Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume: 4 Issue: 1
October 2025
Impact Factor: 10.2
Subject: Computer science

Internet of Things (IoT): A Review of Challenges, Solutions, and Applications

Dr. Jaya Sharma[1]

[1]HOD, Dept. of Computer Science and IT,
College of Professional Studies, Ambikapur, Surguja,
Chhattisgarh, India

Abstract

The Internet of Things (IoT) is changing the communication process of everyday devices, machines, and sensors. IoT enables device data to be collected, aggregated, and shared autonomously which has paved the way for real-time monitoring and better decision making that would have previously been difficult. IoT is affecting every industry, including smart cities, healthcare, agriculture, energy management, and everyday life in general, by linking physical objects to digital management systems as part of a design to automate activities, save time and provide better efficiency. The number of connected devices is increasing at rapid rates, especially with new technologies like 5G, low-power networks, and edge computing. The implementation of these technologies is just one of the many aspects of IoT in applications we regularly encounter related to managing smart homes by controlling lighting and security, wearable health monitoring, automated industrial applications, precision farming, and smart transportation. However, some issues still remain. Administrating on large scales is more complex, with the acknowledgement of privacy, security, and interoperability as factors. Processing and analyzing billions of data streams in real-time while maintaining a reliable and robust system is also difficult. Researchers and developers are working to address these aspects, including developing secure communication protocols, utilizing middleware platforms, cloud processing, and edge processing. More standardized platforms have enhanced compatibility between devices, and as an enhancement of IoT intelligence that incorporates artificial intelligence, machine learning, blockchain, and visible light communications. These solutions are helping devices better understand the environment in which they reside and provide adaptive responses as well as automated decisions. This review will cover IoT applications, challenges, and mitigation methods and suggest a future direction for exploration.

Keywords: *Internet of Things (IoT), Smart devices, IoT applications, Smart home, Security and privacy, Interoperability, Edge computing, IoT frameworks, IoT challenges.*

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume: 4 Issue: 1
October 2025
Impact Factor: 10.2
Subject: Computer science

I. INTRODUCTION

The entire world is quickly heading toward a digitized future, generating what many are calling an increasingly larger "dataSphere." The spotlight of this transition is the IoT, or the Internet of Things, which links all types of physical devices, allowing them to share information and decide on their own. Each IoT device is considered to be a specific "thing" that can send and receive data over the Internet, giving insights into not only each device, but the context around it. By 2025, the International Data Corporation (IDC) predicts that approximately 41.6 billion IoT devices will be connected worldwide, generating a forecasted output of nearly 79.4 zettabytes of data. This is quite dramatic compared to previous years, representing nearly 29% growth per year since 2018. As the number of devices and data generation increases, people, machines, and processes are able to share information much more freely than they could before, opening significant possibilities within industries, transportation, healthcare, and even our everyday household tasks [1].

Certainly, challenges exist as well. The most conspicuous challenges are security and privacy. While devices such as drones, smart sensors, and autonomous machines are interesting, they also have weaknesses that could be exploited through cyberattacks against safety and trust. Governments are beginning to respond; for example, the IoT Cybersecurity Improvement Act of 2017 in the U.S. establishes, among other things, minimum security standards that support prompt installation of security updates and removal of default passwords to mitigate risk. There have already been examples where trust has been compromised. Smart televisions, phones, ATMs, and computers have been hacked to varying degrees. Consumers have expressed concern about the fact those devices have been hacked. Security is not the only challenge. Systems that utilize IoT face a variety of other challenge, including device identity, network addressability, interoperability across heterogeneous devices, mobility, energy consumption, scalability, and efficient network management. As a result, researchers are exploring alternative options, including blockchain technology, intrusion detection systems, cryptography, and fog computing to mitigate risk of cascading consequences of vulnerabilities across systems [2].

