A THOROUGH STUDY OF THE INTERNET OF THINGS: FROM CORE COMPONENTS TO SECURITY AND APPLICATIONS

Jean Pierre Ntayagabiri[1], Youssef Bentaleb[2], Jeremie Ndikumagenge[3], Hind EL Makhtoum[2]

[1]Doctoral School of the University of Burundi, Center for Research in Infrastructure, Environment and Technology (CRIET), University of Burundi, Bujumbura, Burundi
[2]Engineering Sciences Laboratory, ENSA Kenitra, Ibn Tofaïl University, Kenitra, Morocco
[3]Center for Research in Infrastructure, Environment and Technology (CRIET), University of Burundi, Bujumbura, Burundi

ABSTRACT

The Internet of Things (IoT) is a rapidly evolving technology that is disrupting industries and transforming lifestyles. This promising technology offers numerous benefits, but it also raises important questions and challenges. This article aims to explore how IoT can revolutionize connectivity and automation in different domains, as well as the challenges and implications to consider for responsible development and adoption of this technology. It provides an in-depth exploration of IoT technology, from its definition and components to its current applications. It also addresses potential security issues associated with IoT and the measures that can be taken to mitigate them. Finally, it explores the various ways in which IoT can be applied to improve our lives. This research aims to contribute to the understanding of the IoT and its potential impact on society.

KEYWORDS

Actuators, Sensors, Internet of Things, Connectivity, Automation

1. INTRODUCTION

The Internet of Things (IoT) refers to a type of network that allows any object to be connected to the Internet on the basis of stipulated protocols, using information sensing equipment, in order to exchange information and communicate for the purposes of intelligent recognition, positioning, tracking, control and administration. The Internet of Things (IoT) is a revolutionary concept that is transforming the way we interact with the physical world. It enables devices to communicate with each other and with humans through various means such as sensors, actuators and wireless networks. This connectivity enables seamless integration between physical objects and digital systems. The relationship will be between people and people, people and things, and things and things. This "network of objects" has the potential to revolutionise the way we interact with our environment, allowing us to monitor, control and interact with physical objects as never before. At the heart of the IoT is the ability to collect, store, analyse and act on data from connected devices.

The potential of IoT is vast and varied. From smart homes that can be controlled remotely to industrial automation that optimises processes for greater efficiency, IoT technology has the

power to reshape industries as a whole. It offers unprecedented opportunities for automation, data-driven decision-making and improved productivity. It can enhance inventory management, asset maintenance, workforce management and field services in manufacturing [1]. IoT is also helping to manage the logistics of moving billions of people and goods around the world in the aviation sector and to reduce the costs of tracking assets at airports [2]. It identifies inefficiencies and waste, and recommends ways to increase efficiency in manufacturing [3], [4] and improve the efficiency and performance of the electricity grid [5], [6]. By connecting devices in a networked ecosystem, IoT enables automation on a scale never seen before. This can lead to significant time savings, cost reductions and better resource allocation.

However, with billions of devices connected to the internet, the risk of cyberattacks and data breaches increases. Hackers can exploit vulnerabilities in IoT devices to gain unauthorized access to sensitive information or even take control of critical infrastructure. Additionally, there are growing concerns about how the data collected by IoT devices is used and shared. Moreover, with a wide range of different devices from various manufacturers, ensuring seamless communication and compatibility between these devices can be complex. This lack of standardization can hinder the widespread adoption and integration of IoT technology. Furthermore, as new devices are added to the network, managing and maintaining them becomes increasingly challenging.

In this article, we delve into the concept and potential of the Internet of Things (IoT). We'll start by defining IoT and providing an overview of its underlying technologies. We'll explore connectivity options within an IoT ecosystem and the crucial role of automation. Here's how we'll break down the rest of the article:

- Section 2: A review of existing research on the Internet of Things.
- Section 3: Exploration of the fundamental components of an IoT system and their functions.
- Section 4: Presentation of the IoT ecosystem's architecture.
- Section 5: Discussion of the technologies driving the rapid growth of IoT.
- Section 6: Examination of challenges and security concerns to consider when implementing IoT solutions.
- Section 7: Addressing vital security measures to protect sensitive data and prevent unauthorized access within the IoT environment.
- Section 8: Exploration of IoT application domains and its transformative impact on various industries, highlighting opportunities for innovation and efficiency.
- Section 9: Concluding remarks for this comprehensive IoT study.

2. RELATED WORKS

The pervasiveness of IoT has made it a hot topic of research and debate in academia and industry. Numerous papers and articles have explored its various aspects, including:

- Applications (concrete application domains and impact on customer value in business) [7], [8].
- Security and privacy (vulnerabilities, challenges, solutions, and countermeasures) [9], [10], [11], [12]
- Key challenges and issues (big data management, technological convergence, and future developments)[13], [14].

- Economic and societal impact (potential benefits and ethical considerations)[10] Definitions and architecture (basic concepts, architecture description)[15], [16], [17].
- Fundamental technologies (hardware, software, and networking components, technologies critical to the deployment of products and services)[16], [17]

Concrete examples of IoT applications are presented in areas such as healthcare [18], education [10], and agriculture [19]. The integration of emerging technologies such as machine learning and blockchain to strengthen IoT security is also explored [9], [20]. Recent studies have examined the progress made in areas such as materials and devices for IoT [21], IoT-based and IoMT healthcare [22], machine learning and deep learning based security intelligence [20], and machine learning and deep learning based solutions for IoT privacy [23]. This article explores the IoT, its components, and applications. It examines its social and environmental implications, the challenges to its adoption, and the opportunities it offers organizations.

3. BUILDING BLOCKS OF THE INTERNET OF THINGS

The Internet of Things (IoT) is one of the most important technologies after mobile phones and the internet, with the potential to profoundly influence the way we live [24]. It has revolutionised the way we interact with our environment, creating a vast ecosystem of interconnected devices. The Internet of Things (IoT) refers to devices with sensors, processing capabilities, software and other technologies that connect and exchange data with other devices and systems via the internet or other communications networks [25], [26]. The IoT is a rapidly expanding network that extends to every aspect of our daily lives. To understand how it works and its potential, it is crucial to understand its constituent parts. The IoT is based on four fundamental pillars: sensors and devices, data processing units, internet connectivity and platforms and applications.

- **Sensors and Devices:** At the heart of the IoT are the devices themselves equipped with sensors [27], [28] .These IoT devices come in many forms, from smart thermostats and wearables to industrial sensors and surveillance cameras [29], [30]. The sensors built into these devices collect data about their environment [31]. They act as the eyes and ears of the IoT ecosystem, capturing information such as temperature, humidity, movement, etc [32], [33]. There are two categories of sensor: simple (temperature, light) and complex (inertial, GPS, biometric). They can be integrated into the object itself or in the form of external modules.
- **Internet Connectivity:** The third pillar is Internet connectivity, which enables objects to communicate with each other and with the cloud. Various connectivity technologies exist, such as Wi-Fi, Bluetooth, Zigbee and cellular networks (4G, 5G). The choice of technology depends on a number of factors, including distance, throughput and energy consumption.
- **Data Processing Units:** These units analyze the raw data collected by the sensors and transform it into usable information. Processing can be carried out directly on the object via a microcontroller or on a remote server. The processing power required depends on the complexity of the tasks to be carried out.
- **Platforms and Applications:** IoT platforms store the data collected and offer services to analyze and exploit it. They can be hosted in the cloud or on site. A multitude of applications exploit IoT data, in areas such as home automation, healthcare, industry and agriculture.

In addition to these four fundamental pillars, the IoT relies on other crucial technologies, such as communication networks and protocols to transmit data, security and confidentiality to protect

data against attacks and intrusions, and artificial intelligence and machine learning to analyse data and extract valuable insights.

4. ARCHITECTURE OF THE INTERNET OF THINGS ECOSYSTEM

The Internet of Things (IoT) is a fast-growing technology that is transforming the way we interact with the physical world. It connects physical objects to the internet, enabling them to interact with each other and share data. To do this, the IoT must be based on a flexible, scalable and secure architecture. IoT architecture is the framework that allows internet-connected devices to exchange information with each other, as well as with cloud-based and on-premises services and systems.There are different models of IoT architecture [34], but most comprise three or four layers: perception, transport, processing and application [35], [36]. The Figure 1 and Figure 2 represent the three-layer and four-layer architecture respectively.

