millions of interconnected sensors, which can then be utilized to support both automated and human-centric processes. Differentiating between IoT, IoE and IoNT is seen as valuable for anticipating upcoming developments. Furthermore, these technologies offer additional benefits, such as assisting in the formulation of public policy objectives, promoting environmental sustainability and advancing economic and social goals (Bradley et al., 2013). Recently, IoT emerged as a technology with significant capabilities in respect of smart control, connecting various physical devices around the world to the internet for data sharing and reception. The introduction of cloud and fog computing has further advanced IoT, linking it to upcoming web revolutions, each technology driving the other forward. The merging of IoT and cloud computing has yielded numerous advantages as cloud platforms gain popularity among hardware and software developers for their user-friendliness and cost-effectiveness (Kaur et al., 2020). Researchers are striving to integrate artificial intelligence (AI) into interconnected devices, enabling the latter to make decisions and take actions with zero human intervention. Evaluating the functional capabilities of IoT without considering the continuous advancements and changes in the field may, therefore, lead to incorrect assessments. Furthermore, generative AI (GAI) has now been introduced, possessing the impressive capability to create new content such as digital films, audio, images and code, thereby profoundly affecting various domains (Zhang et al., 2023). By integrating GAI into contemporary IoT systems, a new paradigm known as GIoT is emerging. GIoT shows considerable promise for revolutionary applications across multiple fields. Through the synergy of advanced IoT and GAI technologies, GIoT has the potential to facilitate intelligent systems, optimize resource management, improve decision-making processes and enhance overall efficiency and sustainability across various sectors. The merging of GAI technologies with modern IoT represents a significant opportunity to reshape the IoT landscape (Wen et al., 2024).

3. IoT Technologies

Numerous facets of our everyday routines are currently linked wirelessly through compact, energy-efficient devices, such as radio-frequency identification (RFID) tags, near-field communication, Electronic Product Code (EPC) tags, mobile devices, and GPS. These are further supported by the evolution of sensor technology, actuators, embedded computing, M2M communication, and cloud computing. Implementing these technologies can extend the initial idea of IoT into the domains of ambient intelligence and autonomous management. The ongoing advancement of these technologies consistently introduces innovations to the IoT environment (Li et al., 2015). Outlining the technology of the IoT that shapes future-based innovations is a challenging task due to the multitude of inventions and discoveries all around us. Nonetheless, the technology can be explained by categorizing it into four distinct foundations: system hardware, software devices, communication routes, and platforms. IoT further distinguishes itself from other technologies in terms of its middleware (Sezer et al., 2018), hardware (Ojo et al., 2018) and cloud integration platforms (da Cruz et al., 2018). Sensors are particularly prominent among IoT hardware, as IoT devices frequently incorporate sensors on boards equipped with a microcontroller, microprocessor and network interface. The leading IoT hardware boards include Raspberry Pi and Arduino (Swamy & Kota, 2020). IoT technology also encompasses end nodes, edge computing, fog computing, cloudlets, and cloud computing, which collectively bring intelligence to IoT systems. Typically, sensors and signal-conditioning circuits are linked to end nodes, which are utilized in applications that demand the deployment of numerous high-resolution sensors to measure the physical conditions of the environment (Lu et al., 2018). IoT devices need to utilize sufficient communication bandwidth, data preprocessing and computation methods while fulfilling system design specifications, such as those relating to security, mobility, self-diagnosis, privacy management, availability and scalability. IoT contributes significantly to the creation of large volumes of data. Managing such a vast amount of data can be challenging due to limited resources and computing capabilities. Computing paradigms, such as cloudlets and cloud, fog and edge computing, have emerged to support the IoT data lifecycle, encompassing storage, preprocessing and analysis (Elazhary, 2019). IoT can also benefit from various low-power radio technologies, including Bluetooth, IEEE 802.15.4 (ZigBee), Z-Wave, Sigfox, Neul, and NB-IoT, as well as wired technologies such as Ethernet. These technologies enable seamless efficient communication over the internet, whereby IoT systems can benefit from using IPv6 to identify objects easily.

4. IoT Architecture

Various experts have proposed different structures for IoT, but no single architecture has to date been universally standardized by any organization. This is mainly due to each technology introducing a framework and advocating its own best practice (Sabella et al., 2019). All IoT applications require at least one sensor to collect data from the environment, as sensors form essential components of smart objects (Morais et al., 2019). IoT architecture generally includes multiple layers, spanning from the application layer at the top to the data acquisition layer situated at the bottom, with the internet layer serving as a common medium for communication in between. Several architectures have been introduced to provide a clearer understanding of the concept of IoT, with three- and five-layered architectures being used most prominently (Goyal et al., 2018; Zhong et al., 2015). The Institute of Electrical and Electronics Engineers (IEEE) also proposed a framework for an IoT architecture designed for smart cities and grid architecture standards developed between 2018 and 2019, respectively (IEEE Standards Association, 2018, 2019). The complexity of IoT arises from its heterogeneity and broad scalability requirements, particularly in addressing and delivering services. A successful IoT architecture should integrate devices, networks and applications in order for them to work together seamlessly, achieving intelligent outcomes that meet user acceptance criteria through the connection of diverse objects. This architecture typically consists of protocols and standards, as well as multiple layers of technologies that are crucial for facilitating connections in IoT. Currently, IoT architecture reviews tend to follow the OSI layer or TCP/IP model, often exemplified by three-, four- and five-layer architectures (Nižetić et al., 2020). The creation and implementation of self-healing and self-configuring architectures are essential in IoT. Researchers focus on IoT middleware architectures to deliver secure and real-time services for essential applications, including health tracking and disaster management systems. Any effective IoT architecture must encompass a diverse range of devices and technologies while being flexible enough to accommodate identification needs (such as RFID tags) as well as intelligent and smart objects. Furthermore, the IoT architecture should be able to integrate high volumes of data from multiple types of resources, recognize important characteristics, define relationships in the data, examine them against historical data and highlight insights to inform decision-making. The most widely recommended models consist of three- and five-layer architectures (Al-Fuqaha et al., 2015). A three-tier architecture comprises the following layers: (1) perception layer, (2) network layer, and (3) application layer (Yang et al., 2011; Zhang et al., 2012). A five-tier architecture extends this by adding business and middleware layers, thus: business, application, middleware, network, and perception layers (Khan et al., 2012).

