Alkadhim Journal for Computer Science, Vol. 2, No. 1 (2024)

Open Access ISSN: 3007-1437 (Online), ISSN: 3007-1429 (Print)

IRAQI Academic Scientific Journals

Alkadhim Journal for Computer Science (KJCS)

Journal Homepage: https://alkadhum-col.edu.iq/JKCEAS

KJCS ALKADHIM JOURNAL FOR COMPUTER SCIENCE

Internet of Things: Architecture, Technologies, Applications, and Challenges

[1]Sabah Abdulazeez Jebur*, [1]Abbas Khalifa Nawar, [1]Nawar Banwan Hassan, [2]Imad Tareq

[1] Department of Computer Techniques Engineering, Imam Al-Kadhum College (IKC), Baghdad, Iraq.

[2]Faculty of Computer and Information Sciences, Ain Shams University, Cairo, Egypt

Article information

Article history:

Received: January, 13, 2024

Accepted: February, 22, 2024

Available online: March, 14, 2024

Keywords:

RFID,

embedded systems,

healthcare,

IoT.

Corresponding Author:

Sabah Abdulazeez Jebur

sabah.abdulazeez@alkadhum-col.edu.iq

DOI:

Abstract

A subset of cutting-edge information technology is the Internet of things (IoT). IoT refers to a network of physical objects with sensors attached that are linked to the Internet via LAN and WAN networking techniques. It is now commonly used to sense the environment and gather data in a variety of settings, including smart cities, healthcare, intelligent transportation, smart homes, and other structures. The IoT network architecture, core technology, and significant applications were outlined in this overview. The sensing layer, transport layer, and application layer are separated in the IoT network architecture. The essential technologies are embedded systems, network connectivity, sensor, and radio frequency identification (RFID) technology. IoT implementation in logistics still faces challenges despite the potential advantages. The utilization of technology in the IoT context is a topic with many open studies, which are also examined in this paper.

1. Introduction

The term "Internet of things" (IoT) was first used by an individual in the Radio Frequency Identification (RFID) hacking community in 1999. In recent years, the development of mobile equipment, integrated connectivity, virtualization, and data analytics has made the IoT paradigm more applicable to real-world situations[1]. The term "Internet of things" (IoT) refers to a particular kind of network that connects anything to the Internet based on predetermined protocols using data sensing equipment to transfer data and carry out communications to achieve smart recognitions, positioning, tracing, monitoring, and administration[1]. Another definition of IoT is a network of physical devices whose data is routinely collected, processed, and used to trigger action, offering a wealth of knowledge for governance, strategy, and choice. The Internet of Things (IoT) affects the government, research, economy, education, and mankind [2]. The effect of the internet of things on enabling anything to communicate with the internet at any time and from any location to offer any services by any network to everyone is shown in figure 1.

The integration of Artificial Intelligence (AI) in the Internet of Things (IoT) significantly enhances the capabilities of IoT systems, especially in anomaly detection. AI-driven anomaly detection in IoT involves the use of sophisticated algorithms to analyze the vast amounts of data generated by IoT devices, identifying unusual patterns or deviations that could indicate operational issues, security breaches, or system failures[3].

In our assessment, IoT is examined, along with its network architecture, core technology, and several major applications.

The Internet of Things (IoT) has emerged as one of the most transformative and rapidly evolving technological paradigms of recent times. IoT refers to a system of interconnected physical objects or "things" embedded with sensors, software, electronics, and connectivity that enables data exchange between devices over the internet [1]. The past decade has witnessed explosive growth in IoT adoption across application domains such as smart homes, healthcare, transportation, manufacturing, and more. Recent reports estimate that there will be over 30 billion IoT devices worldwide by 2025, up from around 11 billion in 2018 [2]. This massive proliferation of smart, connected devices is transforming supply chains, business models, city infrastructure and more.

IoT applications leverage advanced data analytics and intelligence at the edge to derive actionable insights from the treasure trove of data generated by IoT networks. Key enablers of IoT include ubiquitous connectivity, inexpensive sensors, cloud computing platforms as well as advances in fields like machine learning and edge computing [3]. While IoT innovation has tremendous potential for impact, it also poses formidable challenges related to security, privacy, technical infrastructure and more that must be overcome [4].

The Internet of Things (IoT) has experienced explosive growth over the past decade, with projections of massive future proliferation. Recent reports forecast that there will be over 30 billion connected IoT devices globally by 2025, up from 11.7 billion in 2018 [2]. This anticipated near-tripling of connected devices underscores the breakneck growth of IoT adoption. In addition to the sheer volume of connected devices, the economic impact of IoT is similarly impressive. IoT is forecast to contribute an estimated $13 trillion to the global economy by 2030, highlighting its immense disruptive potential [7]. Specific domains expected to experience high IoT growth include manufacturing, with over $3 trillion of projected economic value by 2025, and healthcare, with IoT systems projected to save $300 billion annually [8]. These striking statistics and forecasts demonstrate that IoT is one of the most profoundly transformative and strategic technological shifts of our time. The rapid proliferation of inexpensive, connected devices is changing consumer experiences, business models, supply chains and potentially entire industries. This paper reviews the technological innovations powering this IoT revolution and its emerging applications.

The Internet of Things (IoT) has experienced explosive growth over the past decade, with projections of massive future proliferation. Recent reports forecast that there will be over 30 billion connected IoT devices globally by 2025, up from 11.7 billion in 2018 [2]. This anticipated near-tripling of connected devices underscores the breakneck growth of IoT adoption. In addition to the sheer volume of connected devices, the economic impact of IoT is similarly impressive. IoT is forecast to contribute an estimated $13 trillion to the global economy by 2030, highlighting its immense disruptive potential [7]. Specific domains expected to experience high IoT growth include manufacturing, with over $3 trillion of projected economic value by 2025, and healthcare, with IoT systems projected to save $300 billion annually [8]. These striking statistics and forecasts demonstrate that IoT is one of the most profoundly transformative and strategic technological shifts of our time. The rapid proliferation of inexpensive, connected devices is changing consumer experiences, business models, supply chains and potentially entire industries. This paper reviews the technological innovations powering this IoT revolution and its emerging applications.

While there have been previous survey papers reviewing IoT architectures, technologies and applications [5,6], the IoT landscape has evolved significantly in recent years warranting an updated look. The motivations for this review are threefold:

- Provide comprehensive coverage of the latest developments in IoT architectures and enabling technologies. Many new innovations have emerged since past reviews, including breakthroughs in fields like edge computing, 5G networks, AI/ML, blockchain, etc[4].