The first layer of the architecture is the physical layer. This layer is made up of devices such as sensors, actuators, RFID tags and other physical objects. These devices are connected to the internet, allowing them to send and receive data [37].

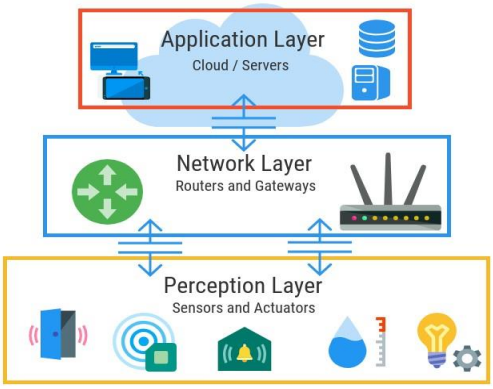

Figure 1: 3-layer IoT architecture[38]

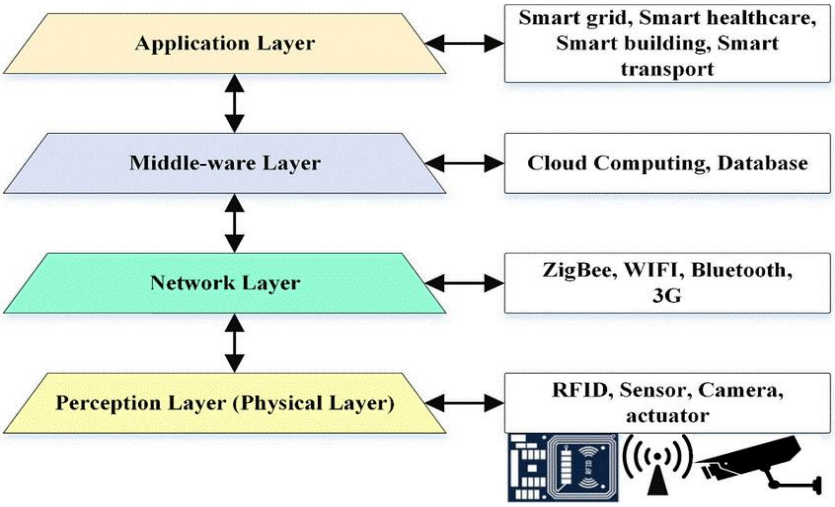

Figure 2: 4-layer IoT architecture [39]

The second layer is the network layer. This layer is made up of different network technologies such as Wi-Fi, Bluetooth, NFC and Zigbee. This layer allows physical devices to communicate with each other and send data to the cloud [40].

The third layer of the IoT ecosystem is called the Middle-ware Layer. It is made up of databases, analysis tools and software applications. This layer is the brain of the IoT ecosystem. Typically, data collected by physical devices is analyzed, preprocessed and stored here before being sent to the data center, where it is accessible to software applications that monitor and manage the data and prepare further actions. As the central layer of the IoT, middleware connects applications and devices, helping to address common IoT challenges and improve application development [41]. It acts as an interface between IoT components, enabling communication between elements that would not otherwise be able to communicate [42]. Middleware simplifies the management of communication and I/O for software developers, enabling them to concentrate on the core goals of their application [43]. Services provided by the middleware include device discovery and management, massive data analysis and integration with cloud services [44]. The IoT middleware must also be equipped with certain security functions, including user authentication and access control management [45].

The fourth layer is the application layer. This layer consists of applications that allow users to interact with physical objects [46]. These applications can be used to monitor and control the physical objects, as well as to visualize the data collected from the physical devices

5. KEY TECHNOLOGIES ENABLING THE INTERNET OF THINGS REVOLUTION

The Internet of Things (IoT) is a revolutionary concept that has reshaped industries and transformed the way we live and work. In simple terms, IoT is the network of physical devices, vehicles, appliances, and other objects equipped with sensors, software, and connectivity, allowing them to gather and share data. The IoT is a constantly evolving field. According to a study done by the Swiss Federal Institute of Technology, Zurich, smartphones and the growing number of connected objects mean that in ten years (2015-2025), 150 billion objects will be connected to each other, to the Internet and to several billion people.

A major advantage of IoT is its potential to boost efficiency and productivity[47]. By connecting devices and enabling real-time data monitoring and analysis, businesses can optimise operations, reduce costs and make informed decisions. From smart manufacturing processes that streamline production to smart homes that improve energy management, the IoT has the power to revolutionize industries.

Additionally, IoT can enhance our quality of life by making environments smarter and more responsive. From wearable health monitors that track vital signs to smart city systems that optimize traffic to ease congestion, IoT applications hold the potential to build safer and more sustainable communities. A variety of technologies are contributing to the IoT revolution.

5.1. Wireless Communication Technologies for Seamless Connectivity

In the digital age, staying connected has become an essential part of our daily lives. From smartphones to smart homes, wireless communication technologies play a vital role in ensuring seamless connectivity. In this section, we'll explore some of the key wireless technologies that keep us connected.

- **Wi-Fi**

In the digital age, wireless communication technologies have become an integral part of our daily lives. Wi-Fi is one such technology [48]. It offers exceptional speed and bandwidth capacity, enabling fast and efficient data transmission between IoT devices [49]. This is essential for applications needing real-time monitoring or instant response, such as smart homes or industrial automation systems. The wireless capability removes the need for physical connections, enabling seamless communication between devices. This not only improves convenience, but also flexibility in deploying IoT devices in a variety of environments. It also offers robust security features to protect sensitive data through advanced encryption protocols and authentication mechanisms [50]. In addition, WiFi's compatibility with a wide range of devices makes it highly versatile for IoT applications. Smartphones, laptops, smart appliances, and wearable devices can all connect effortlessly to a Wi-Fi network and interact with one another.

- **Bluetooth Low Energy (BLE)**

Bluetooth Low Energy (BLE) has established itself as a revolutionary wireless communication technology for low-power devices, offering efficient connectivity and opening up new possibilities in the IoT world. With its low power consumption and long battery life, BLE has become the preferred option for many applications where energy efficiency is essential. A major advantage of BLE is its capacity to connect and communicate effortlessly with a broad array of low-energy devices [51]. BLE allows devices like fitness trackers and smart home gadgets to transmit data efficiently while conserving energy. This makes it an ideal solution for applications in healthcare, wearables, home automation and many other areas of IoT.

- **Zigbee**

Zigbee, the wireless standard, is revolutionising the way we connect and control devices in smart homes and industrial applications. With its reliable mesh network architecture, Zigbee offers a range of features and benefits that make it an ideal choice for these environments. Its ability to create robust [52] and resilient mesh networks by allowing devices to communicate with each other over multiple paths, ensures that even if a device fails or loses connectivity, the network remains intact. This redundancy improves reliability and minimises downtime in critical applications. In smart homes, Zigbee enables seamless integration and interoperability between various devices [53] such as lamps, thermostats, sensors and household appliances. In a similar way, Zigbee is essential in industrial automation systems, offering reliable wireless connectivity for numerous applications. Whether monitoring equipment performance or optimising energy consumption in factories or warehouses, Zigbee ensures smooth communication between devices without the need for complex cabling installations. Furthermore, its low energy consumption makes Zigbee ideal for battery-operated devices in both smart home and industrial settings [52]. This feature not only extends battery life but also greatly reduces the need for maintenance.

- **Z-Wave**

Z-Wave technology is a wireless communication protocol that allows devices from various manufacturers to communicate and function together seamlessly. It offers a dependable and secure platform for smart home devices to connect and interact [54], [55]. Operating on a mesh network topology, each device in the network acts as a repeater, thereby extending the range and coverage of the network [54]. This ensures that signals can reach every corner of your home, eliminating dead zones or weak connections. Unlike other protocols that may be limited to specific manufacturers or brands, Z-Wave offers compatibility with a wide

range of devices from different suppliers [56]. In addition to interoperability, Z-Wave includes built-in encryption and authentication mechanisms, ensuring that your connected devices are secure from unauthorized access or tampering.