Communication is vital for the exchange of both raw and processed data between IoT devices and to facilitate uninterrupted connectivity between endpoints at all times and in any location (Aqeel-ur-Rehman et al., 2013). IoT utilizes various communication models, including edge-to-edge, edge-to-gateway, edge-to-cloud, and back-end data-sharing models (Yu et al., 2018). This involves numerous protocols tailored to specific architecture layers, whether IP-based or non-IP-based. Both the global and local area networks used in IoT communication necessitate the management of mobility protocols based on IP, with IPv6 being favoured for its scalability and reliability. Communication between devices (inter-device and intra-device) occurs at the lowest layer of the architecture and frequently involves adapting access technologies. For instance, the IEEE 802.15.4 protocol is tailored to sustain extended lifecycles in low-power device communications. When choosing the correct communication technology, it is essential to take into account factors that will result in seamless communication, such as the rate of the data, interoperability, range of transmission, operating frequency, and bandwidth consumption. The application layer, situated at the highest level of the IoT architecture, handles application services that facilitate communication between IoT devices for users (Kumar & Mallick, 2018). It formats and presents data to end users through a range of protocols in the application layer, such as MQTT, CoAP, XMPP, DDS and RESTful/HTTP (da Cruz et al., 2019). IoT frequently utilizes existing hardware infrastructure, but new software development is necessary to ensure interoperability among diverse devices and to better manage the extensive data generated (Whitmore et al., 2015). One of the important elements of every IoT object is the operating system (OS), which serves as a bridge between the user applications and the physical environment (Sabri et al., 2017). Generally, the OS comprises the kernel, system shell and utility software. The kernel manages resources, the system shell allows access to the kernel, and the utility software includes tools such as compilers, assemblers and debuggers. Higher-level IoT platforms, such as Raspberry Pi, BeagleBone, Orange Pi, Samsung Artik, Intel Edison, and Galileo, use OSs such as Raspbian, Ubuntu Mate, Snappy Ubuntu, Windows 10 IoT Core and many more, which require substantial memory (Swamy & Kota, 2020). Service-oriented architecture (SOA) plays a crucial role in integrating diverse systems or devices and has proven effective in applications such as cloud computing and vehicle networking (da Silva et al., 2020). The primary benefit of SOA is its capability to facilitate the construction of flexible multilayer frameworks customized to meet individual business requirements (Wang et al., 2021).

5. IoT Applications and Use Cases

As intimated above, the potential applications of IoT are substantial and varied, affecting almost every aspect of daily life. IoT can enhance quality of life across various environments, including homes, workplaces, hospitals and gyms, and while travelling. In these settings, intelligent objects equipped with communication capabilities can exchange information, enabling various applications. In practice, IoT applications can be categorized into five domains: community, transportation, environmental, industrial and entertainment. These applications are increasingly integral to our lives, providing significant benefits and fostering a growing dependence on their functionality. The evolution of distinct IoT application domains depends on several critical factors:

advancements in electronic components, accessible software solutions with user-friendly interfaces, developments in sensor technologies and data acquisition methods, the reliability of network connectivity and infrastructure, and an adequate energy supply for the manufacturing and operation of IoT devices. Information technology, especially IoT-enabled smart technologies, serves as the primary catalyst for effective digitalization across multiple sectors. The energy sector in particular is rapidly advancing through 'energy digitalization' in various energy-related domains. Currently, energy is one of the most significant areas of IoT deployment, encompassing advancements in smart homes, enhanced automation of home energy systems, the establishment of smart and adaptable micro-grids, and enhancements in the efficient demand-side management of power systems. There has also been significant work on the concept of the circular economy, investigating various ideas to support smart waste management and address major societal challenges. IoT technologies have also recently been tested for use in environmental protection, especially in relation to air quality monitoring, demonstrating considerable potential in this area. The following subsections outline some of the main areas in which IoT systems are being applied.

5.1. Smart Homes

IoT-based smart home security systems enhance monitoring, control and security through internet connectivity, making these processes more efficient and accessible. As IoT technology advanced, it was expected to boost the security and safety of home occupants significantly (Ali et al., 2017; Rachman, 2017; Susilo et al., 2021). These systems can, for example, automatically detect motion, monitor temperature and humidity levels, and track activities within the home. Users can also manage and monitor the system remotely through an internet-connected application that is integrated with the IoT system (Faroqi et al., 2017; Riskiono et al., 2018; Setyawan et al., 2021). IoT-based smart home security systems are able to use various sensors, such as gas, passive infrared (PIR) and digital humidity and temperature (DHT11) sensors, flow switches and cameras, along with an ESP32 microcontroller, to enhance home security. This technology allows homeowners to monitor their security systems, respond quickly to emergencies, and maintain greater control. The system communicates with a server or mobile application, analysing the data collected to generate actionable insights (Parti et al., 2024).

5.2. Smart Cities

Smart cities represent a significant application of IoT technology (Cvar et al., 2020). Examples of IoT applications in smart cities encompass automated transportation, urban security, smart energy management systems, smart surveillance, and water supply and environmental monitoring (García et al., 2017). The IoT market predominantly focuses on smart cities and IIoT, with other promising areas including connected buildings, cars and energy sectors. The smart city concept is experiencing the fastest growth among IoT application areas, driven by a rising urban population which leads to severe infrastructure challenges. The primary advantage of IoT technologies in smart cities is their ability to address and mitigate these infrastructure issues in densely populated urban areas.

5.3. Vehicles

Connected vehicles are on the increase (Uddin et al., 2019) and it is also expected to see IoT implementations in budget cars. Previously, this technology was primarily used to optimize internal vehicle functions, but there is now increasing focus on using IoT to enhance the in-car experience (Lengyel et al., 2015). Introducing the concept of IoT to the transportation field has resulted in a new type of network, called the Internet of Vehicles (IoV), which aims at improving the driving experience and road safety. This is achieved by connecting useful information from road objects and distributing it to drivers to avoid road hazards, for example (Priyan & Devi, 2019). Furthermore, road authorities can collect and analyse information from both road objects and vehicles to improve the transportation system in general. This will help in implementing an intelligent transportation system (ITS), which is one of the modern aspects of smart cities (Gracias et al., 2023). For instance, Chowdhury et al. (2023) propose a guided priority-based incident management system to help emergency vehicles reach incident locations faster, which will lead to a reduction in response times.

5.4. Wearables

Wearables have become highly sought-after tech products in recent years (Fernández-Caramés & Fraga-Lamas, 2018b). They appeal to users of all ages, including teenagers, those who are middle-aged, and even older adults, because of their user-friendly interface and health advantages, which include features such as sleep tracking, heart rate sensors, oximeters, and pulse calculators. These devices help us stay connected in our interconnected world (Shafi & Waheed, 2019). Currently, there is considerable excitement surrounding IoT, with new IoT-enabled products being launched by companies almost daily (Hossain, 2023).