- Highlight cutting-edge IoT applications and use cases that are being adopted since earlier reviews. For example, applications in smart homes, autonomous vehicles, smart factories, etc[5].

- Discuss current challenges and open research problems in IoT adoption. As the field matures, new technical and ethical challenges have arisen that require solutions.

In summary, this paper aims to bring readers fully up to date on the state of IoT technologies, architectures, applications and challenges. It provides a holistic overview of the latest IoT innovations and developments that have occurred since previous reviews on this topic. For researchers and practitioners alike, this updated perspective will help situate their work in the broader IoT landscape and identify promising new directions for investigation.

This paper aims to provide a comprehensive updated review of IoT architectures, core technologies, applications as well as ongoing challenges. While there have been previous survey papers on IoT technologies and applications [5,6], the landscape has evolved significantly in recent years warranting an updated review. This paper summarizes the latest developments in areas like IoT architectures, enabling technologies, applications in smart cities, homes, healthcare and more. It also highlights key issues and research gaps that still need to be addressed to successfully unlock the potential of IoT.

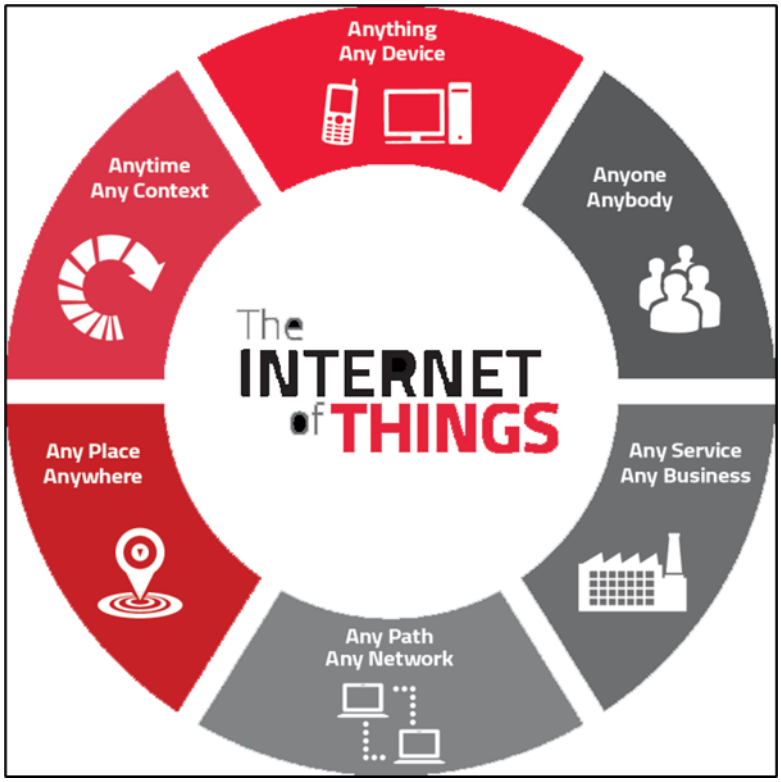

Figure 1. IoT Concept

2. The network architecture of IoT

The overall architecture of an IoT network was organized into three layers: sensing, transport, and application. The operating system and protection were handled in all three levels, as shown in Figure (2), to guarantee that each step works smoothly

The sensing layer consists of many sensors which are worked on data collection of things and matter recognition. These sensors are including temperature, humidity, camera, GPS sensors, etc.[6].

The sensing layer collects data by sensing these terminals such as temperature and humidity, O2 and CO2 concentration, geographical location, etc. RFID and sensor networks were considered the main technologies of the sensing layer.

The transport layer is responsible for transferring and processing information that is collected by the sensing layer. It is composed of a variety of networks such as WIFI, WAN, Cloud computing platform, 3G communication, etc. The main technologies of the transport layer are long-distance wired and wireless communication protocol, network integration technology, and magnanimous intelligent information processing technology.

The application layer is responsible for data analysis and producing helpful information for users by using intelligent computing technologies such as data mining, fuzzy recognition, cloud computing, etc. Applications of the Internet of things are very wide, for example, smart homes or building, smart industry, smart health, smart transportation, and smart city[6].

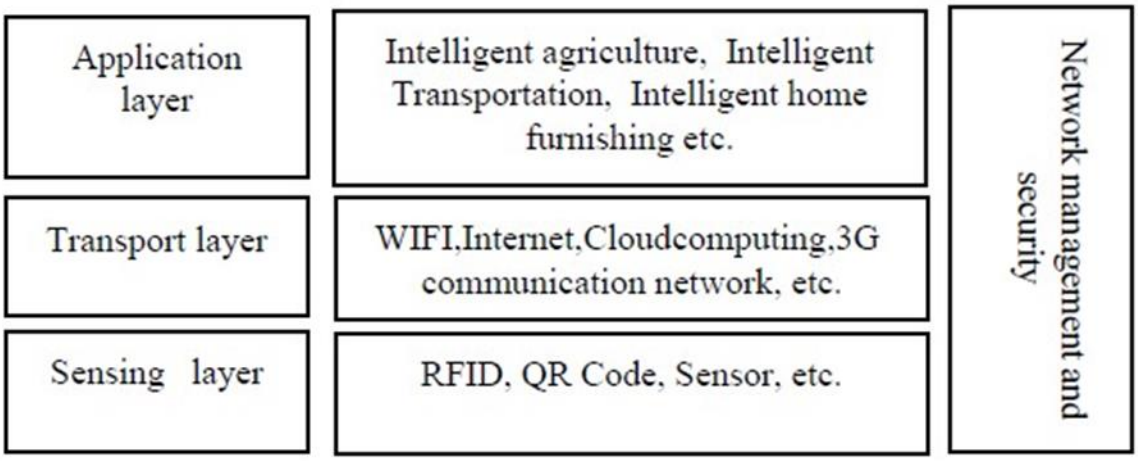

Figure 2. The layers architecture of IoT

Introduce 2-3 alternate IoT architecture models from literature, such as:[7]

- 5-layer architecture: sensing, networking, computing, application, business layers
- SOA-based architecture: things, aggregators, services layers
- Fog computing architecture: edge, fog, cloud layers

2.1. layer architecture

An alternate IoT architecture model proposed in some research consists of 5 layers - sensing, networking, computing, application, and business[8]. The sensing, networking, and application layers are similar to those described previously. The computing layer provides middleware for data processing, storage, and management of the sensors and devices. This layer relies on cloud computing infrastructure to provide the underlying resources

for running analytics and machine learning algorithms on the data. The topmost layer is the business layer, which focuses on managing the overall IoT system and provides capabilities such as business process integration, solution deployment, user privacy and security management. It defines and controls business processes and integration with enterprise IT systems. Compared to the 3-layer model, this 5-layer architecture provides some additional focus on the middleware computing platform for IoT as well as overarching business management aspects. The delineation between computing and application layers enables easier integration and management of the cloud infrastructure underpinning the software components. The business layer highlights the need to weave IoT deployments into broader enterprise architectures and business processes. This model suits IoT solutions that are fully cloud-hosted and entails significant integration with enterprise IT systems. The presence of dedicated computing and business layers facilitates management of large-scale deployments spanning multiple application domains. However, it also increases complexity compared to a 3-layer design. The optimal architecture depends on the specific use cases and functional requirements of an IoT system.