According to [57], Z-Wave is a wireless communication protocol used primarily to integrate radio frequency sensors and actuators and provide smart home and office automation services. It is a mesh network using low-energy radio waves to communicate from device to device, enabling wireless control of smart home devices such as smart lights, security systems, thermostats, sensors, smart locks and garage door openers. The Z-Wave brand and technology are owned by Silicon Labs [47]. More than 300 companies involved in the technology are members of the Z-Wave Alliance [47], [58]. Like other protocols and systems for the residential, commercial and building markets, a Z-Wave system can be controlled from a smartphone, tablet or computer, and locally via a smart speaker, wireless key fob or wall panel with a Z-Wave gateway or central control device acting as both hub and controller [59], [60].

Furthermore, according to [61], Z-Wave is designed to be interoperable between different manufacturers and versions. This interoperability is ensured by the Z-Wave certification programme administered by the Z-Wave Alliance consortium. Z-Wave certification guarantees that all Z-Wave products are compatible with each other, regardless of the brand, and ensures backward compatibility between different versions. The certification process includes technical testing, brand consistency programmes and the application of certification standards.

Finally, according to [62], Z-Wave ensures that your connected devices are protected against unauthorized access or tampering by built-in encryption and authentication mechanisms.

- **LoRaWAN**

LoRaWAN, or Long-Range Wide Area Network, is an advanced protocol that provides an innovative solution for long-distance communication in low-power sensor networks. According to [63], LoRaWAN is one of the Low Power Wide Area Network (LPWAN) technologies that has received particular attention from the research community in recent years. As one of the most popular technologies for low power IoT applications [64], LoRaWAN offers low-power, low-data-rate communications over a wide range of coverage areas.

5.2. Sensor Technologies

In the digital age, the power of IoT sensors and sensing technologies cannot be underestimated. These innovative tools have transformed the way we collect real-world data, enabling intelligent decision-making like never before. IoT sensors, also known as Internet of Things sensors, are at the forefront of this technological advancement. A sensor is a device that detects various types of signals—whether physical, chemical, or biological—and converts them into an electrical signal [65]. These sensors can be integrated into various objects and environments, creating a vast network of interconnected devices known as sensor networks. Sensor technologies are vital for collecting valuable data about our surroundings [66]. They can measure temperature, humidity, pressure, movement, light intensity and much more. Unlike manual methods of data collection that are prone to human error or bias, IoT sensors ensure consistent and accurate measurements. What's more, sensor networks enable seamless integration between physical objects and digital systems. This integration unlocks endless possibilities for intelligent decision-making across various sectors, including manufacturing, agriculture, healthcare, transportation, and smart cities.

6. CHALLENGES AND SECURITY CONSIDERATIONS WHEN IMPLEMENTING IOT SOLUTIONS

The implementation of Internet of Things (IoT) solutions has undoubtedly brought many benefits to various industries. However, it also brings its own set of challenges and security considerations that need to be taken into account.

6.1. Connectivity and Interoperability Challenges in IoT Implementation

In the ever-evolving world of IoT, one of the key challenges facing organisations is ensuring seamless connectivity and interoperability between devices [67].As the number of connected devices continues to grow, so does the complexity of managing their connectivity. Since these devices are created by different companies using various standards and technologies, connectivity becomes a challenge [17]. This can lead to issues such as data loss, communication failures and limited functionality. IoT implementations require gathering data from diverse sources and integrating it into a cohesive system for analysis and decision-making [68], [69]. However, different devices may use different protocols or formats to transmit data, making it difficult to integrate and analyse data effectively. These connectivity and interoperability challenges can hinder the seamless operation of IoT systems and limit their potential benefits. Here are some of the sources of these challenges:

- **Lack of Standardisation of IoT Protocols**

One of the main problems of the IoT is the lack of standardisation of protocols [70]. This poses significant problems for interconnected devices. As the Internet of Things continues to develop, the lack of uniformity in protocols hinders interoperability and creates barriers to communication between devices [71]. Without a common set of protocols, devices from different manufacturers may struggle to understand and interpret each other's data, leading to inefficiencies and limitations in functionality. In addition, this fragmentation of IoT protocols prevents seamless integration between different systems and platforms [72]. The use of multiple proprietary protocols makes it challenging to implement consistent and robust security measures across all connected devices [73].

- **Scalability Challenges in Large-Scale Deployments**

As more and more devices are connected to the network, managing large numbers of devices efficiently has become a daunting task. Resource constraints add further complexity to the equation. The need to scale IoT deployments is driven by the rising demand for connectivity and the vast amounts of data generated by these devices. Businesses across a range of sectors are leveraging IoT technology to gather valuable information, streamline operations and improve customer experience. However, as the number of connected devices grows exponentially, it becomes essential to manage them effectively.

One of the main scalability challenges is ensuring that all devices are smoothly integrated into the network without sacrificing performance or security. As the number of devices increases, issues such as bandwidth limitations and network congestion can arise. This can lead to slower response times and potential interruptions to operations. Resource constraints also pose significant challenges when scaling IoT deployments. The limited power sources and processing capabilities of individual devices can hamper their ability to process increasing amounts of data or perform complex tasks [50]. Optimising the use of resources becomes essential to ensure efficient operation without overloading a specific device or component.

Technological advances have led to innovative solutions for addressing scalability challenges in large-scale IoT deployments. Cloud-based platforms enable the centralized management and monitoring of a vast number of connected devices, providing flexibility in resource allocation based on demand [74], [75]. Additionally, edge computing has emerged as a promising solution by offloading certain processing tasks from cloud servers to local devices within the IoT deployment network [76]. This approach reduces latency and bandwidth requirements while improving overall system performance [77]. In addition, careful design considerations when planning the architecture play a crucial role in addressing scalability issues. Implementing scalable communication protocols, robust security measures and effective data management strategies ensures that an IoT deployment can grow seamlessly without compromising stability or functionality.

6.2. Data Security and Privacy in IoT Deployments

In the rapidly evolving world of IoT deployments, data security and privacy have become paramount issues. As more and more devices become interconnected, the risks of security breaches and data protection increase exponentially. With so much information being exchanged, there is an increased risk of unauthorised access or interception. This can lead to serious consequences, such as identity theft, financial fraud, or even the compromise of critical infrastructures. In addition, privacy considerations must also be taken into account when deploying IoT systems. Users expect their personal information to be handled with the highest level of care and transparency. However, given the sheer volume of data collected by IoT devices - ranging from location information to personal preferences - it is legitimate to be concerned about how this data is stored, used and shared. To meet these challenges, robust security measures must be implemented at all levels of an IoT deployment. This includes encryption protocols for data transmission, authentication mechanisms to guarantee the integrity of devices and regular updates to correct vulnerabilities, which can take many forms.

- **Vulnerabilities of Connected Devices and Networks**

In today’s interconnected world, the proliferation of IoT devices has brought numerous conveniences and opportunities. However, it has also introduced new vulnerabilities and risks. The security of connected devices and networks has become a critical concern, as hackers attempt to exploit these weaknesses for malicious purposes. The IoT connects billions of devices, people, and services, facilitating the exchange of information. With the growing use of IoT devices, IoT networks are increasingly susceptible to various security attacks. Deploying effective security and privacy protocols within IoT networks is essential to ensure confidentiality, authentication, access control, and integrity, among other key protections [78].

Hacking threats represent a significant risk to individuals and organisations [79], [80]. Cybercriminals can exploit vulnerabilities in connected devices and networks to gain unauthorised access, steal sensitive data or launch malicious attacks [81], [82]. This not only compromises privacy, but also poses potential physical risks in critical infrastructure sectors such as healthcare, transport, etc. Vulnerabilities related to unauthorised access compound the problem by allowing attackers to bypass authentication mechanisms and take control of connected devices or networks [83]. Weak passwords, obsolete firmware or unpatched software are common entry points for hackers seeking to gain unauthorised access [82].