5.5. Healthcare

The use of IoT in healthcare has experienced substantial growth in recent years was expected to expand further in the coming decades (Amine & Oumnad, 2018). IoT enables the use of interconnected devices to promote healthier lifestyles. The concept of

connected digital health presents significant potential for individuals and organizations in the medical and pharmaceutical industries, although it has yet to reach widespread adoption among the general population. Healthcare systems can also benefit greatly from IoT devices, particularly through the concept of e-health (Allam et al., 2024). Enhanced monitoring systems supported by IoT can improve quality and patient safety.

5.6. Supply Chains

IoT plays a crucial role in supply chains by tracking, organizing and managing products and inventory information (Ben-Daya et al., 2019). IoT underscores the notion that machines excel in communicating data more effectively than humans, enabling companies to analyse larger volumes of data in less time. As noted by Udeh et al. (2024), IoT has the potential to improve supply chain management in two main directions. First, IoT is used in collecting real-time data, including location, temperature and speed, for the purpose of tracking the conditions of products as well as helping take any necessary actions or adjustments. Second, IoT can play a major role in improving inventory management by increasing the accuracy of product location, which should result in reducing unnecessary high stock levels. Furthermore, IoT can reduce costs in general by utilizing the available resources more efficiently, by, for example, leading shipments to use the optimal and shortest path to reduce both delays and fuel consumption (de Vass et al., 2018).

5.7. Financial Institutions

Devices which are part of IoT networks offer banks and financial institutions real-time data, which enhances decision-making capabilities, improves customer experiences and boosts operational efficiency. These types of institutions have integrated IoT extensively into their daily operations. For instance, door access controllers manage physical access to critical areas, surveillance cameras can detect suspicious activities, and tablets can streamline customer interactions. ATMs, one of the earliest IoT devices in banking, provide customers with round-the-clock access for their banking needs, and wearable devices enable seamless mobile payments (Kannan, 2024).

5.8. E-Learning

IoT facilitates e-learning, particularly through the implementation of m-learning, across educational institutions, providing greater accessibility for both students and teachers. This advancement offers benefits such as enhanced feedback and progress monitoring for learners (Evans, 2013). IoT can also help in dealing with infrastructure limitations by increasing scalability (Wahshat et al., 2024). Today, classrooms and lecture halls are occupied by various IoT-enabled devices for the purpose of increasing interactivity and engagement, which leads to an enhanced learning experience (Özbey & Kayri, 2023). Furthermore, online and offline materials can also be accessed easily.

5.9. Agriculture

As the global population continues to grow, so does the demand for food. In response, smart farming has emerged as one of the most rapidly expanding and essential areas of IoT technology (Alonso et al., 2020). Overall, incorporating IoT technologies in this sector has not only optimized operations but has also brought about remarkable gains in efficiency, sustainability and innovation. Furthermore, IoT helps in the automatic monitoring of farms to detect hazards or potential issues and notify farmers to take the necessary action (Morchid et al., 2023). In addition, controlling costs and reducing waste can be achieved by introducing IoT and other advanced technologies, such as a blockchain (Mishra & Sharma, 2023). In general, introducing IoT into agriculture will transform traditional farming into what is now referred to as data-driven farming (Liang & Shah, 2023).

6. IoT Challenges

IoT offers extensive opportunities but also presents various challenges. Key challenges include interoperability, scalability, power consumption and battery life, data management and analytics, lack of standardization, regulatory compliance, and implementation costs. Addressing these challenges requires a collaborative approach involving industry stakeholders, policymakers and technology innovators. This collective effort is necessary for ensuring the sustainable growth and success of the IoT ecosystem. For instance, in the case of energy consumption, IoT devices are constrained by energy and often connect with and disconnect from access technologies because of their short-range coverage and mobility through multiple hops. In terms of scalability, the vast number of IoT devices connected within an application is considered another challenge. Hence, handling the deployment and functionality of these devices effectively requires scalable operations. Furthermore, integrating multiple protocols and standards is an expensive and intricate undertaking, making it imperative to find solutions that reduce these costs and complexities. Interoperability in IoT networking is a challenge due to many factors, such as the different technologies in use, the variety of the existing applications and architectures, and the protocols available to manage communications and ensure a high standard of security and privacy. One of the practices of handling such a challenge has been to introduce cloud computing and cloudlet concepts. Moreover,

sustainability has emerged as a critical consideration amid the rapid evolution of IoT technologies which offer various benefits. However, this rapid progress needs vigilant monitoring and assessment from an environmental standpoint to mitigate negative impacts and ensure the efficient utilization of limited global resources. Furthermore, the diverse characteristics and growing adoption of IoT, combined with the rapid growth of IoT networks, create difficulties in consolidating existing IoT architectures. The large volume of data generated by connected objects also plays a vital role in the realm of big data. Big data analysis has been found to be a significant drawback in IoT due to the vast quantities of data gathered from diverse sensors in different locations. In addition to the aforementioned IoT challenges, the following factors are considered to affect IoT deployment directly and may render achieving its optimal benefits.

6.1. Security

Securing IoT networks is a top research challenge and a priority for various critical applications. Several factors contribute to the vulnerability of IoT systems. One key reason is that IoT components often remain unchecked for extended periods, causing them to be susceptible to physical attacks. The predominance of wireless communication in IoT also makes eavesdropping relatively easy. Traditional security models are inadequate for addressing the new security challenges exacerbated by the high volume of data produced by IoT. In addition, traditional security mechanisms and protocols, originally designed for conventional devices, often lack the requisite interoperability, scalability and integrity for IoT environments. Furthermore, IoT elements typically have limited processing power and computational resources, which restricts their ability to enable advanced security protocols. IoT security aims to safeguard assets and provide a high level of protection in terms of communication, as well as ensuring data availability and integrity. Consequently, researchers have focused on studying vulnerabilities (Zolanvari et al., 2019), defences (Lin et al., 2018), types of attacks (Pourghebleh et al., 2019) and mitigation strategies (Nguyen et al., 2019) by using various simulators, emulators and platform analysis. To safeguard IoT connections from disruption and unauthorized access, security measures must be implemented through all layers of the architecture, spanning from the lowest to the highest levels. Various mechanisms have been developed in order to provide a high level of protection in IoT networks. In practice, however, optimizing latency and enhancing computation speed for security algorithms in IoT applications is challenging. Mobile applications control most IoT applications, making securing these apps a major concern. For instance, implementing a multifaceted approach to securing networks and mitigating cyber threats while adhering to regulatory standards can provide substantial benefits. Leveraging machine learning and AI technologies can also play a pivotal role in achieving this balance (Alsamiri & Alsubhi, 2019).