The IoT has great potential, going far beyond security. Devices can act autonomously, resulting in smarter traffic systems, environmental sensing, and the automation of industrial processes. These IoT applications can ultimately improve efficiencies, make better use of resources, and create new technology advancement, especially in transportation, energy, and health care settings. However, challenges remain, such as securing edge communications, sustaining sensor energy, safeguarding sensitive data, and developing trust across interconnected systems. Over the past decade, it has evolved from a simple concept around connecting devices, into a self-contained ecosystem, that includes enabling technologies like Wireless Sensor Networks, RFID, Bluetooth, NFC, and LTE. IoT now encompasses creating smart cities, automating industrial processes, health care systems, energy management, and much more. Earlier research offered insights into the enabling technologies, system architecture, and applications of IoT. More recently, research has built on

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume: 4 Issue: 1
October 2025
Impact Factor: 10.2
Subject: Computer science

this research and offered application classifications, suggested some solutions and provided a clearer idea of the current state of IoT, and the future potential to come [3].

In short, IoT is transforming how we live and work, but adoption comes with challenges. Understanding its growth, applications, and limitations is key for designing systems that are both reliable and secure in our increasingly connected world.

II. IOT ARCHITECTURE AND DESIGN

A strong architecture is the foundation for a successful IoT system, which addresses important issues including scalability, routing, and networking. IoT architectures are usually organized in three key dimensions. First, the dimension of information items, encompasses all objects connected to the IoT environment, including sensing items, identifying items, and control items. Second, independent network, includes self-configuration, self-protection, self-adaptation, and self-optimization. The third dimension, intelligent applications, is related to applications that exhibit intelligent behavior on the internet, such as intelligent control, and data processing, as well as methods to exchange data among the objects found in the network. The intersection of these three dimensions is what defines the "infrastructure of IoT" to support the connected objects and provide services such as goods identification, location tracking, and data protection. Two of the more common architectures are the EPC global network and Unite and Ubiquitous IoTs (U2IoTs) [4].

The EPC global network, designed by the Auto-ID Center, leverages RFID technology to transmit dynamic information about mobile objects, providing a record of product transit to authorized individuals. It is a reference model for advancing open IoT architectures and facilitating unconstrained sharing of information. The U2IoTs meanwhile, integrate the physical, cyber, and social worlds, and navigate systems that resemble human neural networks, across industrial, local, national, and global IoT layers. U2IoTs facilitate connectivity, interactivity, space-time consistency, and multi-identity status across units. IoT architectures also have a layered perspective comparable to U2IoTs to develop a modular design and promote security through integration across "layers" of the IoT infrastructure. The physical layer consists of basic sensing hardware such as sensors, actuators, smart appliances, and power supplies, which provide the overall structure for IoT networks. The perception layer consists of sensory systems and technologies such as temperature, vibration, pressure, and RFID sensory systems that ultimately perceive and capture information about their environment. The network layer covers data packets transmitted between devices and receivers, software that enables communication, network topologies, servers, and nodes. Finally, the application layer comprises IoT services such as smart cities, smart healthcare, smart transportation, and smart utility management [5].

These levels not only serve as a design guide for IoT systems, but they also illuminate potential security vulnerabilities. The application layer, for example, may suffer from attacks that leverage malicious code to take over services or disrupt normal function. In the physical and perception layers, incidences can lead to data loss, manipulation, or unauthorized device control. Addressing the vulnerabilities related to these incidences is vital for the implementation of an IoT system in a trusted and reliable manner. To sum up, IoT architecture can be considered a foundational structure for IoT systems to be scalable, safe, and efficient. The design of IoT systems, whether it be through

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume: 4 Issue: 1
October 2025
Impact Factor: 10.2
Subject: Computer science

EPC global network to identifier and track objects or the U2IoTs framework for added connectivity of cyber-physical-social systems, is a layered context for many reasons, including for modularity, interoperability, and for maximum ability to deal with the security and scalability issues of IoT regions.

III. ESSENTIAL IOT TECHNOLOGIES AND APPLICATIONS

The successful deployment of IoT-based products and services relies on several essential technologies that form the backbone of the ecosystem. These include Radio Frequency Identification (RFID), Wireless Sensor Networks (WSN), middleware, cloud computing, and IoT application software.