2.2. SOA-based architecture

SOA is an architectural style that structures software into reusable, interoperable services that can be aggregated and orchestrated to build applications. Applying SOA principles to IoT yields a layered architecture consisting of the following:[9] Things Layer: This contains the sensors, actuators, embedded devices and hardware components that interact with the physical environment.

Aggregators Layer: Aggregators collect, filter, and preprocess data from the Things layer before transmitting it to the upper layers. They act as intermediaries between devices and services.

Services Layer: This layer contains various shared, reusable software services that operate on the IoT data received from aggregators. Examples include analytics services, visualization services, storage services etc. Applications Layer: End-user IoT applications are developed by leveraging and combining services from the underlying service layer into solution-specific workflows.

The SOA-based model promotes loose coupling between layers via standard interfaces. Adding new data sources and endpoints is easy - they just integrate with the standardized service interfaces. Services can also be reused across different applications due to their platform-independent design. However, the proliferation of services and integration complexity can make governance challenging at scale. Latency may also be higher due to additional communication hops through the intermediate layers. Overall, SOA facilitates interoperability, reproducibility and scalability in IoT systems, making it suitable for enterprise-grade deployments.

2.3. Fog computing architecture

Fog computing is an architectural paradigm that extends cloud computing by distributing some processing, storage, and control functions closer to the network edge. A fog computing architecture for IoT consists of:[10]

Edge Layer: This consists of the endpoint IoT devices as well as edge nodes with computing/storage capabilities. Data analytics and filtering occur at this layer to reduce upstream data traffic.

Fog Layer: The fog layer contains intermediate compute nodes between the edge and cloud layers. More substantial analysis, aggregation and storage takes place here relative to edge nodes.

Cloud Layer: This layer encompasses centralized compute and storage infrastructure. Long term storage and big data analytics occur in the cloud.

Key benefits of fog computing include:

Reduced latency - Processing on edge and fog nodes close to endpoints provides lower latency. Critical tasks can happen locally.

Improved reliability - Applications continue functioning even if cloud connectivity fails since edge nodes have some compute capabilities.

Geographic distribution - Fog nodes are dispersed ensuring wide coverage.

Scalability - Computation is distributed across many nodes instead of a centralized cloud.

Fog computing suits time-sensitive Internet of Things use cases where cloud latency is prohibitive. It also helps mitigate connectivity and bandwidth bottlenecks. However, substantial configuration and coordination between nodes is required. In summary, fog computing pushes intelligence to the edge to support latency-sensitive IoT applications.

3. The key technology of IoT

IoT technology collects data by perception, processing, and information transmission, then analyzing them. So, the key technologies which are required for IoT include RFID technology, sensor technology, network communication technology, embedded system technology, etc.[11]

3.1. RFID technology

RFID technique allows for the automatic identification of things and persons. RFID could be thought of as a way of formally marking items to ease their "recognition" by digital equipment[6]. RFID system generally RFID technological label, and user, and when an item with a digital label goes through a certain communication audience, it is processed by a data processor., the label is enabled by the audience, and the information carried in the label is transmitted across radio waves to the user and the data processing system, completing the work of real-time signal acquiring. The information processing system is responsible for data collection and processing. An Embedded device, commonly known as an RFID tag, is a tiny semiconductor intended to transmit data wirelessly. In general, it is connected to an antenna in the form of a package resembling a standard permanent sticker. An RFID tag sends data over the air in response to interrogation by an RFID reader[12]. The chipset itself equates to roughly a piece of rock.

RFID systems consist of three key components - the RFID tag (transponder), RFID reader (transceiver), and backend database. Tags contain a small integrated chip and antenna which stores identification data for the object. Readers broadcast radio waves to interrogate tags and read data from them. The collected data is then passed to a database/software application for processing.

There are two main types of RFID tags:

- Passive tags - powered by the electromagnetic waves sent by the reader. Low cost but short read range. Used in applications like asset tracking.
- Active tags - powered by an internal battery source. More expensive but can transmit over longer distances. Used for managing high-value assets.

RFID systems typically operate in lower frequency bands like LF (125 KHz), HF (13.56 MHz), UHF (868-956 MHz) or microwave (2.4 GHz). Frequency choice involves tradeoffs between factors like read range, speed, interference, and cost. Common RFID protocols include ISO-14443 and ISO-15693 which define wireless communications and anti-collision methods between tags and readers. Other proprietary protocols also exist.

3.2. Sensor Technology

Sensors are in charge of collecting real-time data and updating data based on real-world data and results. It can detect original information for IoT by sensing light, sound, electricity, heat, and humidity, among

other things. Sensor nodes, sinks, internet or communication satellites, task management nodes, and other components comprise a sensor network structure[6].

Sensors for IoT can be classified based on the physical phenomenon they sense - motion, temperature, pressure, gas, optical, etc. Each type works on different sensing principles - for example, temperature sensors may operate based on thermal expansion or change in resistivity. Important sensor characteristics include measurement range, sensitivity, accuracy, linearity, drift, noise, and frequency response. IoT systems integrate multiple types of sensors to collect diverse data.

Sensor packaging is an important consideration for ruggedness and miniaturization. Packages include thin-film, IC-type, hybrid and composite sensors. MEMS technology enables micro-scale sensors through microfabrication techniques. For IoT, sensors must provide digital interfaces like I2C, SPI for connectivity with microcontrollers and RF modules. Power consumption minimization is also critical for battery-powered devices. Wireless Sensor Networks (WSN) interconnect smart sensor nodes with wireless links to collaboratively monitor environments. Standards like ZigBee and 6LoWPAN target low-power wireless networking of resource-constrained sensors. Application areas for sensors in IoT include air quality monitoring, predictive maintenance, smart homes/buildings, industrial automation, and many more. Low cost, miniaturization and energy harvesting are enabling ubiquitous sensing.