6.2. Standardization

Standardization poses a primary challenge in IoT deployment. Standards are essential for establishing and advancing IoT technologies, ensuring equitable access and service utilization for all stakeholders. The absence of standards can also reduce the competitiveness of IoT products. Consequently, various organizations have developed numerous technical standards over the past decade, including middleware and interface standards. For instance, the National Institute of Standards and Technology (NIST) has been active in drafting cyber-security specifications, such as NISTIR 8259, 8259A and 8228 (NIST, 2019). In addition, in 2019, the European Union Agency for Cybersecurity (ENISA) published good practices for IoT security (Brass et al., 2018; ENISA, 2019). Furthermore, oneM2M (2016) applies security standards for IoT in its own systems, such as the European Telecommunications Standards Institute (ETSI) TS 118 103 and TS 003. One reason for the lack of standardization is that most of the existing internet protocols and standards were not originally developed with IoT devices in mind. Embedded devices also have severe constraints in terms of power, memory and processing capabilities, as they sometimes enter extended sleep periods to conserve energy. Thus, challenges will arise, such as the risk of losing packets, varying patterns of traffic, limitations in network topology, negative impacts on throughput, and limits on the maximum size of a payload. As a result, the lack of a unified definition of IoT architecture or widespread consensus on protocols and standards for all components remains. However, numerous efforts have been made to provide unified protocols and standards, such as the Internet Engineering Task Force (IETF), World Wide Web Consortium (W3C), IEEE, EPC Global and ETSI having designed supporting protocols for the types of IoT networks (Shammar & Zahary, 2020).

6.3. Privacy and Authentication

One of the most concerning aspects of IoT is that consumers unwittingly compromise their privacy one piece at a time, as they are often unaware of what data is being collected and how these are used. Many devices transmit sensitive client data, such as names, addresses, dates of birth, healthcare information, credit card details and more without encryption (Foltz & Foltz, 2020). Furthermore, IoT devices produce and collect large quantities of data, including sensitive information that is susceptible to potential leakage. Therefore, encrypting these data, both during transmission and while at rest, and carefully controlling access to them are crucial measures. Given that a device itself can be a point of vulnerability, it is essential to design devices with security in mind and ensure they have mechanisms for secure software updates or patches. Recent research has concentrated on developing sophisticated authentication mechanisms to tackle the security challenges in IoT environments (Hasan et al., 2024). Authentication is crucial for verifying the identities of both devices and users. The growing adoption of authentication measures, such as

biometrics and multifactor authentication, reflects the industry's commitment to bolstering security without compromising usability (Rao & Prema, 2019). These strategies are not, however, without potential drawbacks.

6.4. Quality of Service

Numerous researchers and organizations have developed IoT applications, yet there remains a need to consider the user's quality of experience and ensure quality of service (QoS) (Laghari et al., 2019). QoS is critical, especially regarding networking aspects related to traffic characteristics. Traffic patterns in wireless sensor networks (WSNs) rely heavily on specific application contexts. However, integrating sensor nodes into the internet under the IoT paradigm introduces complexities. In IoT scenarios, the internet manages extensive data from different sensor networks, serving diverse targets with varying communication profiles. Furthermore, the development of some distributed large-scale systems, such as RFID, is considered to be in the early stages. Therefore, significant research efforts are required to support QoS in IoT environments. QoS management strategies developed for M2M communications may potentially be adapted to address QoS challenges in IoT scenarios. Cloud and fog computing form the backbone of IoT, making QoS essential for distinguishing between cloud service providers. Given the competitive and open nature of the cloud computing market, QoS is crucial. To thrive, cloud service providers must offer exceptional services that meet customer expectations (Mahmud et al., 2019).

7. IoT Research Trends and Future Directions

The rapid evolution of communication solutions and global market demands have resulted in an overall increase in IoT as a suitable solution. However, beyond protocol standardization, numerous challenges persist. These include managing dormant nodes, enhancing energy efficiency, improving security measures, ensuring scalability, optimizing resource representation, integrating cloud services, simplifying application development, utilizing semantics effectively, and ensuring a high level of maintenance. The merging of AI with IoT is also advancing data analytics, predictive modelling and intelligent decision-making within IoT devices and systems. In addition, 5G connectivity promises faster and more reliable data transfer speeds, addressing questions relating to, for example, autonomous robots, self-driving vehicles, and virtual reality, which represent advancements in technology but also bring new security challenges (Ali et al., 2024). A blockchain can, for example, offer unique characteristics to IoT networks, such as high levels of security and decentralized device management. However, integration between these technologies poses challenges, such as scalability and throughput concerns, as well as in managing elevated costs and overall administration. This integration finds various industrial applications in 5G-enabled networks, among them Healthcare 5.0, autonomous vehicles, Industry 5.0, supply chain management, e-voting, and smart homes. Blockchain, AI and 5G combined could enhance overall performance and security parameters across these sectors (Dwivedi et al., 2024). To tackle limitations in short-range IoT capabilities, satellite providers are considering new avenues. The introduction of long-range terrestrial IoT technologies has played a pivotal role in overcoming the constraints of WSNs with limited range (Ayoub et al., 2019), thereby broadening the scope of potential application scenarios for IoT deployment. Therefore, satellite network support presents a viable alternative in order to compensate for a lack of terrestrial infrastructure (Centenaro et al., 2021). Introducing cloud, fog and edge computing can significantly reduce latency and improve overall system efficiency, particularly in significant IoT networks, either by leveraging the robust capacities and scalability of these computing paradigms or enabling data processing closer to the data source. Nonetheless, achieving this goal requires the development of a strong architecture that considers the limitations and diverse characteristics of IoT-connected devices, such as battery constraints and heterogeneity. As a consequence of the lack of a standardized architecture (Rababah et al., 2020), there is a need to construct a cross-platform architecture capable of accommodating the wide array of applications used in IoT, while also addressing the unique features of IoT networks and devices. Furthermore, such a unified architecture must incorporate robust security features to ensure user satisfaction.

Finally, privacy and security are critical issues in IoT, necessitating efforts focused on developing trust management techniques. With the increasing number of IoT users, there is an opportunity for researchers to explore innovative solutions to deliver reliable and scalable services. While there are ongoing efforts to improve the security and privacy of IoT networks, more initiatives are required to ensure high-level protection, especially for sensitive data such as those utilized in the healthcare sector.

8. Conclusion

IoT integrates sensor, embedded computing and communication technologies to facilitate continuous services across any location and time. IoT serves a crucial role across diverse sectors, representing the fourth technological revolution following the internet and ICT. Experts in research and development foresee IoT as having a more profound societal impact than the internet and ICT, fostering societal welfare and industrial progress. Focusing on key system-level design issues, including energy efficiency, security, scalability, robustness, and interoperability is vital to fully realizing the potential of IoT systems. IoT applications are poised to revolutionize our lifestyles with advancements in wireless setups, more powerful sensors, and enhanced computing capacities, promising to simplify daily life. As technologies such as AI, cloud computing and cellular networks gain traction, researchers are increasingly exploring intelligent IoT solutions that leverage these technologies to expand IoT-based networks.