1. Radio Frequency Identification (RFID)

RFID, or Radio-Frequency Identification, facilitates automatic identification and data capture through the use of radio waves, a tag, and a reader. Unlike traditional barcodes, RFID tags can hold a much larger amount of information through the Electronic Product Code (EPC), which is a global identification system for items that was developed by the Auto-ID Center. There are three main types of RFID tags. Passive RFID tags do not have batteries and rely on the energy transferred from the reader; they are used in supply chains, passports, electronic toll collection systems, and item-level tracking. Active RFID tags use a battery, actively communicating with the RFID reader, and may include sensors on the device to track conditions (e.g., temperature or pressure); they can be used for manufacturing, hospitals, and remote IT asset management. Semi-passive tags use a battery to supply power to the microchip but rely on the reader for communication. Active and semi-passive tags are more expensive than passive ones, but they also offer more advanced monitoring capability [6].

2. Wireless Sensor Networks (WSN)

Wireless sensor networks (WSNs) are composed of autonomously distributed sensors across a field of sensor network. They often work in conjunction with radio-frequency identification systems (RFID) to monitor the location, temperature, and movement of objects. WSNs can employ many topologies and support multi-hop communication. Thanks to advancements in low-power integrated circuits and wireless communication systems, low-cost, efficient, miniature sensors are becoming widely available for the Internet of Things applications (IoT). WSNs most frequently appear in cold chain logistics monitoring the transport of temperature-sensitive goods, and for monitoring and maintenance systems. For example, General Electric has installed sensors to jet engines, turbines, and wind farms for predictive maintenance. In aeronautics, American Airlines can collect terabytes of data in a single flight to provide preventive maintenance and increase operational efficiency.

3. Middleware

Middleware is a software layer located between applications that facilitates communications, input/output, and coexistence of diverse IoT devices. Its main function is to hide complexity to let developers concentrate only on the application side. Open-source frameworks such as Global Sensor Networks (GSN) will simplify the development and deployment of sensor services with

ISSN: 2320-3714
Volume: 4 Issue: 1
October 2025
Impact Factor: 10.2
Subject: Computer science

minimal programming overhead. The majority of IoT middleware architectures utilize a service-oriented approach to manage changing and unpredictable network topologies [6].

4. Cloud Computing

Cloud computing is on-demand access to shared resources such as servers, storage, applications, and services, usually in the form of Infrastructure as a Service (IaaS) or Software as a Service (SaaS). IoT produces large volumes of data streams requiring high-speed processing and storage of that data. Cloud platforms are able to provide scalable back-end solutions to achieve real-time analytics and decision making, as well as a large-scale streaming experience for the IoT [6].

5. IoT Applications

IoT applications enable device-to-device and human-to-device interactions in a reliable and robust manner. For example, in transportation and logistics, IoT systems monitor temperature, humidity, shock, and other factors during the shipment of perishable goods. Services like FedEx SenseAware track packages' location, temperature, and tampering status in real time. Human-centered IoT applications often include visualization interfaces to present information intuitively, allowing users to interact with devices and monitor the environment. Intelligent applications can autonomously detect issues, communicate with other devices, and even resolve problems without human intervention [6].

6. Enhancing Customer Value through IoT

Enterprises can leverage IoT to enhance customer value in several ways [6]. Monitoring and control allows for real-time tracking of products, assets, and services, providing greater visibility and operational oversight. Big data and business analytics enable organizations to analyze the vast amounts of data collected from IoT devices, optimizing operations and supporting more informed decision-making. Additionally, information sharing and collaboration facilitate seamless communication across devices, teams, and stakeholders, improving coordination and responsiveness. Understanding these three categories is essential for organizations seeking to successfully adopt IoT and maximize both operational efficiency and customer satisfaction.

IV. SECURITY, CHALLENGES, AND LIMITATIONS IN IOT

The Internet of Things (IoT) is changing how people interact with their surroundings. What used to be ordinary objects—like watches, refrigerators, or traffic lights—are now becoming connected and "smart." This shift promises convenience and efficiency, but it also brings one unavoidable question: can users actually trust the system? If there is even a small doubt about privacy or data safety, many people will think twice before adopting IoT devices. That hesitation is understandable because security issues exist at nearly every layer of IoT [7].