3.3. Network Communication Technology

Sensor network communication technology is divided into two types: short-range networks and long-range networks. Bluetooth, ZigBee, and low-power Wi-Fi are currently used to support short-range M2M communication applications. These technologies are available and best-suited for consumer Application areas, but they may be unable to support civic, industrial, as well as other associated IoT devices whose demands exceed the capacity of their attributes[13].

- Bluetooth - ubiquitous, low-power, low-cost. Used for many consumer IoT devices. Range up to 100m.
- Zigbee - mesh networking standard built on 802.15.4. Optimized for low data rates, long battery life. Typical range 10-100m.
- WiFi - provides high bandwidth wireless connectivity. More power hungry than above. Range up to 100m typically.
- 6LoWPAN - IPv6 networking over low-power wireless networks like Zigbee. Enables Internet connectivity.

For long-range connectivity:

- Cellular networks (2G, 3G, 4G, 5G) provide wide area connectivity. Allow global IoT deployments. High power consumption[4].
- LPWAN technologies like LoRaWAN and SigFox target low-power, long-range (up to 10km) wireless sensor networking using ISM bands. Lower bandwidth.
- WiMax - wireless standard for MANs. Provides multi-megabit connectivity with mile-range coverage.
- Satellite networks - offer connectivity for remote/rural IoT deployments though high latency.

IoT applications have diverse connectivity needs based on factors like latency, mobility, range, cost. A heterogeneous network integrating multiple wireless technologies provides the flexibility to meet requirements. Standard IoT protocols like MQTT, CoAP enable interoperability.

3.4. Embedded System Technology

Computer both hardware and software, smart sensors, embedded system science, and automation and robotics applications are all combined in embedded system technology[14]. Intelligent terminal goods based on embedded system technology may be found everywhere after several decades of progress, such

as cellular telephones, vehicle synthesizers, robotics, medical products, set-top machines, aircraft equipment, and control systems are just a few examples. People's professions are being transformed by the microcontroller, which is increasing asset utilization and household safety. Embedded systems provide the processing intelligence in IoT devices. Key hardware components include:

- Microcontrollers (MCUs) - integrated chips with processor, memory, I/O peripherals optimized for control tasks. Low power consumption. Popular MCUs for IoT include ARM Cortex-M, PIC, AVR, ESP32.
- System-on-Chips (SoCs) - highly integrated ICs packing multiple processing cores, graphics, wireless networking, sensors, etc. Examples are ARM AM series, Intel Quark, Qualcomm QCA4020.
- FPGAs and ASICs - for custom hardware acceleration and unique design needs.

On the software side, embedded operating systems like FreeRTOS, Zephyr, and TinyOS provide real-time task scheduling, device drivers, protocol stacks. Programming is typically done in C/C++, Rust, or assembly language.Debugging and performance monitoring tools are critical for robust embedded software. Over-the-air (OTA) firmware updates are also essential for maintainingdeployed IoT devices remotely.Embedded systems must be optimized for reliability, power, cost and form factor - striking a balance between performance and resource constraints. Trusted execution environments and hardware roots of trust are also required to secure IoT edge nodes.

4. IoT APPLICATIONS

The IoT offers a plethora of technologies in humanity that will make life easier, safer, and smarter. Smart cities, houses, mobility, energy, and the environment are just a few of the uses.

4.1. Smart Cities

Smart projects have helped several major cities, including Seoul, New York, Tokyo, Shanghai, Singapore, and Amsterdam. Smart cities may still be viewed as cities of the future and cities of smart living, and with the present rate of innovation in constructing smart cities, incorporating IoT solutions into city planning will be highly realistic [15]. Smart cities need meticulous planning at every level, in addition to consent from governments and people to fully integrate internet of things technologies. The IoT has the potential to help cities develop on a variety of fronts, including infrastructure and public transit. Reducing traffic congestion while keeping citizens safe, healthy, and more involved in their communities as shown in Figure (3). Cities will become smarter through the internet of things by connecting all systems in cities such as road transport, medical services, and weather forecasting systems, in addition to supporting people through the internet in every location to access the database of airports, railways, and transportation tracking operating under specified protocols[16].