- **Data Breaches and Unauthorised Access to Data**

A security breach is characterised by the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed [84]. In the digital age, data breaches and unauthorised access to data have become major concerns in IoT systems. This refers to any security event, whether caused by malicious intent or not, and regardless of whether it is intentional or accidental, that results in a breach of the integrity, confidentiality, or availability of personal data. The increasing interconnection of devices and the large amount of data generated make it imperative to deal with these risks effectively. Data breaches in IoT systems can have serious consequences, ranging from financial loss to reputational damage for individuals and organisations alike. Unauthorised access to sensitive information can lead to identity theft, fraud and even compromise national, regional and/or international security. To address these risks, it is crucial to put in place strong security measures, including encryption protocols, multi-factor authentication, and routine vulnerability assessments.

The potential applications of Artificial Intelligence (AI) in detecting and preventing data breaches are promising. AI-driven algorithms can process vast amounts of data in real time to detect anomalies or suspicious behavior that could signal a breach [85], [86]. In addition, AI can help improve threat intelligence by continuously monitoring emerging trends and patterns associated with data breaches. By leveraging machine learning algorithms, AI systems can adapt and evolve along with threats, providing organisations with an intelligent defence against unauthorised data access.

7. ENSURING ROBUST SECURITY MEASURES FOR IOT AND REGULATORY COMPLIANCE

The Internet of Things has become an integral part of our daily lives. From smart home gadgets to industrial equipment, the IoT has revolutionized how we engage with technology. However, with this increased connectivity comes the need for robust security measures and regulatory compliance. Ensuring IoT security best practice is crucial to protecting sensitive data and preventing unauthorised access. Given the large volume of data exchanged between devices, it is crucial to implement encryption protocols, robust authentication methods, and regular software updates to reduce potential vulnerabilities.

7.1. Implementation of Strong Authentication and Access Controls

In today's interconnected world, it is essential to implement strong security measures and ensure regulatory compliance for the successful deployment of the Internet of Things (IoT). As the use of IoT devices and networks grows, prioritizing security becomes crucial to safeguard sensitive data and prevent unauthorized access. A key aspect of securing IoT devices and networks is the implementation of strong authentication protocols and access controls [87]. By using robust authentication mechanisms, such as two factor authentication or biometric verification, the risk of unauthorised access can be significantly reduced [88]. These methods add an extra layer of security by requiring users to provide credentials in addition to traditional passwords.

Access control mechanisms also play a key role in securing IoT ecosystems. It is imperative to establish strict access policies that define who can access specific devices or networks and what levels of privileges they have. Implementing role-based access control (RBAC) can help ensure that only authorised people have the necessary permissions to interact with IoT devices [89]. Additionally, encryption technologies must be employed to secure the data transmitted between

IoT devices and networks [56]. Regulatory compliance is equally important in maintaining a secure IoT environment. Organisations need to keep up to date with relevant legislation and industry standards regarding data privacy and security. Compliance with regulations such as the General Data Protection Regulation (GDPR) ensures that personal information collected by IoT devices is handled securely and responsibly [90].

7.2. Regular Monitoring and Updating of IoT Systems and Firmware

Ensuring robust security measures and regulatory compliance is paramount with the Internet of Things. Given the rapid expansion of IoT devices, it is essential to prioritize regular monitoring and updating of IoT systems and firmware. Ensuring that IoT systems are consistently updated with the latest firmware can help fix vulnerabilities and safeguard against emerging cyber threats. Firmware updates often include patches that fix known security issues or vulnerabilities discovered in previous versions. Moreover, conducting regular vulnerability scans is crucial for ensuring the ongoing security of the IoT infrastructure. By periodically scanning a system for potential weaknesses or vulnerabilities, any potential risks can be identified and addressed before they can be exploited by malicious actors. Adopting this proactive strategy not only helps prevent security breaches but also guarantees adherence to industry regulations.

8. Areas of Application and Impact of the IoT in Various Industries

As Figure 3 shows, there are a wide range of application areas for the Internet of Things sectors. From healthcare to smart homes, from agriculture to manufacturing, transport and logistics, the applications and impact of the IoT are vast and promising. IoT is essential in various fields because it enables real-time data collection, monitoring, and automation, which can significantly improve efficiency, decision-making, and innovation. In industrial applications, IoT is pivotal for optimizing production, reducing downtime, and improving safety. By connecting machinery and equipment, IoT enables predictive maintenance which minimizes costly downtimes.

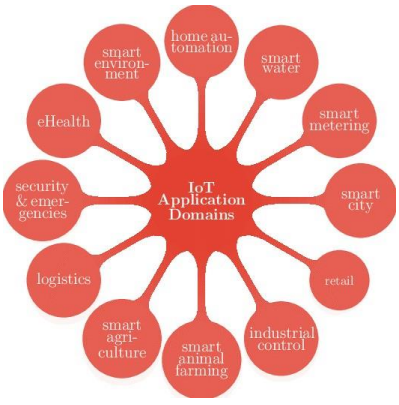

Figure 3. Areas of application of the IoT **[91]**

8.1. Smart Home

Smart homes are a branch of pervasive computing that involves the integration of intelligence into homes for the purposes of comfort, healthcare, security and energy saving [96]. It uses different technologies to equip the elements of the home for more intelligent remote monitoring and control and to enable them to interact harmoniously with each other in an influential way, so

that everyday tasks and activities in the home are automated without user intervention or with remote control, in an easier, more convenient, more efficient, safer and less expensive way. With the rapid progress of the IoT industry, technology companies have begun to develop and launch products that allow homeowners to control and monitor their home environment remotely. These include smart thermostats, voice-activated home assistants and automated lighting systems. IoT technology can also be used to manage energy consumption in homes and businesses [97]. Smart meters and connected devices allow energy consumption to be monitored more closely, which can help reduce energy costs.

8.2. Agriculture and Livestock

The Internet of Things (IoT) is revolutionising the agricultural sector. IoT technology has revolutionized agriculture by enabling precise automation and data collection. Farmers can now monitor soil and weather conditions, track crop growth, and automate processes such as irrigation and fertilization. Smart farming integrates a variety of advanced technologies, including wireless sensor networks, IoT, robotics, farm robots, drones, artificial intelligence, and cloud computing [98]. A key advantage of IoT in agriculture is the ability to gather realtime data in the field, which can be used to automate tasks like irrigation and fertilization, as well as monitor crop health and soil conditions [99][100]. Moreover, IoT sensors help farmers track livestock, providing vital information on animal health and location [33]. This data can then be used to optimise production processes and ensure that livestock are properly cared for. The IoT can also improve efficiency through automated processes, such as automated harvesting and automated pest control [101].

8.3. Transport and Logistics

The Internet of Things (IoT) is a technology that is rapidly transforming the logistics and transport sector. The IoT enables organisations to connect physical objects such as vehicles, sensors and machines to a network and track data in real time, improving efficiency, saving money and enhancing the customer experience [102]. In the logistics and transport sector, the IoT can be used to optimise transport routes, monitor shipments and reduce operational costs [103]. Many logistics and transport companies have begun to deploy IoT solutions to gain realtime visibility of their supply chain operations. Using sensors, connected devices and intelligent analytics, companies can better track shipments, optimise routes, reduce fuel costs and improve customer service [104], [105]. Additionally, AI and machine learning are being leveraged to automate processes and forecast customer demands, driving further efficiency and cost savings [103]. The use of IoT in logistics and transport is set to have a profound effect on the industry in the coming years. Companies that embrace this technology will be able to gain a competitive advantage and maximise the potential of their operations.

8.4. Manufacturing Process

As it evolves, the Internet of Things could revolutionise the manufacturing process. IoT technology has already made significant strides across various industries, and its potential to enhance the efficiency and productivity of manufacturing processes is vast. In the near future, IoT is expected to play a crucial role in optimizing manufacturing operations, including inventory management, quality assurance, and supply chain optimization [10], [106]. The use of IoT-enabled sensors, cloud computing, artificial intelligence (AI), machine learning (ML) and blockchain technology will enable more efficient and accurate production processes, and allow manufacturers to respond faster to customer demands [107], [108]. As the Internet of Things continues to evolve, its potential to revolutionise the manufacturing process is immense. Manufacturing processes have also been revolutionised by IoT technologies known as Industry

4.0 [103], [109]. Connected machines communicate with each other thanks to the sensors built into them. This facilitates predictive maintenance by detecting anomalies before breakdowns occur - avoiding costly downtime.