For instance, take RFID tags. They are used everywhere - from supply chains to payment methods - to encode identification or product data. The issue is that these tags can be hacked. An attacker may steal information, alter data, or hack the tag in a way that was never intended. These are real examples of RFID being hacked: RFID-based viruses spreading, attacks through mobile phones,

ISSN: 2320-3714
Volume: 4 Issue: 1
October 2025
Impact Factor: 10.2
Subject: Computer science

and then old hacks like the old “SpeedPass” incident when payment systems were successfully hacked. These vulnerabilities are not just theoretical issues found in a textbook; they happened in the real world. Similarly, wireless sensor networks (WSNs) have significant gaps. These networks connect hundreds, if not thousands, of tiny devices, continuously transmitting data among themselves. Because the communication is bi-directional, attackers have many points of entry. There are classic attacks like “jamming”: an attack is mounted just simply by jamming the signal frequency - devices cannot talk to one another. Some more sophisticated attempts involve tampering with nodes to access information or change data, as in a Sybil attack where a device pretends to occupy many different nodes to gain access, and flooding where an attacker will flood a network or protocol with useless traffic. Imagine an environmental monitoring medical system going down as a result of memory overload—that’s the kind of risk we’re talking about. The cloud, which supports most IoT infrastructure, introduces another layer of complexity. While cloud platforms make it possible to store and process huge amounts of data, they also create vulnerabilities. A dishonest insider at a cloud service provider could leak private information. Man-in-the-middle attacks can intercept sensitive communications. Large botnets may even use the cloud itself to launch attacks against millions of devices at once. If the cloud is compromised, the reliability of the entire IoT system is at stake [8].

Security is only one part of the puzzle. IoT has to solve the technical and operational issues as well. For example, in fault tolerance, if a sensor fails in health monitoring, doctors won’t see an important signal, and people's lives could be put in jeopardy. Node systems with backup nodes or gateways that can diagnose problems themselves create a scenario of safety versus disaster. Latency is another critical issue. Some IoT applications such as remote surgery or self-driving cars will not tolerate even seconds worth of latency. This is one of the reasons why fog and edge computing have increased in popularity. If you can process information close to the device, you don’t have to always rely on a more distant cloud server. Energy consumption is also a constant concern. Most IoT devices are powered by small batteries, and in remote regions, having to change batteries regularly just won’t happen. That is why engineers are looking at energy-harvesting approaches, like solar energy sensors or ultra-low-power processors. Finally, interoperability is another issue. With so many manufacturers, communication protocols, and hardware designs, making devices communicate with the many other devices isn’t easy. Middleware platforms and frameworks are being developed to resolve these differences, but they still aren't seamless.

Data availability is equally important. Think about it, what happens if an emergency system that relies on sensors suddenly stops receiving updates? It could fail at the worst possible time. To address these questions of reliability, there are high-availability solutions that utilize a mix of cloud and fog computing that keep things operating during failures. Additionally, when dealing with the Internet of Things, systems must also deal with scalability. A smart home may have a few devices, but a smart city may have millions of devices. Systems evolve to deal with ever-increasing scales from one or two devices to hundreds or millions without sacrificing reliability. And finally, we

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume: 4 Issue: 1
October 2025
Impact Factor: 10.2
Subject: Computer science

must contend with "big data," meaning we must not only deal with the streams of data flowing to the systems but also have the need to process the information generated by these devices into something useful. And also consider doing this along with the device software development difficulties of devices being small, cheap, and with limited device resources. In actuality, these are not that simple.