Collaboration between researchers and industry stakeholders is crucial to overcome limitations and explore possibilities for employing IoT across sectors such as healthcare, agriculture and industry, and in smart cities. This collaborative effort aims at fostering a more interconnected, secure and innovative technological landscape. However, addressing the diverse environments and data types (e.g., text, audio, images and video) handled by IoT networks requires concerted efforts to optimize performance.

This paper examined current IoT-based network technologies and ongoing efforts to improve their performance, identifying open research opportunities and emerging trends. Key challenges in IoT implementation were reviewed, with examples of how technologies such as AI and cloud computing can mitigate those factors. Tackling these issues is crucial for fully unlocking the capabilities of IoT applications.

As demonstrated in this paper, there is scope for researchers to focus on developing standardized interoperability protocols, robust security frameworks and energy-efficient IoT devices. In addition, examining the possibility of new applications, particularly those integrating IoT with cloud computing and AI and exploring synergies with other cutting-edge technologies, is crucial for advancing IoT applications. This holistic approach will shape the future of IoT, promoting a more interconnected, secure and innovative technological landscape.

References

Akbar, A., Kousiouris, G., Pervaiz, H., Sancho, J., Ta-Shma, P., Carrez, F., & Moessner, K. (2018). Real-time probabilistic data fusion for large-scale IoT applications. *IEEE Access*, *6*, 10015–10027.

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials*, *17*(4), 2347–2376.

Ali, S.M., Rahu, M.A., Karim, S., Jatoi, G.M., & Sattar, A. (2024). Internet of Things (IoT), applications and challenges: A comprehensive review. *Journal of Innovative Intelligent Computing and Emerging Technologies (JIICET)*, *1*(1), 20–27.

Ali, W., Dustgeer, G., Awais, M., & Shah, M.A. (2017). IoT based smart home: Security challenges, security requirements and solutions. In *2017 23rd International Conference on Automation and Computing (ICAC)* (pp. 1–6). IEEE.

Allam, A.H., Gomaa, I., Zayed, H.H., & Taha, M. (2024). IoT-based eHealth using blockchain technology: A survey. *Cluster Computing*. https://doi.org/10.1007/s10586-024-04357-y

Alonso, R.S., Sittón-Candanedo, I., García, O., Prieto, J., & Rodríguez-González, S. (2020). An intelligent Edge-IoT platform for monitoring livestock and crops in a dairy farming scenario. *Ad Hoc Networks*, *98*, 102047.

Alsamiri, J., & Alsubhi, K. (2019). Internet of things cyber attacks detection using machine learning. *International Journal of Advanced Computer Science and Applications*, *10*(12), 627–634.

Amine, R., & Oumnad, A. (2018). Challenges and opportunities of internet of things in healthcare. *International Journal of Electrical and Computer Engineering*, *8*(5), 2753–2761.

Aqeel-ur-Rehman, Mehmood, K., & Baksh, A. (2013). Communication technology that suits IoT – A critical review. In *Wireless Sensor Networks for Developing Countries: First International Conference, WSN4DC, Jamshoro, Pakistan, April 24–26, 2013, Revised Selected Papers* (pp. 14–25). Springer, Berlin.

Asghar, M.H., Negi, A., & Mohammadzadeh, N. (2015). Principle application and vision in Internet of Things (IoT). In *2015 International Conference on Computing, Communication & Automation (ICCCA)* (pp. 427–431). IEEE.

Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, *54*(15), 2787–2805.

Ayoub, W., Samhat, A.E., Nouvel, F., Mroue, M., & Prévote, J.-C. (2019). Internet of Mobile Things: Overview of LoRaWAN, DASH7, and NBIoT in LPWANs standards and supported mobility. *IEEE Communications Surveys and Tutorials*, *21*(2), 1561–1581.

Bălău, N., & Utz, S. (2017). Information sharing as strategic behaviour: The role of information display, social motivation and time pressure. *Behaviour and Information Technology*, *36*(6), 589–605.

Bandyopadhyay, D., & Sen, J. (2011). Internet of Things: Applications and challenges in technology and standardization. *Wireless Personal Communications*, *58*(1), 49–69.

Ben-Daya, M., Hassini, E., & Bahroun, Z. (2019). Internet of things and supply chain management: A literature review. *International Journal of Production Research*, *57*(15–16), 4719–4742.

Bradley, J., Reberger, C., Dixit, A., Gupta, V., & Macaulay, J. (2013). Internet of Everything (IoE): Top 10 insights from Cisco's IoE value at stake analysis for the public sector. San Jose, CA: Cisco Internet Business Solutions Group (IBSG), Cisco Systems, Inc. *Economic Analysis 2013*. http://www.cisco.com/web/about/ac79/docs/IoE/IoE-VAS_PublicSector_Top-10-Insights.pdf

Brass, L., Tanczer, M., Carr, M., Elsden, M., & Blackstock, J. (2018). Standardising a moving target: The development and evolution of IoT security standards. In *Living in the Internet of Things: Cybersecurity of the IoT – 2018*. London: IET.

Centenaro, M., Costa, C.E., Granelli, F., Sacchi, C., & Vangelista, L. (2021). A survey on technologies, standards and open challenges in satellite IoT. *IEEE Communications Surveys and Tutorials*, *23*(3), 1693–1720.

Chowdhury, A., Kaisar, S., Khoda, M.E., Naha, R., Khoshkholghi, M.A., & Aiash, M. (2023). IoT-based emergency vehicle services in intelligent transportation system. *Sensors*, *23*(11), 5324.

Cvar, N., Trilar, J., Kos, A., Volk, M., & Duh, E.S. (2020). The use of IoT technology in smart cities and smart villages: Similarities, differences, and future prospects. *Sensors*, *20*(14), 3897.

da Cruz, M.A.A., Rodrigues, J. J. P. C., Al-Muhtadi, J., Korotaev, V.V., & de Albuquerque, V.H.C. (2018). A reference model for Internet of Things middleware. *IEEE Internet of Things Journal*, *5*(2), 871–883.

da Cruz, M.A.A., Rodrigues, J.J.P.C., Lorenz, P., Solic, P., Al-Muhtadi, J., & Albuquerque, V.H.C. (2019). A proposal for bridging application layer protocols to HTTP on IoT solutions. *Future Generation Computer Systems*, *97*, 145–152.

da Silva, F.S.T., da Costa, C.A., Crovato, C.D.P., & da Rosa Righi, R. (2020). Looking at energy through the lens of Industry 4.0: A systematic literature review of concerns and challenges. *Computers & Industrial Engineering*, *143*, 106426.

de Vass, T., Shee, H., & Miah, S.J. (2018). The effect of "Internet of Things" on supply chain integration and performance: An organisational capability perspective. *Australasian Journal of Information Systems*, *22*. https://doi.org/10.3127/ajis.v22i0.1734

Dwivedi, A.D., Singh, R., Kaushik, K., Mukkamala, R.R., & Alnumay, W. (2024). Blockchain and artificial intelligence for 5G-enabled Internet of Things: Challenges, opportunities, and solutions. *Transactions on Emerging Telecommunications Technologies*, *35*(6), e4329.