8.5. Improving Safety and Security

IoT technology can be leveraged to develop intelligent systems that not only detect security threats but also alert authorities and initiate preventative measures when a breach occurs [110]. In addition, IoT devices can be used to monitor security levels in homes and offices, as well as to help protect citizens from natural disasters.

9. CONCLUSION

The Internet of Things (IoT) is weaving an unprecedented digital web, transforming our everyday reality and paving the way for revolutionary applications. This increased connectivity is transforming industries, lifestyles and business opportunities, offering a multitude of benefits such as automation, resource optimisation, increased security and a better understanding of the world around us. Automation, the cornerstone of the IoT, enables resources to be managed more efficiently and costs to be reduced. From smart homes to connected factories, the IoT is revolutionising efficiency across the board. What's more, intelligent monitoring of environments is proving to be a crucial asset for public safety and asset protection. The IoT is not just about automation, it's a bridge to a better understanding of the world around us. By collecting and analysing real-time data from a multitude of sources, the IoT offers a holistic and accurate view of our environment. This in-depth knowledge enables us to make more informed decisions, anticipate needs and prevent problems. Interaction with the world becomes more intuitive and personalised thanks to the IoT. Connected devices adapt to our needs and habits, offering a fluid, customised user experience. This increased connectivity also opens the way to new forms of communication and collaboration, fostering the creation of intelligent, connected communities. However, the rise of the IoT is not without its challenges. Data security and privacy protection are major issues that need to be addressed proactively. What's more, seamlessly integrating the IoT into our existing systems and infrastructures requires careful planning and multi-sector collaboration. To help understand, secure and enhance IoT in the future, we propose to focus our efforts on the following areas:

- Exploring deep learning for IoT network optimization, anomaly detection and predictive maintenance.
- Designing embedded AI systems for low-power, resource-constrained IoT devices.
- Develop robust security architectures and protocols for IoT devices and networks.
- Exploring cryptography and blockchain techniques to guarantee the confidentiality and integrity of IoT data.

By working on these perspectives, we can better help shape a future where the IoT is used for the benefit of all.

REFERENCES

[1] Z. Abdussamad, I. Tweneboah Agyei, E. Sipahi Döngül, J. Abdussamad, R. Raj, and F. Effendy, 'Impact of Internet of Things (IOT) on Human Resource Management: A review', *Materials Today: Proceedings*, vol. 56, pp. 3534–3543, 2022, doi: 10.1016/j.matpr.2021.11.247.

[2] J. Zhang, M. Ma, P. Wang, and X. dong Sun, 'Middleware for the Internet of Things: A survey on requirements, enabling technologies, and solutions', *Journal of Systems Architecture*, vol. 117, p. 102098, Aug. 2021, doi: 10.1016/j.sysarc.2021.102098.

[3] H. P. Nguyen, P. Q. H. Le, V. V. Pham, X. P. Nguyen, D. Balasubramaniam, and A.-T. Hoang, 'Application of the Internet of Things in 3E (efficiency, economy, and environment) factor-based energy management as smart and sustainable strategy', *Energy Sources, Part A: Recovery, Utilization, and Environmental Effects*, pp. 1–23, Jul. 2021, doi: 10.1080/15567036.2021.1954110.

[4] M. Ben-Daya, E. Hassini, and Z. Bahroun, 'Internet of things and supply chain management: a literature review', *International Journal of Production Research*, vol. 57, no. 15–16, pp. 4719–4742, Aug. 2019, doi: 10.1080/00207543.2017.1402140.

[5] P. Nirmala, S. Ramesh, M. Tamilselvi, G. Ramkumar, and G. Anitha, 'An Artificial Intelligence enabled Smart Industrial Automation System based on Internet of Things Assistance', in *2022 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI)*, Jan. 2022, pp. 1–6. doi: 10.1109/ACCAI53970.2022.9752651.

[6] U. Tariq, I. Ahmed, A. K. Bashir, and K. Shaukat, 'A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review', *Sensors*, vol. 23, no. 8, Art. no. 8, Jan. 2023, doi: 10.3390/s23084117.

[7] E. Rodríguez, B. Otero, and R. Canal, 'A Survey of Machine and Deep Learning Methods for Privacy Protection in the Internet of Things', *Sensors*, vol. 23, no. 3, Art. no. 3, Jan. 2023, doi: 10.3390/s23031252.

[8] S. Y. Y. Tun, S. Madanian, and F. Mirza, 'Internet of things (IoT) applications for elderly care: a reflective review', *Aging Clin Exp Res*, vol. 33, no. 4, pp. 855–867, Apr. 2021, doi: 10.1007/s40520-020-01545-9.

[9] B.-X. Wang, J.-L. Chen, and C.-L. Yu, 'An AI-Powered Network Threat Detection System', *IEEE Access*, vol. 10, pp. 54029–54037, 2022, doi: 10.1109/ACCESS.2022.3175886.

[10] S. ZandiZand, *Impacts of IoT on Supply chain management : Case of E-commerce Firms*. 2023. Accessed: Oct. 28, 2024. [Online]. Available: https://urn.kb.se/resolve?urn=urn:nbn:se:uu:diva-502324

[11] Rachit, S. Bhatt, and P. R. Ragiri, 'Security trends in Internet of Things: a survey', *SN Appl. Sci.*, vol. 3, no. 1, p. 121, Jan. 2021, doi: 10.1007/s42452-021-04156-9.

[12] D. Sahu, B. Pradhan, A. Khasnobish, S. Verma, D. Kim, and K. Pal, 'The Internet of Things in Geriatric Healthcare', *Journal of Healthcare Engineering*, vol. 2021, pp. 1–16, Jul. 2021, doi: 10.1155/2021/6611366.

[13] A. M. Rahmani, S. Bayramov, and B. Kiani Kalejahi, 'Internet of Things Applications: Opportunities and Threats', *Wireless Pers Commun*, vol. 122, no. 1, pp. 451–476, Jan. 2022, doi: 10.1007/s11277-021-08907-0.

[14] S. Nižetić, P. Šolić, D. López-de-Ipiña González-de-Artaza, and L. Patrono, 'Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future', *J Clean Prod*, vol. 274, p. 122877, Nov. 2020, doi: 10.1016/j.jclepro.2020.122877.

[15] M. Ahmid and O. Kazar, 'A Comprehensive Review of the Internet of Things Security', *Journal of Applied Security Research*, vol. 18, no. 3, pp. 289–305, Jul. 2023, doi: 10.1080/19361610.2021.1962677.

[16] T. Domínguez-Bolaño, O. Campos, V. Barral, C. J. Escudero, and J. A. García-Naya, 'An overview of IoT architectures, technologies, and existing open-source projects', Jan. 27, 2024, *arXiv*: arXiv:2401.15441. Accessed: Oct. 28, 2024. [Online]. Available: http://arxiv.org/abs/2401.15441

[17] J. Ding, M. Nemati, C. Ranaweera, and J. Choi, 'IoT Connectivity Technologies and Applications: A Survey', *IEEE Access*, vol. 8, pp. 67646–67673, 2020, doi: 10.1109/ACCESS.2020.2985932.

[18] F. Alshehri and G. Muhammad, 'A Comprehensive Survey of the Internet of Things (IoT) and AI-Based Smart Healthcare', *IEEE Access*, vol. 9, pp. 3660–3678, 2021, doi: 10.1109/ACCESS.2020.3047960.

[19] M. Raj *et al.*, 'A survey on the role of Internet of Things for adopting and promoting Agriculture 4.0', *Journal of Network and Computer Applications*, vol. 187, pp. 1–29, Aug. 2021.

[20] M. G. Samaila, M. Neto, D. A. B. Fernandes, M. M. Freire, and P. R. M. Inácio, 'Challenges of securing Internet of Things devices: A survey', *Security and Privacy*, vol. 1, no. 2, p. e20, Mar. 2018, doi: 10.1002/spy2.20.

[21] A. Chatterjee *et al.*, 'Powering internet-of-things from ambient energy: a review', *J. Phys. Energy*, vol. 5, no. 2, p. 022001, Feb. 2023, doi: 10.1088/2515-7655/acb5e6.