Despite these hurdles, IoT continues to expand into more areas of daily life. The road ahead depends on stronger architectures, more efficient energy use, and better coordination across devices and platforms. Progress in these areas will make IoT safer, more reliable, and more widely trusted. If those challenges are addressed, IoT has the potential to transform industries such as healthcare, transport, and smart urban planning in ways we are only beginning to see**.**

Table 1 the challenges or limitations associated with each

Solution	**Approach / Domain**	**Security**	**Reliability**	**Scalability**	**Privacy**	**Real-time Support**	**Interoperability**	**Key Features**	**Limitations**
Hermes	Event-based	Low	High	High	Low	High	Medium	Event delivery, fault tolerance, scalable routing	No mobility support, no composite events, limited IoT network support
Tinny DDS	Middleware / WSN	Medium	Low	Medium	Low	High	High	Protocol interoperability, lightweight, memory efficient	Not holistic for IoT, limited network requirements support
PRISMA	Resource-oriented	Low	High	Medium	Low	High	Medium	High-level data	Bottleneck at sink nodes, not

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume: 4 Issue: 1
October 2025
Impact Factor: 10.2
Subject: Computer science

								access, three-layer architecture (access, service, application)	scalable, no dynamic real-time adaptation
Hydra	Middleware	High	Low	Medium	High	Low	High	Device/context management, semantic interoperability, energy-efficient	Virtualization vulnerable to attacks, ontology standards not feasible for large-scale networks
KASOM	Pervasive embedded networks	High	High	High	Low	High	Medium	Knowledge management, security services, real-time healthcare data	No dynamic service for mobile/resource-constrained IoT, limited access control
CHOReOS	Large-scale heterogeneous IoT	Low	Low	High	High	Medium	High	Service composition, discovery, cloud/grid	Probabilistic services fail for real-time requirements, insufficien

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume: 4 Issue: 1
October 2025
Impact Factor: 10.2
Subject: Computer science

								resource management	t redundancies
MOSDEN	Decentralized peer-to-peer	Low	High	High	High	Medium	Medium	Plugin architecture, scalable heterogeneous device support	Predefined resource/discovery composition, not ideal for dynamic IoT networks

V. APPLICATIONS OF IOT

The Internet of Things, or IoT, manifests itself differently depending on the context. To understand IoT, people often separate applications into three broad categories: personal, industrial, and much larger systems such as cities or healthcare. For the everyday user, or consumer, IoT is still easy to identify. Smart home devices abound. For example, lights will turn off when there is no one in a room (or they will turn on when someone enters a room); AC units will turn off or adjust when a room reaches a certain temperature; or cameras on a front door will allow the user to see a live video without having to approach the door. Wearable devices also tend to fit in this broad category, whether it is smart watches or fitness bands that capture step, heart rate, or sleep pattern data and send the data to the user's phone. Voice assistants, like Alexa or Google Home, could also be considered IoT devices, as they may appear very simple, yet they fundamentally alter people's engagement in their daily activities. In an industrial context, the Internet of Things happens on a larger scale; sometimes it is referred to as the Industrial Internet of Things (IIoT). An example of IIoT would be a factory placing sensors on machines to measure the vibration, speed, and temperatures of components. If one of the measures looks out of the ordinary, the system sends a message to the engineers and can alert them to check on the machine before it fails. This can help avoid expensive downtime. Another example is the use of trackers in shipping and logistics on trucks and containers, sometimes even on specific packages, so that companies know exactly where their products are physically located, and whether or not they are delayed. The third area is more public—what cities, hospitals, or energy providers do with IoT. In smart cities, sensors can monitor traffic and adjust signals to reduce jams. Garbage bins can even “tell” the city when they’re full, so workers only collect when needed. Hospitals use IoT to watch patients in real time, whether they’re inside the hospital or at home, and doctors can respond quickly if something goes

ISSN: 2320-3714
Volume: 4 Issue: 1
October 2025
Impact Factor: 10.2
Subject: Computer science

wrong. Energy companies also rely on IoT for tasks like spotting leaks, balancing the grid, or saving power during peak times [9].

The entire process relies on data. Devices not only gather it but can also transmit it somewhere to be processed, often in real time. For instance, a sensor on the road may collect data regarding traffic and automatically change light timing, in another example, a machine sensor may virtually assure that equipment is stopped before wear and tear or damage occurs. This is, after all, what IoT ultimately represents—not only is it about connecting devices but, through responsive action, it's about being intelligent without reliant data.