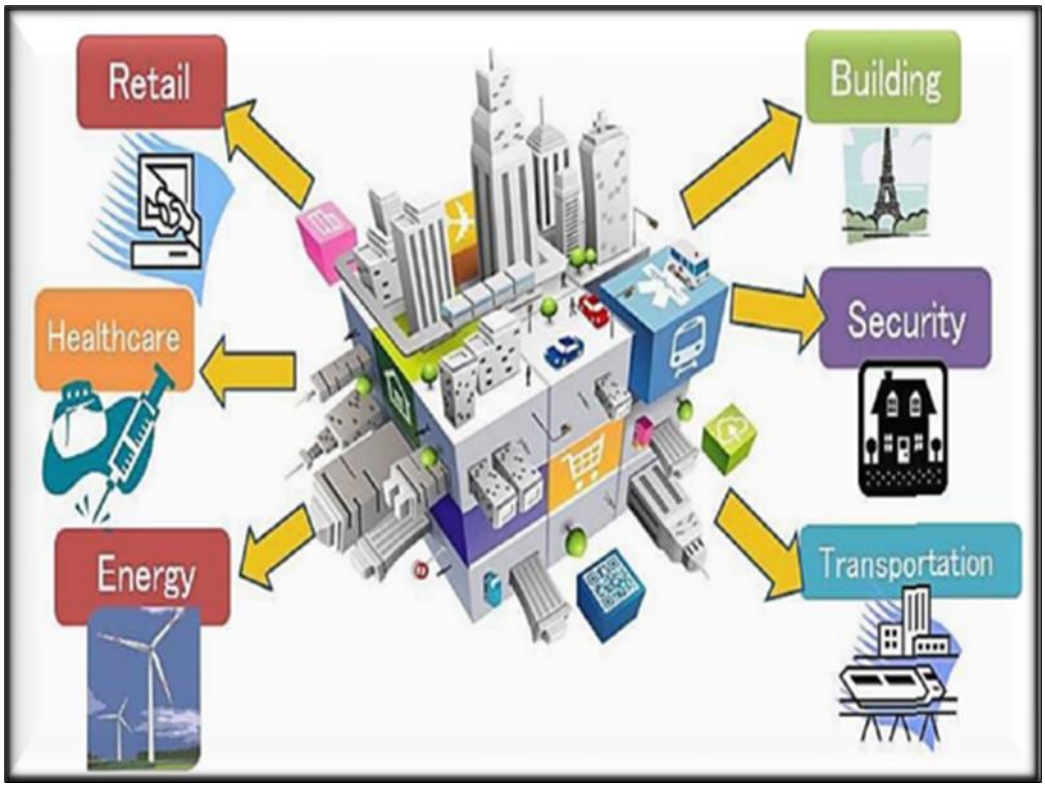

Figure 3. Smart Cities Aspects

4.2. Smart Home and Buildings

Wi-Fi approaches have been employed in embedded devices, with Wi-Fi commonly enabling digital equipment such as TVs, mobile devices, and so on, Because of the connected nature of modern devices. Wi-Fi has evolved to get to be a component of the home IP network due to the rising rate of adoption of mobile computing smartphones and tablets and tablets. A network used to deliver online streaming services, for example, or a network location, should provide a means to regulate device functioning across the network. Simultaneously, digital phones provide users with a mobile 'interface' for infrastructure electronics. Both sorts of devices can act as Internet of Things gateways. Several businesses are considering upgrading solutions that integrate technical aspects with enjoyment, medical applications, energy management systems, and smart sensor checking in the building services settings[16]. Some of the most fascinating IoT systems in smart residences include smart lighting, building automation and multimedia, air defense and central heating, energy efficiency, and security, as illustrated in Figure (4).

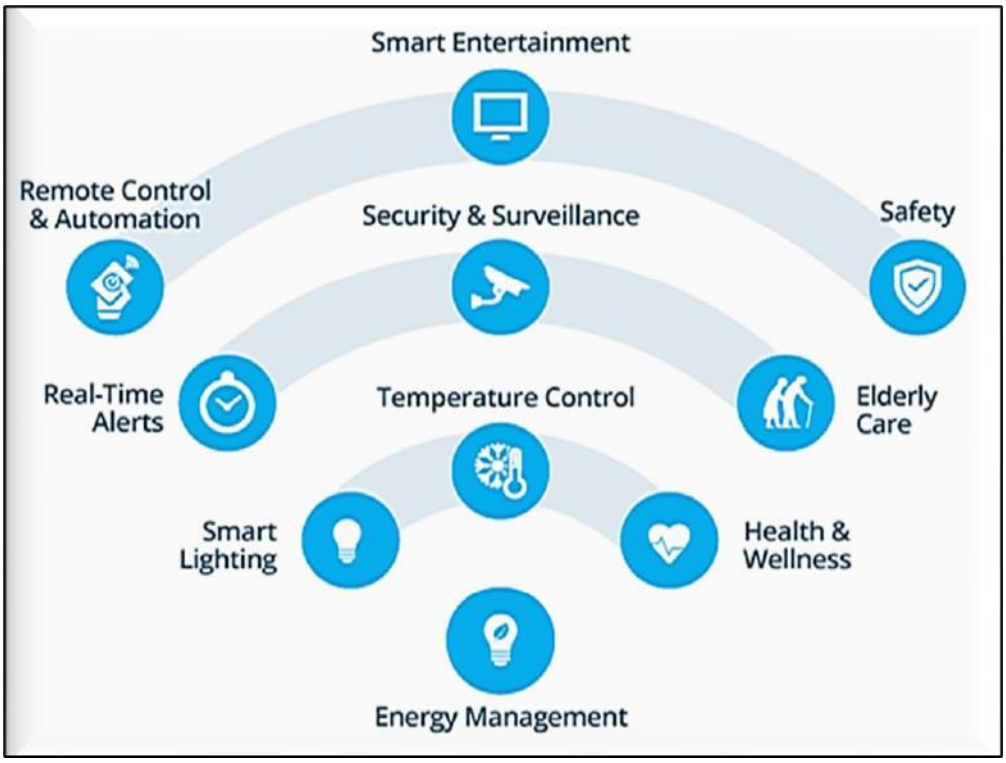

Figure 4. Smart Home Ecosystem

In addition to apparent sustainable resources, wireless sensor networks (WSNs) with the internet of things integration will allow effective energy monitoring in buildings. The Internet, in conjunction with energy management systems, enables access to a building's energy information and control systems from any location in the globe through a laptop or smartphone. The next IoT technology will enable sophisticated infrastructure, which will be a component of a wider computer network utilized by building facilities managers to control energy usage, energy acquisition, and construction techniques.

4.3. Smart Health

A telemonitoring system consists of several components, including data acquisition, storage in traditional or digital form, quick access, healthcare information supervision, and visualization. It offers various benefits over previous approaches, including the opportunity for doctors to monitor patients when they are isolated, increased healthcare quality, and a more time-efficient and dependable technique. This strategy incorporates IoT, which links each unit to the Internet by providing unique addresses, resulting in improved intelligence and flexibility[17]. Health monitoring sensors capture detailed physiological data, which is then evaluated and saved by gateways and the cloud before being wirelessly communicated to providers for additional examination and analysis. as shown in Figure (5), It eliminates Rather than requiring a medical expert to visit this same patient at scheduled intervals to assess vital signs, a constantly automatic stream of data is provided. This approach, both enhance the quality of treatment and decreases the cost of care by decreasing the expense of conventional methods. of care in addition to data collection and analysis.

As Connected systems grow more prevalent in people's daily lives, the integrity of the data obtained remains increasingly important mean a thing. IoT E-health is one example of a privacy risk. Wearable technology gadgets are being utilized to monitor patients' health statuses which include heart rate, heart rate, and sugar levels. Personalized health information is the most delicate to user privacy and is heavily controlled by government guidelines and laws for any form of data sharing when compared to other categories of data. As a result, strategies like FL are required for detectives and researchers to create cutting-edge Machine learning in a dispersed and highly restricted data ecosystem. The capacity to train algorithms for machine learning at scale across many

healthcare centers without collecting data is a vital tool for addressing patient privacy and data security concerns. Effective supervised learning deployment in healthcare has the potential to provide precision medicine on a wide scale, assisting in matching the appropriate medication to the right person at the correct time.