[22] M. Alsudani *et al.*, 'Smart logistics with IoT-based enterprise management system using global manufacturing', *Journal of Combinatorial Optimization*, vol. 45, Jan. 2023, doi: 10.1007/s10878-022-00977-5.

[23] A. Soro, A. H. Ambe, and M. Brereton, 'Minding the Gap: Reconciling Human and Technical Perspectives on the IoT for Healthy Ageing', *Wireless Communications and Mobile Computing*, vol. 2017, pp. 1–15, 2017, doi: 10.1155/2017/7439361.

[24] R. Abdmeziem and D. Tandjaoui, 'Internet of Things: Concept, Building blocks, Applications and Challenges', Jan. 02, 2014, *arXiv*: arXiv:1401.6877. Accessed: Oct. 28, 2024. [Online]. Available: http://arxiv.org/abs/1401.6877

[25] H. Dadhaneeya, P. K. Nema, and V. K. Arora, 'Internet of Things in food processing and its potential in Industry 4.0 era: A review', *Trends in Food Science & Technology*, 2023, Accessed: Oct. 28, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0924224423002169

[26] M. Mansour *et al.*, 'Internet of things: A comprehensive overview on protocols, architectures, technologies, simulation tools, and future directions', *Energies*, vol. 16, no. 8, p. 3465, 2023.

[27] H. Ruotsalainen, G. Shen, J. Zhang, and R. Fujdiak, 'LoRaWAN physical layer-based attacks and countermeasures, a review', *Sensors*, vol. 22, no. 9, p. 3127, 2022.

[28] M. Bilal and S. Parveen, 'Synthesis of multi wall carbon nanotubes based electronic sensors for internet of things (IoT)', *J. Condens. Matter*, vol. 1, pp. 51–54, 2023.

[29] B. R. Payne and T. T. Abegaz, 'Securing the Internet of Things: Best Practices for Deploying IoT Devices', in *Computer and Network Security Essentials*, K. Daimi, Ed., Cham: Springer International Publishing, 2018, pp. 493–506. doi: 10.1007/978-3-31958424-9_28.

[30] B. Nguyen and L. Simkin, 'The Internet of Things (IoT) and marketing: the state of play, future trends and the implications for marketing', *Journal of Marketing Management*, vol. 33, no. 1–2, pp. 1–6, Jan. 2017, doi: 10.1080/0267257X.2016.1257542.

[31] M. Pyingkodi *et al.*, 'Sensor Based Smart Agriculture with IoT Technologies: A Review', in *2022 International Conference on Computer Communication and Informatics (ICCCI)*, Jan. 2022, pp. 1–7. doi: 10.1109/ICCCI54379.2022.9741001.

[32] A. Razzaq, A. Ahmad, A. W. Malik, M. Fahmideh, and R. A. Ramadan, 'Software engineering for internet of underwater things to analyze oceanic data', *Internet of Things*, vol. 24, Jan. 2023, doi: 10.1016/j.iot.2023.100893.

[33] S. Mishra and S. Sharma, 'Advanced contribution of IoT in agricultural production for the development of smart livestock environments', *Internet of Things*, vol. 22, p. 100724, Jul. 2023, doi: 10.1016/j.iot.2023.100724.

[34] P. Sethi and S. R. Sarangi, 'Internet of Things: Architectures, Protocols, and Applications', *Journal of Electrical and Computer Engineering*, vol. 2017, pp. 1–25, 2017, doi: 10.1155/2017/9324035.

[35] M. Bhavsar, K. Roy, J. Kelly, and O. Olusola, 'Anomaly-based intrusion detection system for IoT application', *Discov Internet Things*, vol. 3, no. 1, p. 5, May 2023, doi: 10.1007/s43926-023-00034-5.

[36] 'JAKO202213042366210.pdf'. Accessed: Oct. 28, 2024. [Online]. Available: https://koreascience.kr/article/JAKO202213042366210.pdf

[37] F. L. Mouël and L. Maille, 'IoT Design - Quelles architectures et couches logicielles pour l'IoT ?', report, INSA Lyon ; SPIE ICS, 2020. Accessed: Oct. 28, 2024. [Online]. Available: https://inria.hal.science/hal-03020321

[38] S. Parween, S. Z. Hussain, M. A. Hussain, and A. Pradesh, 'A survey on issues and possible solutions of cross-layer design in Internet of Things', *Int. J. Comput. Networks Appl*, vol. 8, no. 4, p. 311, 2021.

[39] S. K. Mousavi, A. Ghaffari, S. Besharat, and H. Afshari, 'Security of internet of things based on cryptographic algorithms: a survey', *Wireless Netw*, vol. 27, no. 2, pp. 1515– 1555, Feb. 2021, doi: 10.1007/s11276-020-02535-5.

[40] N. Singh, 'IoT enabled HELMET to safeguard the health of mine workers', Accessed: Oct. 28, 2024. [Online]. Available: https://www.academia.edu/82996142/IoT_enabled_HELMET_to_safeguard_the_health_of_mine_workers

[41] K. Zeeshan, T. Hämäläinen, and P. Neittaanmäki, 'Internet of Things for Sustainable Smart Education: An Overview', *Sustainability*, vol. 14, no. 7, Art. no. 7, Jan. 2022, doi: 10.3390/su14074293.

[42] Q. Alfalouji *et al.*, 'IoT Middleware Platforms for Smart Energy Systems: An Empirical Expert Survey', *Buildings*, vol. 12, no. 5, Art. no. 5, May 2022, doi: 10.3390/buildings12050526.

[43] D. A. N. Venkatesh, 'Connecting the Dots: Internet of Things and Human Resource Management', Feb. 08, 2017, *Social Science Research Network, Rochester, NY*: 2913400. Accessed: Oct. 28, 2024. [Online]. Available: https://papers.ssrn.com/abstract=2913400

[44] Z. Ali *et al.*, 'A Generic Internet of Things (IoT) Middleware for Smart City Applications', *Sustainability*, vol. 15, no. 1, Art. no. 1, Jan. 2023, doi: 10.3390/su15010743.

[45] H. Garg and M. Dave, 'Securing User Access at IoT Middleware Using Attribute Based Access Control', in *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Jul. 2019, pp. 1–6. doi: 10.1109/ICCCNT45670.2019.8944879.

[46] D. Alulema, J. Criado, L. Iribarne, A. J. Fernandez Garcia, and R. Ayala, 'SI4IoT: A methodology based on models and services for the integration of IoT systems', *Future Generation Computer Systems*, vol. 143, pp. 132–151, Jun. 2023, doi: 10.1016/j.future.2023.01.023.

[47] Z. Łukasik and A. Ushakov, 'Comparative analysis of data transmission technologies in industrial systems of the Internet of things (IoT)', *Journal of Automation, Electronics and Electrical Engineering*, vol. 2, no. 1, pp. 31–39, 2020.

[48] C. Deng *et al.*, 'IEEE 802.11be Wi-Fi 7: New Challenges and Opportunities', *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2136–2166, 2020, doi: 10.1109/COMST.2020.3012715.

[49] D. Eridani, A. F. Rochim, and F. N. Cesara, 'Comparative Performance Study of ESPNOW, Wi-Fi, Bluetooth Protocols based on Range, Transmission Speed, Latency, Energy Usage and Barrier Resistance', in *2021 International Seminar on Application for Technology of Information and Communication (iSemantic)*, Sep. 2021, pp. 322–328. doi: 10.1109/iSemantic52711.2021.9573246.

[50] W. C. Tan and M. S. Sidhu, 'Review of RFID and IoT integration in supply chain management', *Operations Research Perspectives*, vol. 9, p. 100229, 2022.

[51] A. E. Alattar and S. Mohsen, 'A Survey on Smart Wearable Devices for Healthcare Applications', *Wireless Pers Commun*, vol. 132, no. 1, pp. 775–783, Sep. 2023, doi: 10.1007/s11277-023-10639-2.

[52] K. F. Haque, A. Abdelgawad, and K. Yelamarthi, 'Comprehensive Performance Analysis of Zigbee Communication: An Experimental Approach with XBee S2C Module', *Sensors*, vol. 22, no. 9, Art. no. 9, Jan. 2022, doi: 10.3390/s22093245.