When you think about it on a macro scale, IoT is already integrated into our lives and businesses. It is embedded into everyday devices at home, in factory settings, throughout cities, and in hospitals, often working without all of our focus and attention. By connecting devices and making them responsive, IoT is creating systems that are more efficient, safer, and even sometimes more sustainable. It is happening already.

VI. RELATED WORK

The Internet of Things is quietly weaving itself into our daily lives, connecting objects so they can talk to each other and make decisions on their own. In smart homes, for example, your lights, thermostat, and security cameras can adjust themselves without you lifting a finger. Out on the farm, sensors keep an eye on soil moisture and crop health, letting farmers save water and boost yields. Factories are using similar setups, tracking machines in real time to prevent breakdowns and keep everything running smoothly.

Smart homes illustrate the potential and the peril of this technology. For example, researchers such as Stojkoska and Trivodaliev [10] have outlined how gadgets can interact as a lone system. The research of Raja and Dhiliphan [11] indicates that IoT usage can help minimize energy usage and improve daily ease of life, ict would still require coordination of devices from multiple brands and management of large amounts of incoming data, all of which can prove problematic. Similar shifts exist for industries. Mu and Antwi-Afari [12] acknowledge that IoT allows firms to control production and logistics and even try out new business models. Machines are constantly sending out updates, and managers are using them to resolve issues and make decisions far more rapidly than they used to. Connecting all these technologies and keeping the system running are far from easy.

Agriculture is also experiencing benefits, as noted by Khan and Ismail [13] where they suggest technologies such as soil sensors and weather trackers to help farmers make more informed decisions. These devices can lead to improvements in efficiency and productivity, but challenges exist with software complexity, security considerations, and the need for people with technical expertise. Even energy systems are becoming smarter; for example, Motlagh et al. [14] report that smart grids can regulate and analyze electricity use; they can forecast possible issues; and they can help integrate renewable energy sources into the grid. In sum, smart energy can provide solutions for a more reliable and greener grid. There are still challenges associated with security and privacy;

ISSN: 2320-3714
Volume: 4 Issue: 1
October 2025
Impact Factor: 10.2
Subject: Computer science

however, a new generation of solutions could be at hand, e.g., blockchain technology. Overall, the IoT is supporting connections and efficiencies in the home, in agriculture, in manufacturing, and in energy systems. Reductions in time, expense, and convenience are all promised benefits. The full realization of these benefits relies on challenges such as security, compatibility, and scaling being managed effectively. If done well, however, these connected technologies could make our world much smarter and more responsive.

Overall, the literature demonstrates that IoT is highly versatile, with applications across home, industry, agriculture, and energy. Yet, alongside the opportunities, the recurring concerns of interoperability, scalability, and security highlight the need for next-generation frameworks that are flexible, safe, and capable of supporting widespread adoption.

VII. CHALLENGES AND FUTURE DIRECTIONS

The rapid advancement of electronics and telecommunication technologies has paved the way for new horizons of investigation in the field of IoT research, including the ultra-promising area involving Visible Light Communication (VLC) technology and its integration within IoT systems. Even though advances are steady, challenges still exist that require further investigation. One of the challenges raised in discussions is of mobility. In IoT environments based on VLC, mobility can be hindered by human non-linear movement, as even the movement of a single person across the light path or a device suddenly and inadvertently exiting line-of-sight in the VLC environment can cause signal disruption. In addition to consequently blocking line-of-sight, signal blocking caused by shadowing effects can drastically reduce performance and cause disruptions within communication. Therefore, determining and executing a mobility handover procedure is paramount for further development within this area of research. Protocols need to be devised in such a manner that they ensure devices stay connected within the communication network while still upholding quality of service (QoS) in highly dynamic or obstructed environments [15].