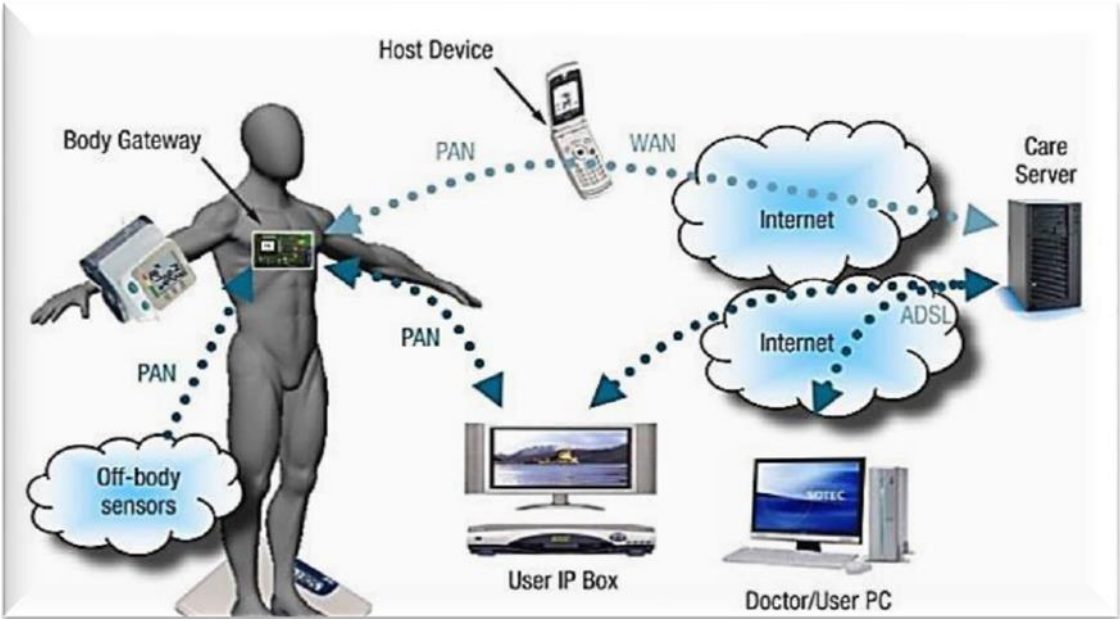

Figure 5. Smart healthcare concept

4.4. Autonomous Driving

Autonomous driving technology is being incorporated into regular automobiles in tandem with the growth of automobile IoT. Frequent real-time communication with a multi-access communication environment is required for a functional personality system. Furthermore, the spatial and temporal variations of the vehicular environment necessitate a smart methodology that can grow as the conditions change. The driving system must transfer a huge quantity of raw data to the server for the usual consolidated technique, which might result in information leakage. Because of the communication cost caused by large-size data transfer and restricted network capacity, the driving system may be unable to correctly adapt to actual offers a unique.

Applying participants learned in automobile edge computing for driverless cars has therefore emerged as a possible avenue for mitigating the aforementioned problems. With FL, each automobile solely requires to broadcast a minimal amount of data to the cloud and can respond more quickly to real-time local adjustments.

4.5. Automated surveillance

Automated surveillance in the Internet of Things (IoT) is a transformative application that leverages the widespread connectivity of devices to enhance security and monitoring processes. By integrating AI and IoT, this system can autonomously monitor environments, analyze data from various sensors and cameras in real-time, and detect potential security threats or anomalies[18].

This automation not only increases efficiency but also reduces the need for human intervention in surveillance tasks. Key areas benefiting from this technology include public safety, home security, and industrial monitoring, where the ability to quickly and accurately identify unusual activities can be crucial[19].

4.6. Metaverse and Virtual Reality

Many improvements have been seen in human understanding, behavior, and how humans respond to the external environment since the primitive age was left. When it comes to profits, humans as a whole are demanding. Humans

desire more, reach for items even when their hands are full, and pursue goals that offer humans a rush of pleasure. Humans are always trying to stuff their wallets with more and more because it is hard to resist human inclinations when such a world offers so much offer. So when humans obtain an ounce of anything, they try to dig deeper to get more of it. The human hunger for more is what has propelled technological advancement to its apex. Humans have progressed from a time when possessing a computer was considered a luxury to the period of the Metaverse, in which the virtual world appears to be more real than the actual physical world the humans live in. Virtual world technology has lately exploded in popularity, particularly when Facebook renamed itself Meta Platforms to bolster its position in the burgeoning business. With the active engagement of global commercial entities, metaverse technology is evolving into a full-fledged business area. The Metaverse has become a favorite experimental hub for technology professionals. They are looking at new methods to tap into the metaverse's potential as an industrial resource for innovation. This expansion, however, is not achievable on its own, and this is where the value of IoT becomes tripled.

5. Challenges in IoT

The devices are vulnerable to hacking because there is no device to detect hacking. It is one of the major concerns. As a result, there has been an increase in the number of threats in which hackers have simply manipulated methods designed to protect people[20]. Manufacturers are rushing to market their products, with little regard for privacy. As a result, the software isn't being tested or upgraded properly. Data is more susceptible to hacking if the logins are weak. When a company employs business educational requirements on its own devices, the risk of data exposure to outsiders increases[21]. Device adoption raises the costs of the product as well as causes this one to take longer to hit the market. This is the most concerning attribute of the Internet of Things. The new systems must be designed with the protection interests of all stakeholders in mind[22]. When it comes to connecting devices, applications, and cloud services, connectivity is the most important factor to consider. IoT devices should be developed sequential manner while keeping in mind rapid technological ideas[23]. IoT programmers should consider how to receive, store, and acquire data while protecting their customers' privacy[24].

Despite the immense possible advantages of IoT use in management, effective inclusion of these pairings (i.e., IoT and logistics) restricts due to substantial difficulties. the developmental disabilities are categorized into three key categories: technique, business, and cooperation, and discuss viable answers as future developments for the paper's growth as shown in figure 6 [25].

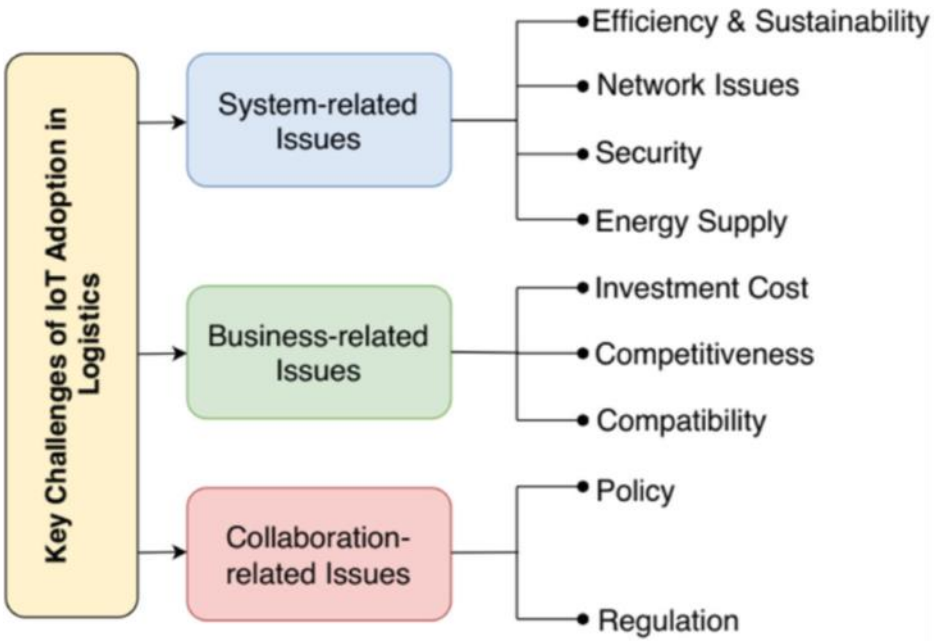

Figure 6. The main challenges of IoT adoption in logistics

5.1. Systemic Concerns

As the inherent issues raise multiple concerns about the overall performance of IoT-based systems in logistics activities, the first and most pressing issue is the flexibility of IoT adoption in logistics.