[53] F. K. Shaikh, S. Karim, S. Zeadally, and J. Nebhen, 'Recent Trends in Internet-ofThings-Enabled Sensor Technologies for Smart Agriculture', *IEEE Internet of Things Journal*, vol. 9, no. 23, pp. 23583–23598, Dec. 2022, doi: 10.1109/JIOT.2022.3210154.

[54] A. K. S, S. S, A. K. S, A. R, and A. M. A, 'Enhanced and Secured Smart Home using ZWave Technology', in *2023 2nd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA)*, Jun. 2023, pp. 1–6. doi: 10.1109/ICAECA56562.2023.10200829.

[55] D. Swessi and H. Idoudi, 'A Survey on Internet-of-Things Security: Threats and Emerging Countermeasures', *Wireless Pers Commun*, vol. 124, no. 2, pp. 1557–1592, May 2022, doi: 10.1007/s11277-021-09420-0.

[56] P. Williams, I. Dutta, H. Daoud, and M. Bayoumi, 'A Survey on Security in Internet of Things with a Focus on the Impact of Emerging Technologies', *Internet of Things*, vol. 19, p. 100564, Jul. 2022, doi: 10.1016/j.iot.2022.100564.

[57] C. W. Badenhop, S. R. Graham, B. W. Ramsey, B. E. Mullins, and L. O. Mailloux, 'The Z-Wave routing protocol and its security implications', *Comput. Secur.*, vol. 68, no. C, pp. 112–129, Jul. 2017, doi: 10.1016/j.cose.2017.04.004.

[58] F. Y. Aslan and B. Aslan, 'Comparison of IoT Protocols with OSI and TCP/IP Architecture', *International Journal of Engineering Research and Development*, vol. 15, no. 1, pp. 333–343, 2023.

[59] D. Bastos, M. Shackleton, and F. El-Moussa, 'Internet of Things: A Survey of Technologies and Security Risks in Smart Home and City Environments', in *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, London, UK: Institution of Engineering and Technology, 2018, p. 30 (7 pp.)-30 (7 pp.). doi: 10.1049/cp.2018.0030.

[60] E. Fraccaroli and D. Quaglia, 'Engineering IoT Networks', in *Intelligent Internet of Things*, F. Firouzi, K. Chakrabarty, and S. Nassif, Eds., Cham: Springer International Publishing, 2020, pp. 97–171. doi: 10.1007/978-3-030-30367-9_3.

[61] S. J. Danbatta and A. Varol, 'Comparison of Zigbee, Z-Wave, Wi-Fi, and bluetooth wireless technologies used in home automation', in *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*, IEEE, 2019, pp. 1–5. Accessed: Oct. 29, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8757472/

[62] C. Braghin, M. Lilli, and E. Riccobene, 'A model-based approach for vulnerability analysis of IoT security protocols: The Z-Wave case study', *Computers & Security*, vol. 127, p. 103037, 2023.

[63] J. Haxhibeqiri, E. De Poorter, I. Moerman, and J. Hoebeke, 'A survey of LoRaWAN for IoT: From technology to application', *Sensors*, vol. 18, no. 11, p. 3995, 2018.

[64] K. Rose, S. Eldridge, and L. Chapin, 'The internet of things: An overview', *The internet society (ISOC)*, vol. 80, no. 15, pp. 1–53, 2015.

[65] B. C. Patel, G. R. Sinha, and N. Goel, 'Introduction to sensors', in *Advances in Modern Sensors: Physics, design, simulation and applications*, IOP Publishing Bristol, UK, 2020, pp. 1–1. Accessed: Oct. 29, 2024. [Online]. Available: https://iopscience.iop.org/book/edit/978-0-7503-2707-7/chapter/bk978-0-7503-27077ch1

[66] M. A. Ramírez-Moreno *et al.*, 'Sensors for sustainable smart cities: A review', *Applied Sciences*, vol. 11, no. 17, p. 8198, 2021.

[67] L. Fetahu, A. Maraj, and A. Havolli, 'Internet of Things (IoT) benefits, future perspective, and implementation challenges', in *2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO)*, IEEE, 2022, pp. 399–404. Accessed: Oct. 29, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9803487/

[68] X. Huang, Y. Liu, L. Huang, E. Onstein, and C. Merschbrock, 'BIM and IoT data fusion: The data process model perspective', *Automation in Construction*, vol. 149, p. 104792, 2023.

[69] M. E. E. Alahi *et al.*, 'Integration of IoT-enabled technologies and artificial intelligence (AI) for smart city scenario: recent advancements and future trends', *Sensors*, vol. 23, no. 11, p. 5206, 2023.

[70] S. A. Al-Qaseemi, H. A. Almulhim, M. F. Almulhim, and S. R. Chaudhry, 'IoT architecture challenges and issues: Lack of standardization', in *2016 Future technologies conference (FTC)*, IEEE, 2016, pp. 731–738. Accessed: Oct. 29, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7821686/

[71] S. A. Al-Qaseemi, H. A. Almulhim, M. F. Almulhim, and S. R. Chaudhry, 'IoT architecture challenges and issues: Lack of standardization', in *2016 Future technologies conference (FTC)*, IEEE, 2016, pp. 731–738. Accessed: Oct. 29, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7821686/

[72] M. Aly, F. Khomh, Y.-G. Guéhéneuc, H. Washizaki, and S. Yacout, 'Is Fragmentation a Threat to the Success of the Internet of Things?', *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 472–487, 2018.

[73] C. Tomazzoli, S. Scannapieco, and M. Cristani, 'Internet of Things and artificial intelligence enable energy efficiency', *J Ambient Intell Human Comput*, vol. 14, no. 5, pp. 4933–4954, May 2023, doi: 10.1007/s12652-020-02151-3.

[74] T. Alam, 'Cloud-based IoT applications and their roles in smart cities', *Smart Cities*, vol. 4, no. 3, pp. 1196–1219, 2021.

[75] B. H. Banimfreg, 'A comprehensive review and conceptual framework for cloud computing adoption in bioinformatics', *Healthcare Analytics*, vol. 3, p. 100190, 2023.

[76] L. Kong *et al.*, 'Edge-computing-driven Internet of Things: A Survey', *ACM Comput. Surv.*, vol. 55, no. 8, pp. 1–41, Aug. 2023, doi: 10.1145/3555308.

[77] J. Almutairi and M. Aldossary, 'Resource Management and Task Offloading Issues in the Edge-Cloud Environment.', *Intelligent Automation & Soft Computing*, vol. 30, no. 1, 2021, Accessed: Oct. 29, 2024. [Online]. Available: https://www.researchgate.net/profile/Mohammad-Aldossary 3/publication/353604991_Resource_Management_and_Task_Offloading_Issues_in_the_ Edge-Cloud_Environment/links/61054f0e1e95fe241a9e4759/Resource-Managementand-Task-Offloading-Issues-in-the-Edge-Cloud-Environment.pdf

[78] M. A. Razzaq, S. H. Gill, M. A. Qureshi, and S. Ullah, 'Security issues in the Internet of Things (IoT): A comprehensive study', *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 6, p. 383, 2017.