Receiver technology is another area of active interest. Today, most VLC systems utilize camera chips, but these are not designed to support the very high bit-rates demanded by modern IoT applications. The goal with these technologies is to create optical sensors that can transmit and receive at much higher speeds, are more sensitive, and finally achieve real-time communication. The availability of these types of receivers could provide greater robustness and speed for VLC-IoT links. Related to this is the increased interest around camera-based VLC that is being explored as a possible standard for optical camera communication. In this sense, improvements in the sensor technology will be both useful, but possibly essential for the next generation of IoT systems. VLC-IoT is also becoming popular in vehicular networks and will certainly be used in even more challenging situations than vehicular networks. These would include vehicular networks operating in tunnels, or even more confined road settings. Traditional RF-based radio networks often have significant limitations in relatively confined spaces due to interference effects or simply due to fading. Light-based communication offers much more stable conditions. However, before these

ISSN: 2320-3714
Volume: 4 Issue: 1
October 2025
Impact Factor: 10.2
Subject: Computer science

VLC systems can deployed and used, additional research in terms of modeling the channels under real-world, time-varying conditions and testing how large data frames can be sent without error, as well as evaluation of other ambient conditions like vehicle speed, external lighting or environmental conditions such as rain will also be required[16].

In conclusion, there is an emerging movement toward software-centric VLC-IoT architectures. Rather than relying primarily on specialized hardware, future IoT applications—particularly those with relatively modest requirements of bandwidth—are likely to embrace lightweight, software-defined architecture. This would enable remote programmability, increased flexibility, and adaptable communication without infrastructure. In practical terms, this approach could decrease costs, simplify deployment, and maintain the adaptability of IoT devices without frequent hardware upgrades.

To summarize, the future direction of VLC-IoT research is focused on four directions: mobility management, advanced receiver hardware, vehicular applications, and software-based frameworks. Each of these directions would help build faster and more efficient IoT networks, but also provide the versatility to meet future requirements.

VIII. CONCULSION

The Internet of Things (IoT) has rapidly emerged as one of the foremost technologies of the past decade, transforming smart homes, healthcare, industrial automation, energy systems, and transportation. Its primary contribution is the ability to connect a collection of objects, sensors, and applications into a single monitored network to enable real-time tracking of objects, task automation, and algorithm-driven decision making based on tracking data. The connectivity provided by networks offers significant benefits, particularly in terms of efficiency, simplicity, and timeliness. However, this connectivity often presents a number of complicated challenges. While it may seem easy in theory to transition to (or deploy) a large number of IoT devices, practical challenges of scalability, interoperability, mobility, security, and resource management often complicate the migration. A number of approaches have been presented for addressing the migration challenges of the Internet of Things (IoT). Most can be classified as event-based, agent-based, middleware-driven, or application-specific. For example, event-based migration relies on efficient messaging and routing. Frameworks such as Hermes illustrate how well this can work for scaling, but challenges remain with high mobility of devices or continuously changing networks. PRISMA and other resource-oriented platforms are focused on interoperability through user access to high-level data and structured architectures. These are helpful for connecting different devices, but hardware limitations still cause bottlenecks and limits on scalability.

Middleware has proven to be a favorable method. Systems like Hydra or KASOM already support dynamic configuration, semantic interoperability, and energy-efficient communication. The problem is that large networks are often immobile and that there has not been anywhere near sufficient work on creating common standards or ontologies. Other methods such as CHOReOS or MOSDEN, work on discovering services and addressing heterogeneous device types, but

ISSN: 2320-3714
Volume: 4 Issue: 1
October 2025
Impact Factor: 10.2
Subject: Computer science

become less relevant when it comes to responsiveness in real-time. Overall, there is little doubt that there has been progress, but once again there is not a single solution that can address the full complexity of IoT. Identifying resources and managing resources still remain a pivotal challenge. As seen previously, when there are many devices and applications attempting to run concurrently, they will negotiate for available bandwidth, deplete the power supply, potentially degrading QoS, or in some instances ceasing operations. Event handling is another weak link, too many events and requests can block system responsiveness and cause congestion within the system. Finally, many of today's most popular platforms do not offer flexible or programmable frameworks, which is less adaptable in the medium to long term. Future IoT systems will need solutions that will offer such integrated features and adjust whenever possible. This means that frameworks need to be able to handle dynamic resource allocation, optimise event flows, make sure security is strong, and still work well in real time across different types of networks. New technologies might be able to help. For instance, visible light communication could help with spectrum overload, and edge computing could help with latency by processing data closer to where it is created. Combining IoT with AI is also promising because AI can make networks more autonomous and aware of their surroundings.