Despite the reality that perhaps the purpose of logistics operations is to be efficient and sustainable, the implementation of IoT in this sector may produce a contradiction. Because transport resources, for one, are integrated with intelligent homes (e.g., RFID, sensors) that are often powered by batteries, saving energy is a primary goal. These Internet of Things devices may be called upon at any moment to offer essential information for the creation and implementation of autonomous judgment call services and tools[26]. As a result, to keep up with such expanding dimensions, they may need to be continually active. To save power, the WSN cluster may sleep for the bulk of the time (reduced power mode), only waking up to gather sensor data. As a result, an analysis framework is required to investigate and evaluate the system's sustainability when IoT technologies are used[27].

5.2. Business-Related Issues

To realize a Digital environment, it is important to incorporate enabling capabilities of RFID and IoT systems, for example. As a result, the first barrier for users and enterprises may be improved system expenses. In addition, The businesses should build the necessary facilities. To fully fulfill the promise of the Internet of Things, a rising system with a high capital cost is necessary to manage, process, and analyze massive volumes of data created by a wide range of smart devices via a variable flow of logistical activities. Furthermore, the introduction of new technology and the associated ecosphere may result in increasing company expenditures for services such as training and working together, supervising, and managing technology functions. Nonetheless, by extending more capabilities and services based on the technologies used, a good trade between assurance and logistics management profitability and efficiency can potentially be achieved. Sensors, for example, can work collaboratively in ad-hoc networks to provide additional functionality such as tracking and tracing in addition to sensing[28].

5.3. Issues Concerning Collaboration

In this work, teamwork refers to the arrangement and equalization of command-and-control legislation produced by enterprises and states. These norms and restrictions, per the current research, can be integrated and managed by applying data and improving corporate activities to enhance order fulfillment procedures such as global logistics

transit[29]. Inadequate partnerships, however, due to varied and even independent norms, remain a significant impediment to introducing and/or advancing IoT in the logistics area.

Future research

A fall during their current lifestyle may occur although doing complex movements such as cycling; so, it is not as simple as a fall while walking. The complex operations of the information are numerous, involving dependent and autonomous data in a variety of aspects and styles. Edge, fog, and server layers of an IoT architecture offer computational, storage, data management, and decision-making for fall scenarios. Three steps are suggested for a fall clinical diagnosis[30], with every level determining whose layer appears appropriate. To implement stages on each layer, protocols, power efficiency, and smartphone and layer-to-layer lead to an expansion, as well as unique learning algorithms for each layer, need to be employed. A device can identify falls on the periphery and in the fog, as well as calculate layers. So that peripheral computing, for example, a timepiece, is now too weak to efficiently perform sophisticated learning procedures, data is transferred to another device placed in fog. High-performance processors, rather than extra layers, might be offered to recognize falls by processing measured data and validating fall events at the edge. Smart sensors are more complex than normal detectors as they incorporate miniature processors, noise filters, transducers, and amplifiers. A further type of tracking is a static, within-the-body implanted sensor[31]. Sensors with both static and dynamic contexts must be consequences, network-connected, and pleasant to wear. It is crucial to forecast when a fall occurrence may occur. The importance of aberrant trunk, leg walking time, and body histograms in predicting fall occurrences has been studied. Future studies should look into dizzy episodes, neurological conditions, heart problems, and gastrointestinal discomfort (muscle contraction). Assessing fall risks in the proportion of older people utilizing biochemical markers such as heart rate and blood pressure is the most significant component of the prediction system[32]. The forecasting stage conclusions are applied to platform IoT-based parameters.

6. Conclusions

This paper has reviewed IoT architectures, core technologies, and applications along with key challenges. A few key concluding points are IoT architectures can be broadly classified as 3-layer (sensing, network, application), 5-layer, SOA-based, and fog computing designs. The optimal choice depends on factors like scale, performance needs, and application domain. For example, fog computing is well suited for industrial IoT deployments that are latency-sensitive.

Enabling technologies like low-power sensors, RFID, LPWANs, and embedded AI accelerators are critical for scaling IoT across energy-constrained devices. However, interoperability, standards, and unified data models are still lacking.

While IoT has tremendous potential for domains like smart cities, homes, and healthcare, substantial technical and ethical challenges remain around security, data privacy, regulation, and infrastructure costs. For instance, security is a foremost concern in healthcare IoT, while cost and technical maturity impede smart city adoption.

Research priorities include optimized IoT architectures for specific applications, improved device efficiency and interoperability, robust embedded security mechanisms, decentralized data sharing models, and testing IoT systems at scale.this review has sought to provide a comprehensive landscape of IoT technologies, architectures, applications and open challenges. As IoT proliferates, overcoming key hurdles around standards, security, and costs will unlock immense economic and societal value from connected intelligent systems.

Acknowledgement: This is an optional section.

Conflict of Interest: The authors declare that there are no conflicts of interest associated with this research project. We have no financial or personal relationships that could potentially bias our work or influence the interpretation of the results.

References

[1] K. K. Patel, S. M. Patel, and P. Scholar, “Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges,” International journal of engineering science and computing, vol. 6, no. 5, 2016.

[2] A. Murray, A. Papa, B. Cuozzo, and G. Russo, “Evaluating the innovation of the Internet of Things: Empirical evidence from the intellectual capital assessment,” Business Process Management Journal, vol. 22, no. 2, pp. 341–356, 2016.

[3] S. A. Jebur, K. A. Hussein, H. K. Hoomod, L. Alzubaidi, and J. Santamaría, “Review on deep learning approaches for anomaly event detection in video surveillance,” Electronics, vol. 12, no. 1, p. 29, 2022.