[79] Y. Li and Q. Liu, 'A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments', *Energy Reports*, vol. 7, pp. 8176–8186, 2021.
[80] F. Cremer *et al.*, 'Cyber risk and cybersecurity: a systematic review of data availability', *The Geneva papers on risk and insurance. Issues and practice*, vol. 47, no. 3, p. 698, 2022.
[81] M. Alawida, A. E. Omolara, O. I. Abiodun, and M. Al-Rajab, 'A deeper look into cybersecurity issues in the wake of Covid-19: A survey', *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 10, pp. 8176–8206, 2022.
[82] J.-P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, 'Ethical hacking for IoT: Security issues, challenges, solutions and recommendations', *Internet of Things and Cyber-Physical Systems*, vol. 3, pp. 280–308, 2023.
[83] Z. Muhammad, Z. Anwar, A. R. Javed, B. Saleem, S. Abbas, and T. R. Gadekallu, 'Smartphone Security and Privacy: A Survey on APTs, Sensor-Based Attacks, SideChannel Attacks, Google Play Attacks, and Defenses', *Technologies*, vol. 11, no. 3, p. 76, 2023.
[84] B. M. A. Wahhab, 'The Concept of Online Privacy and Personal Data Protection in Iraq: A Way Forward', *Journal of Positive School Psychology*, vol. 6, no. 3, pp. 6870–6881, 2022.
[85] J. P. Bharadiya, 'AI-driven security: how machine learning will shape the future of cybersecurity and web 3.0', *American Journal of Neural Networks and Applications*, vol. 9, no. 1, pp. 1–7, 2023.
[86] S. Ariyo and E. Olufemi, 'The Future of Cyber Security in An AI-Driven World', *The Cable*, 2023, Accessed: Oct. 29, 2024. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4423835
[87] W. Alnahari and M. T. Quasim, 'Authentication of IoT device and IoT server using security key', in *2021 International Congress of Advanced Technology and Engineering (ICOTEN)*, IEEE, 2021, pp. 1–9. Accessed: Oct. 29, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9493492/
[88] S. P. Otta, S. Panda, M. Gupta, and C. Hota, 'A systematic survey of multi-factor authentication for cloud infrastructure', *Future Internet*, vol. 15, no. 4, p. 146, 2023.
[89] T. Zaidi, M. Usman, M. U. Aftab, H. Aljuaid, and Y. Y. Ghadi, 'Fabrication of flexible role-based access control based on blockchain for internet of things use cases', *IEEE Access*, 2023, Accessed: Oct. 29, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10261179/
[90] M. Barati, O. Rana, I. Petri, and G. Theodorakopoulos, 'GDPR compliance verification in internet of things', *IEEE access*, vol. 8, pp. 119697–119709, 2020.
[91] R. Petrolo, V. Loscrì, and N. Mitton, 'Towards a smart city based on cloud of things, a survey on the smart city vision and paradigms', *Trans. Emerging Tel. Tech.*, vol. 28, no. 1, p. e2931, Jan. 2017, doi: 10.1002/ett.2931.
[92] R. K. Kaushal *et al.*, 'Using Mobile Computing to Provide a Smart and Secure Internet of Things (IoT) Framework for Medical Applications', *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–13, Oct. 2022, doi: 10.1155/2022/8741357.
[93] M. Kumar *et al.*, 'Healthcare Internet of Things (H-IoT): Current trends, future prospects, applications, challenges, and security issues', *Electronics*, vol. 12, no. 9, p. 2050, 2023.
[94] P. Mishra and G. Singh, 'Internet of medical things healthcare for sustainable smart cities: current status and future prospects', *Applied Sciences*, vol. 13, no. 15, p. 8869, 2023.
[95] M. Dadkhah, M. Mehraeen, F. Rahimnia, and K. Kimiafar, 'Use of internet of things for chronic disease management: an overview', *Journal of Medical Signals & Sensors*, vol. 11, no. 2, pp. 138–157, 2021.
[96] M. R. Alam, M. B. I. Reaz, and M. A. M. Ali, 'A review of smart homes—Past, present, and future', *IEEE transactions on systems, man, and cybernetics, part C (applications and reviews)*, vol. 42, no. 6, pp. 1190–1203, 2012.
[97] K. M. Al-Obaidi, M. Hossain, N. A. Alduais, H. S. Al-Duais, H. Omrany, and A. Ghaffarianhoseini, 'A review of using IoT for energy efficient buildings and cities: a built environment perspective', *Energies*, vol. 15, no. 16, p. 5991, 2022.
[98] F. K. Shaikh, S. Karim, S. Zeadally, and J. Nebhen, 'Recent trends in internet-of-thingsenabled sensor technologies for smart agriculture', *IEEE Internet of Things Journal*, vol. 9, no. 23, pp. 23583–23598, 2022.
[99] M. Dhanaraju, P. Chenniappan, K. Ramalingam, S. Pazhanivelan, and R. Kaliaperumal, 'Smart farming: Internet of Things (IoT)-based sustainable agriculture', *Agriculture*, vol. 12, no. 10, p. 1745, 2022.

[100] D. A. Zyukin and I. V. Khasambiev, 'IoT as a high degree of autonomy system', in *Journal of Physics: Conference Series*, IOP Publishing, 2022, p. 012020. Accessed: Oct. 29, 2024. [Online]. Available: https://iopscience.iop.org/article/10.1088/17426596/2176/1/012020/meta

[101] P. Rajak, A. Ganguly, S. Adhikary, and S. Bhattacharya, 'Internet of Things and smart sensors in agriculture: Scopes and challenges', *Journal of Agriculture and Food Research*, vol. 14, p. 100776, 2023.

[102] D. Oladimeji, K. Gupta, N. A. Kose, K. Gundogan, L. Ge, and F. Liang, 'Smart transportation: an overview of technologies and applications', *Sensors*, vol. 23, no. 8, p. 3880, 2023.

[103] M. Soori, B. Arezoo, and R. Dastres, 'Artificial intelligence, machine learning and deep learning in advanced robotics, a review', *Cognitive Robotics*, vol. 3, pp. 54–70, 2023.

[104] V. Selvakumar, S. Sivanandan, V. Saillaja, and A. Subbarayudu, 'Smart Asset Management: Tracking and Optimizing Assets with IoT Sensors', in *2023 2nd International Conference on Edge Computing and Applications (ICECAA)*, IEEE, 2023, pp. 1354–1358. Accessed: Oct. 29, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10212115/

[105] L. Zhou, 'The Convergence of IoT, Big Data, and International Logistics: Enhancing Supply Chain Efficiency', *Law and Economy*, vol. 2, no. 9, pp. 35–40, 2023.

[106] A. GAMAL, 'loT in supply chain management', *IMPLEMENTATION OF DISRUPTIVE TECHNOLOGIES IN SUPPLY CHAIN MANAGEMENT*, pp. 103–132, 2023.

[107] A. Shrivastava, K. M. Krishna, M. L. Rinawa, M. Soni, G. Ramkumar, and S. Jaiswal, 'Inclusion of IoT, ML, and blockchain technologies in next generation industry 4.0 environment', *Materials Today: Proceedings*, vol. 80, pp. 3471–3475, 2023.

[108] M. S. Rahman, T. Ghosh, N. F. Aurna, M. S. Kaiser, M. Anannya, and A. S. Hosen, 'Machine learning and internet of things in industry 4.0: A review', *Measurement: Sensors*, vol. 28, p. 100822, 2023.

[109] T. C. Ng, S. Y. Lau, M. Ghobakhloo, M. Fathi, and M. S. Liang, 'The application of industry 4.0 technological constituents for sustainable manufacturing: A content-centric review', *Sustainability*, vol. 14, no. 7, p. 4327, 2022.

[110] A. Mosenia and N. K. Jha, 'A comprehensive study of security of internet-of-things', *IEEE Transactions on emerging topics in computing*, vol. 5, no. 4, pp. 586–602, 2016.

AUTHORS

Jean Pierre Ntayagabiri obtained his Master's degree in Computer Engineering. He is currently a Ph.D. student at the Research Center for Infrastructure, Environment, and Technologies at the University of Burundi. His research focuses on machine learning, the Internet of Things, and cybersecurity.

Pr. Youssef BENTALEBis a professor and research director with a Ph.D. in applied mathematics and computer science. His expertise covers modeling and digital simulation, signal and image processing, security, and big data analysis. He has over ten years of professional experience in human resources management, particularly in database administration and IT management. He is also the President of the Moroccan Center for Polytechnic Research and Innovation (CMRPI), Director of the International Journal of Scientific Research and Innovation (IJRSI-CMRPI), Editor-in-Chief of the JCCE Journal, and a member of the EECOMAS research laboratory.

Pr. Jeremie Ndikumagenge is a lecturer and researcher at the University of Burundi, where he is responsible for the Master's program in Computer Engineering. His main research areas include information systems, real-time systems, and data structures.

Hind El Makhtoum earned her engineering degree in Electronics and Telecommunications from ENSEM in Casablanca, Morocco. She is currently a Ph.D. researcher at the Engineering Sciences Laboratory of Ibn Tofaïl University - ENSA in Kenitra, Morocco. Her research focuses on networks, security, and the Internet of Things.