Elazhary, H. (2019). Internet of Things (IoT), mobile cloud, cloudlet, mobile IoT, IoT cloud, fog, mobile edge, and edge emerging computing paradigms: Disambiguation and research directions. *Journal of Network and Computer Applications*, *128*, 105–140.

European Union Agency for Cybersecurity. (2019, Nov. 19). *Good practices for security of IoT – Secure software development lifecycle*. https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1

Evans, D. (2012a, Nov. 29). *How the Internet of Everything will change the world for the better*. Cisco blog. http://blogs.cisco.com/news/how-the-internet-of-everything-willchange-the-worldfor-the-better-infographic/

Evans, D. (2012b). *The Internet of Everything: How more relevant and valuable connections will change the world.* San Jose, CA: Cisco Internet Business Solutions Group (IBSG), Cisco Systems, Inc. White Paper. https://www.cisco.com/web/about/ac79/docs/innov/IoE.pdf

Evans, D. (2013, Sept. 12). *Ask the futurist: "How will the Internet of Everything impact teachers' roles in the connected classroom?"* Cisco blog. http://blogs.cisco.com/ioe/connected-classroom/

Faroqi, A., Halim, D.K., Mada Sanyaya, W.S., & Hadisantoso, E.P. (2017). *Perancangan alat pendeteksi kadar polusi udara mengunakan sensor gas MQ-7 dengan teknologi wireless HC-05* / Design of air pollution level detection device using MQ-7 gas sensor with HC-05 wireless technology. *Jurnal Istek* / *Science Journal*, *10*(2). ISSN: 1979–8911.

Fernández-Caramés, T.M., & Fraga-Lamas, P. (2018a). A review on the use of blockchain for the Internet of Things. *IEEE Access*, *6*, 32979–33001.

Fernández-Caramés, T.M., & Fraga-Lamas, P. (2018b). Towards the Internet of smart clothing: A review on IoT wearables and garments for creating intelligent connected e-textiles. *Electronics*, *7*(12), 405.

Foltz, C.B., & Foltz, L. (2020). Mobile users' information privacy concerns instrument and IoT. *Information and Computer Security*, *28*(3), 359–371.

García, C.G., Meana-Llorián, D., Pelayo G-Bustelo, B.C., Lovelle, J.M.C., & Garcia-Fernandez, N. (2017). Midgar: Detection of people through computer vision in the Internet of Things scenarios to improve the security in Smart Cities, Smart Towns, and Smart Homes. *Future Generation Computer Systems*, *76*, 301–313.

GlobalDots (2019, June 21). *41.6 billion IoT devices will be generating 79.4 zettabytes of data in 2025*. GlobalDots blog. https://www.globaldots.com/blog/41-6-billion-iot-devices-will-begenerating-79-4-zettabytes-of-data-in-202

Goyal, K.K., Garg, A., Rastogi, A., & Singhal, S. (2018). A literature survey on Internet of Things (IoT). *International Journal of Advanced Networking and Applications*, *9*(6), 3663–3668.

Gracias, J.S., Parnell, G.S., Specking, E., Pohl, E.A., & Buchanan, R. (2023). Smart cities – A structured literature review. *Smart Cities*, *6*(4), 1719–1743.

Hasan, M.K., Weichen, Z., Safie, N., Ahmed, F.R.A., & Ghazal, T.M. (2024). A survey on key agreement and authentication protocol for Internet of Things application. *IEEE Access*, *12*, 61642–61666.

Haslett, A.M., & Brown, R.W. (2018). *Method and system of monitoring appliance usage* (U.S. Patent Application No. 15/552,087). Filed 24 Feb. 2016. U.S. Patent and Trademark Office.

Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A survey on IoT security: Application areas, security threats, and solution architectures. *IEEE Access*, *7*, 82721–82743.

Hossain, K.A. (2023). Evaluation of influence of "Internet of Things" (IoT) on technologies and devices in 21st century. *Scientific Research Journal*, *11*(7), 1-27.

Institute of Electrical and Electronics Engineers Standards Association. (2018). *IEEE Draft Standard for an Architectural Framework for the Internet of Things (IoT)*, Standard IEEE P2413/D0.4.5, Dec. 2018, pp. 1–264.

Institute of Electrical and Electronics Engineers Standards Association. (2019). *IEEE Draft Standard for an Architectural Framework for the Internet of Things (IoT)*, Standard IEEE P2413/D0.4.6, Mar. 2019, pp. 1–265.

Islam, S.M.R., Kwak, D., Kabir, M.H., Hossain, M., & Kwak, K.-S. (2015). The Internet of Things for health care: A comprehensive survey. *IEEE Access*, *3*, 678–708.

Jatoi, G.M., Rahu, M.A., Karim, S., Ali, S.M., & Sohu, N. (2023). Water quality monitoring in agriculture: Applications, challenges and future prospectus with IoT and machine learning. *Journal of Applied Engineering and Technology*, *7*(2), 46–54.

Javed, F.M., Afzal, K., Sharif, M., & Kim, B. (2018). Internet of Things (IoT) operating systems support, networking technologies, applications, and challenges: A comparative review. *IEEE Communications Surveys & Tutorials*, *20*(3), 2062–2100.

Kannan, Y. (2024). Impact of Internet of Things (IoT) devices on network security at financial institutions. *Authorea Preprints*, 10 March 2024.

Kaur, M.J., Riaz, S., & Mushtaq, A. (2020). Cyber-physical cloud computing systems and Internet of Everything, in Peng, S.L., Pal, S., & Huang, L. (Eds.), *Principles of Internet of Things (IoT) ecosystem: Insight paradigm*. Springer, Cham, pp. 201–227.

Khairnar, A.G., & Birari, D.A. (2018). IoT ("connected life") and its use in different applications: A survey. *MVP Journal of Engineering Sciences*, *1*(1), 24–28.

Khan, R., Khan, S.U., Zaheer, R., & Khan, S. (2012). Future internet: The Internet of Things architecture, possible applications and key challenges. In *2012 10th International Conference on Frontiers of Information Technology (FIT)* (pp. 257–260). IEEE.

Khanna, A., & Kaur, S. (2020). Internet of Things (IoT), applications and challenges: A comprehensive review. *Wireless Personal Communications*, *114*(15), 1687–1762.

Kuchuk, H., & Malokhvii, E. (2024). Integration of IoT with cloud, fog, and edge computing: A review. *Advanced Information Systems*, *8*(2), 65–78.