[4] K. B. Letaief, W. Chen, Y. Shi, J. Zhang, and Y.-J. A. Zhang, “The roadmap to 6G: AI empowered wireless networks,” IEEE communications magazine, vol. 57, no. 8, pp. 84–90, 2019.

[5] Z. Zhou, X. Chen, E. Li, L. Zeng, K. Luo, and J. Zhang, “Edge intelligence: Paving the last mile of artificial intelligence with edge computing,” Proceedings of the IEEE, vol. 107, no. 8, pp. 1738–1762, 2019.

[6] X. Xingmei, Z. Jing, and W. He, “Research on the basic characteristics, the key technologies, the network architecture and security problems of the internet of things,” in Proceedings of 2013 3rd International Conference on Computer Science and Network Technology, 2013, pp. 825–828.

[7] S. Rudrakar and P. Rughani, “IoT based agriculture (Ag-IoT): A detailed study on architecture, security and forensics,” Information Processing in Agriculture, 2023.

[8] Y. Meir, I. Ben-Noam, Y. Tzach, S. Hodassman, and I. Kanter, “Learning on tree architectures outperforms a convolutional feedforward network,” Scientific Reports, vol. 13, no. 1, p. 962, 2023.

[9] V. Raj and H. Bhukya, “Assessing the Impact of Migration from SOA to Microservices Architecture,” SN Computer Science, vol. 4, no. 5, p. 577, 2023.

[10] S. Rani and G. Srivastava, “Secure hierarchical fog computing-based architecture for industry 5.0 using an attribute-based encryption scheme,” Expert Systems with Applications, vol. 235, p. 121180, 2024.

[11] Y. P. Duan, C. X. Zhao, and Z. Tian, “Application of the internet of things Technology in Agriculture,” Applied Mechanics and Materials, vol. 687, pp. 2395–2398, 2014.

[12] A. Juels, “RFID security and privacy: A research survey,” IEEE journal on selected areas in communications, vol. 24, no. 2, pp. 381–394, 2006.

[13] M. Kocakulak and I. Butun, “An overview of Wireless Sensor Networks towards internet of things,” in 2017 IEEE 7th annual computing and communication workshop and conference (CCWC), 2017, pp. 1–6.

[14] A. Kumar and V. Nath, “Study and design of smart embedded system for smart city using internet of things,” in Nanoelectronics, Circuits and Communication Systems: Proceeding of NCCS 2017, 2019, pp. 397–408.

[15] S. Kauf, “Smart logistics as a basis for the development of the smart city,” Transportation Research Procedia, vol. 39, pp. 143–149, 2019.

[16] K. A. M. Zeinab and S. A. A. Elmustafa, “Internet of things applications, challenges and related future technologies,” World Scientific News, vol. 67, no. 2, pp. 126–148, 2017.

[17] S. Anand and V. Nath, “Study and design of smart embedded system for remote health monitoring using internet of things,” in Nanoelectronics, Circuits and Communication Systems: Proceeding of NCCS 2017, 2019, pp. 409–414.

[18] S. A. Jebur, K. A. Hussein, and H. K. Hoomod, “Abnormal Behavior Detection in Video Surveillance Using Inception-v3 Transfer Learning Approaches,” IRAQI JOURNAL OF COMPUTERS, COMMUNICATIONS, CONTROL AND SYSTEMS ENGINEERING, vol. 23, no. 2, pp. 210–221, 2023.

[19] S. A. Jebur, K. A. Hussein, H. K. Hoomod, and L. Alzubaidi, “Novel deep feature fusion framework for multi-scenario violence detection,” Computers, vol. 12, no. 9, p. 175, 2023.

[20] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen, and S. Shieh, “IoT security: ongoing challenges and research opportunities,” in 2014 IEEE 7th international conference on service-oriented computing and applications, 2014, pp. 230–234.

[21] M. B. Barcena and C. Wueest, “Insecurity in the Internet of Things,” Security response, symantec, vol. 20, 2015.

[22] A. N. Duc, R. Jabangwe, P. Paul, and P. Abrahamsson, “Security challenges in IoT development: a software engineering perspective,” in Proceedings of the XP2017 scientific workshops, 2017, pp. 1–5.

[23] Y.-T. Lee et al., “Cross platform IoT-malware family classification based on printable strings,” in 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2020, pp. 775–784.

[24] A. P. Plageras, K. E. Psannis, C. Stergiou, H. Wang, and B. B. Gupta, “Efficient IoT-based sensor BIG Data collection–processing and analysis in smart buildings,” Future Generation Computer Systems, vol. 82, pp. 349–357, 2018.

[25] D. Tsamboulas, H. Vrenken, and A.-M. Lekka, “Assessment of a transport policy potential for intermodal mode shift on a European scale,” Transportation Research Part A: Policy and Practice, vol. 41, no. 8, pp. 715–733, 2007.

[26] E. Qin, Y. Long, C. Zhang, and L. Huang, “Cloud computing and the internet of things: Technology innovation in automobile service,” in Human Interface and the Management of Information. Information and Interaction for Health, Safety, Mobility and Complex Environments: 15th International Conference, HCI International 2013, Las Vegas, NV, USA, July 21-26, 2013, Proceedings, Part II 15, 2013, pp. 173–180.

[27] E. Macioszek, “First and last mile delivery–problems and issues,” in Advanced Solutions of Transport Systems for Growing Mobility: 14th Scientific and Technical Conference" Transport Systems. Theory & Practice 2017" Selected Papers, 2018, pp. 147–154.

[28] A. Rejeb, J. G. Keogh, and H. Treiblmaier, “Leveraging the internet of things and blockchain technology in supply chain management,” Future Internet, vol. 11, no. 7, p. 161, 2019.

[29] T. Meyer, M. Kuhn, and E. Hartmann, “Blockchain technology enabling the Physical Internet: A synergetic application framework,” Computers & industrial engineering, vol. 136, pp. 5–17, 2019.

[30] E. Cippitelli, F. Fioranelli, E. Gambi, and S. Spinsante, “Radar and RGB-depth sensors for fall detection: A review,” IEEE Sensors Journal, vol. 17, no. 12, pp. 3585–3604, 2017.

[31] A. T. Özdemir, “An analysis on sensor locations of the human body for wearable fall detection devices: Principles and practice,” Sensors, vol. 16, no. 8, p. 1161, 2016.

[32] D. Yacchirema, J. S. de Puga, C. Palau, and M. Esteve, “Fall detection system for elderly people using IoT and ensemble machine learning algorithm,” Personal and Ubiquitous Computing, vol. 23, pp. 801–817, 2019.