Kumar, N.M., & Mallick, P.K. (2018). The Internet of Things: Insights into the building blocks, component interactions, and architecture layers. *Procedia Computer Science*, *132*, 109–117.

Laghari, A.A., He, H., Shafiq, M., & Khan, A. (2019). Application of quality of experience in networked services: Review, trend and perspectives. *Systemic Practice and Action Research*, *32*(5), 501–519.

Lengyel, L., Ekler, P., Ujj, T., Balogh, T., & Charaf, H. (2015). SensorHUB: An IoT driver framework for supporting sensor networks and data analysis. *International Journal of Distributed Sensor Networks*, *11*(7), 454379.

Li, S., Xu, L.D., & Zhao, S. (2015). The Internet of Things: A survey. *Information Systems Frontiers*, *17*(2), 243–259.

Liang, C., & Shah, T. (2023). IoT in agriculture: The future of precision monitoring and data-driven farming. *Eigenpub Review of Science and Technology*, *7*(1), 85–104.

Lin, H., Yan, Z., Chen, Y., & Zhang, L. (2018). A survey on network security-related data collection technologies. *IEEE Access*, *6*, 18345–18365.

Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal*, *4*(5), 1125–1142.

Liu, H., Han, D., & Li, D. (2020). Fabric-IoT: A blockchain-based access control system in IoT. *IEEE Access*, *8*, 18207–18218.

Lu, L., Xu, L., Xu, B., Li, G., & Cai, H. (2018). Fog computing approach for music cognition system based on machine learning algorithm. *IEEE Transactions on Computational Social Systems*, *5*(4), 1142–1151.

Mahmud, R., Srirama, S.N., Ramamohanarao, K., & Buyya, R. (2019). Quality of experience (QoE)-aware placement of applications in Fog computing environments. *Journal of Parallel and Distributed Computing*, *132*, 190–203.

Marjani, M., Nasaruddin, F., Gani, A., Karim, A., Hashem, I.A.T., Siddiqa, A., & Yaqoob, I. (2017). Big IoT data analytics: Architecture, opportunities, and open research challenges. *IEEE Access*, *5*, 5247–5261.

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of Things: Vision, applications and research challenges. *Ad Hoc Networks*, *10*(7), 1497–1516.

Miori, V., & Russo, D. (2017) Improving life quality for the elderly through the Social Internet of Things (SIoT). In *2017 Global Internet of Things Summit (GIoTS)*, Geneva, Switzerland (pp. 1–6). IEEE.

Miraz, M.H., Ali, M., Excell, P.S., & Picking, R. (2015). A review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT). In *2015 Internet Technologies and Applications (ITA)*, Wrexham, UK (pp. 219–224). IEEE.

Mishra, S., & Sharma, S.K. (2023). Advanced contribution of IoT in agricultural production for the development of smart livestock environments. *Internet of Things*, *22*, 100724.

Morais, C.P. de, Sadok, D., & Kelner, J. (2019). An IoT sensor and scenario survey for data researchers. *Journal of the Brazilian Computer Society*, *25*(1), Art. no. 4.

Morchid, A., El Alami, R., Raezah, A.A., & Sabbar, Y. (2023). Applications of internet of things (IoT) and sensors technology to increase food security and agricultural Sustainability: Benefits and challenges. *Ain Shams Engineering Journal*, *15*(3), 102509.

Motlagh, N.H., Taleb, T., & Arouk, O. (2016). Low-altitude unmanned aerial vehicles-based internet of things services: Comprehensive survey and future perspectives. *IEEE Internet of Things Journal*, *3*(6), 899–922.

National Institute of Standards and Technology. (2019, Aug. 1). *NIST releases draft security feature recommendations for IoT devices*. NIST, US Department of Commerce. https://www. nist.gov/news-events/news/2019/08/nist-releases-draft-security-featurerecommendations-iot-devices

Nguyen, V., Lin, P., & Hwang, R., (2019). Energy depletion attacks in low power wireless networks. *IEEE Access*, *7*, 51915–51932.

Nižetić, S., Šolić, P., Gonzalez-de-Artaza, D.L. de I., & Patrono, L. (2020). Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future. *Journal of Cleaner Production*, *274*(5), 122877.

Ojo, M.O., Giordano, S., Procissi, G., & Seitanidis, I.N. (2018). A review of low-end, middle-end, and high-end IoT devices. *IEEE Access*, *6*, 70528–70554.

oneM2M. (2016). *oneM2M; Security solutions (ETSI TS 118 103, v1.1.0 (2016-03)*. https://www.etsi.org/deliver/etsi_ts/118100_118199/118103/02.04.01_60/ts_118103v020401p.pdf

Özbey, M., & Kayri, M. (2023). Investigation of factors affecting transactional distance in E-learning environment with artificial neural networks. *Education and Information Technologies*, *28*(4), 4399–4427.

Parti, I.K., Mudiana, I.N., Darminta, I.K., & Rasmini, N.W. (2024). Modellings smart home security based Internet of Things (IoT). In *International Conference on Applied Science and Technology on Engineering Science 2023 (iCAST-ES 2023)* (pp. 41–48). Atlantis Press.

Perera, C., Liu, C.H., Jayawardena, S., & Chen, M. (2014). A survey on Internet of Things from industrial market perspective. *IEEE Access*, *2*, 1660–1679.

Pourghebleh, B., Wakil, K., & Navimipour, N.J. (2019). A comprehensive study on the trust management techniques in the Internet of Things. *IEEE Internet of Things Journal*, *6*(6), 9326–9337.

Priyan, M.K., & Devi. G. (2019). A survey on internet of vehicles: Applications, technologies, challenges and opportunities. *International Journal of Advanced Intelligence Paradigms*, *12*(1–2), 98–119.

Rababah, B., Alam, T., & Eskicioglu, R. (2020). The next generation Internet of Things architecture towards distributed intelligence: Reviews, applications, and research challenges. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, *12*(2), 11–19.

Rachman, F.Z. (2017). Smart Home based on IoT. In *Seminar Nasional ITT-Politeknik Negeri Balikpapan / ITT-Balikpapan State Polytechnic National Seminar.*

Rao, V., & Prema, K.V. (2019). Light-weight hashing method for user authentication in internet-of-things. *Ad Hoc Networks*, *89*, 97–106.

Riskiono, S.D., Septiawan, D., Amarudin, A., & Setiawan, R. (2018). *Implementasi sensor PIR sebagai alat peringatan pengendara terhadap penyeberang jalan raya* / Implementation of PIR sensor as a warning tool for motorists to cross the highway. *Jurnal Mikrotik/Mikrotik / Journal of Informatics Management*, *8*(1). E-ISSN: 2443–4027.

Rose, D. (2014). *Enchanted objects: Design, human desire, and the Internet of Things*. Scribner eBook, Simon & Schuster.

Rothmuller, M., & Barker, S. (2020, Mar. 1). *IoT – The Internet of Transformation 2020*. Basingstoke, UK: Juniper Research. White Paper. https://www.juniperresearch.com/resources/whitepapers/iot-the-internet-of-transformation-2020/

Sabella, A., Irons-Mclean, R., & Yannuzzi, M. (2019). *Orchestrating and automating security for the Internet of Things: Delivering advanced security capabilities from Edge to cloud for IoT*. Indianapolis: Cisco Press.

Sabri, C., Lobna, K., & Azzouz, A.L. (2017). Comparison of IoT constrained devices operating systems: A survey. In *Proceedings IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA)* (pp. 369–375). IEEE.

Setyawan, R., Amrita, A.A.N., & Saputra, K.O. (2021). *Rancang bangun sistem penampungan air menggunakan tandon atas secara otomatis berbasis mikrokontroler* / Design and construction of a water storage system using an automatic top tank based on a microcontroller. *Jurnal SPEKTRUM / Spectrum Journal*, *8*(1), 254–259.

Sezer, O.B., Dogdu, E., & Ozbayoglu, M. (2018). Context-aware computing, learning, and big data in Internet of Things: A survey. *IEEE Internet of Things Journal*, *5*(1), 1–27.

Shafi, J., & Waheed, A. (2019). Role of smart wearable in healthcare: Wearable Internet of Medical Things (WIoMT), in Goyal, D., Balamurugan, S., Peng, S.-L., & Jat, D.S. (Eds.), *The IoT and the next revolutions automating the world*. IGI Global, pp. 133–155.

Shammar, E.A., & Zahary, A.T. (2020). The Internet of Things (IoT): A survey of techniques, operating systems, and trends. *Library Hi Tech*, *38*(1), 5–66.

Susilo, D., Sari, C., & Krisna, G.W. (2021). *Sistem kendali lampu pada smart home berbasis IOT (Internet of Things)* / The lighting control system in a smart home is based on IOT (Internet of Things). *Jurnal ELECTRA: Electrical Engineering Articles*, *2*(1), 23–30.

Swamy, S.N., & Kota, S.R. (2020). An empirical study on system level aspects of Internet of Things (IoT). *IEEE Access*, *8*, 188082–188134.

Talavera, J.M., Tobón, L.E., Gómez, J.A., Culman, M.A., Aranda, J.M., Parra, D.T., Quiroz, L.A., Hoyos, A., & Garreta, L.E. (2017). Review of IoT applications in agro-industrial and environmental fields. *Computers and Electronics in Agriculture*, *142*(1), 283–297.

Uddin, H., Gibson, M., Safdar, G.A., Kalsoom, T., Ramzan, N., Ur-Rehman, M., & Imran, M.A. (2019). IoT for 5G/B5G applications in smart homes, smart cities, wearables and connected cars. In *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)* (pp. 1–5). IEEE.

Udeh, E.O., Amajuoyi, P., Adeusi, K.B., & Scott, A.O. (2024). The role of IoT in boosting supply chain transparency and efficiency. *Magna Scientia Advanced Research and Reviews*, *11*(1), 178–197.

Wahshat, H., Khalifeh, A., Taha, A., Wahsheh, F., Amayreh, K., & Matalka, M. (2024). Individual, technological, organizational, and environmental factors impact of the internet of things on e-learning adoption in higher education institutions in Jordan. *International Journal of Data and Network Science*, *8*(3), 1451–1462.

Wanasinghe, T.R., Gosine, R.G., James, L.A., Mann, G.K.I., de Silva, O., & Warrian, P.J. (2020). The Internet of Things in the oil and gas industry: A systematic review. *IEEE Internet of Things Journal*, *7*(9), 8654–8673.

Wang, J., Lim, M.K., Wang, C., & Tseng, M.L. (2021). The evolution of the Internet of Things (IoT) over the past 20 years. *Computers & Industrial Engineering*, *155*, 107174.

Wen, J., Nie, J., Kang, J., Niyato, D., Du, H., Zhang, Y., & Guizani, M. (2024). From generative AI to Generative Internet of Things: Fundamentals, framework, and outlooks. *IEEE Internet of Things Magazine*, *7*(3), 30–37.

Whitmore, A., Agarwal, A., & Xu, L. (2015). The Internet of Things – A survey of topics and trends. *Information Systems Frontiers*, *17*(2), 261–274.

Xu, L.D., He, W., & Li, S. (2014). Internet of Things in industries: A survey. *IEEE Transactions on Industrial Informatics*, *10*(4), 2233–2243.

Yang, Z., Yue, Y., Yang, Y., Peng, Y., Wang, X., & Liu, W. (2011). Study and application on the architecture and key technologies for IOT. In *2011 International Conference on Multimedia Technology (ICMT)* (pp. 747–751). IEEE.

Yu, W., Liang, F., He, X., Hatcher, W.G., Lu, C., Lin, J., & Yang, X. (2018). A survey on the edge computing for the Internet of Things. *IEEE Access*, *6*, 6900–6919.

Zhang, C., Zhang, C., Zheng, S., Qiao, Y., Li, C., Zhang, M., Dam, S.K., Thwal, C.M., Tun, Y.L., Le, H., Kim, D., Bae, S.-H., Lee, L.-H., Yang, Y., Shen, H.T., Kweon, I., & Hong, C.S. (2023). A complete survey on generative AI (AIGC): Is ChatGPT from GPT-4 to GPT-5 all you need? *ArXiv* preprint: arXiv:2303.11717.

Zhang, M., Sun, F., & Cheng, X. (2012). Architecture of Internet of Things and its key technology integration based-on RFID. In *2012 Fifth International Symposium on Computational Intelligence and Design* (pp. 294–297). IEEE.

Zhong, C.-L., Zhu, Z., & Huang, R.-G. (2015). Study on the IOT architecture and gateway technology. In *2015 14th International Symposium on Distributed Computing and Applications for Business Engineering and Science (DCABES)* (pp. 196–199). IEEE.

Zhou, W., Jia, Y., Peng, A., Zhang, Y., & Liu, P. (2019). The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. *IEEE Internet of Things Journal*, *6*(2), 1606–1616.

Zhu, C., Leung, V.C.M., Shu, L., & Ngai, E.C.-H. (2015). Green Internet of Things for smart world. *IEEE Access*, *3*, 2151–2162.

Zolanvari, M., Teixeira, M.A., Gupta, L., Khan, K.M., & Jain, R. (2019). Machine learning-based network vulnerability analysis of Industrial Internet of Things. *IEEE Internet of Things Journal*, *6*(4), 6822–6834.