In short, IoT research has made a lot of progress, but it hasn't solved all of the big problems yet. To make systems that are safe, scalable, and adaptable, we will need to keep working on middleware, communication protocols, and adaptive architectures. With these improvements, IoT will be better able to support smarter, more resilient, and more human-centered apps in a variety of fields.

References

[1] Abiodun, Oludare Isaac, et al. "A review on the security of the internet of things: Challenges and solutions." Wireless Personal Communications 119.3 (2021): 2603-2637.

[2] Albishi, Saad, et al. "Challenges and Solutions for Applications and Technologies in the Internet of Things." Procedia Computer Science 124 (2017): 608-614.

[3] Khanna, Abhishek, and Sanmeet Kaur. "Internet of things (IoT), applications and challenges: a comprehensive review." Wireless Personal Communications 114.2 (2020): 1687-1762.

[4] Ali, Zainab H., Hesham A. Ali, and Mahmoud M. Badawy. "Internet of Things (IoT): definitions, challenges and recent research directions." International Journal of Computer Applications 128.1 (2015): 37-47.

[5] Kumar, Sathish Alampalayam, Tyler Vealey, and Harshit Srivastava. "Security in internet of things: Challenges, solutions and future directions." 2016 49th Hawaii International Conference on System Sciences (HICSS). IEEE, 2016.

ISSN: 2320-3714
Volume: 4 Issue: 1
October 2025
Impact Factor: 10.2
Subject: Computer science

[6] Lee, In, and Kyoochun Lee. "The Internet of Things (IoT): Applications, investments, and challenges for enterprises." Business horizons 58.4 (2015): 431-440.

[7] Farooq, Muhammad Umar, et al. "A review on internet of things (IoT)." International journal of computer applications 113.1 (2015).

[8] Naresh, Vankamamidi S., et al. "Internet of things in healthcare: Architecture, applications, challenges, and solutions." Computer Systems Science & Engineering 35.6 (2020).

[9] Zeinab, Kamal Aldein Mohammed, and Sayed Ali Ahmed Elmustafa. "Internet of things applications, challenges and related future technologies." World Scientific News 2.67 (2017): 126-148.

[10] Stojkoska, Biljana L. Risteska, and Kire V. Trivodaliev. "A review of Internet of Things for smart home: Challenges and solutions." Journal of cleaner production 140 (2017): 1454-1464.

[11] Raja, S. P., T. Dhiliphan Rajkumar, and Vivek Pandiya Raj. "Internet of things: Challenges, issues and applications." Journal of Circuits, Systems and Computers 27.12 (2018): 1830007.

[12] Mu, Xiaoshao, and Maxwell Fordjour Antwi-Afari. "The applications of Internet of Things (IoT) in industrial management: a science mapping review." International Journal of Production Research 62.5 (2024): 1928-1952.

[13] Khan, Sarfraz Fayaz, and Mohammed Yusoof Ismail. "An Investigation into the Challenges and Opportunities Associated with the Application of Internet of Things (IoT) in the Agricultural Sector-A Review." J. Comput. Sci. 14.2 (2018): 132-143.

[14] Hossein Motlagh, Naser, et al. "Internet of Things (IoT) and the energy sector." Energies 13.2 (2020): 494.

[15] Qureshi, Kashif Naseer. "New trends in Internet of Things, applications, challenges, and solutions." TELKOMNIKA (Telecommunication Computing Electronics and Control) 16.3 (2018): 1114-1119.

[16] Oyewobi, Stephen S., Karim Djouani, and Anish Matthew Kurien. "Visible light communications for internet of things: Prospects and approaches, challenges, solutions and future directions." Technologies 10.1 (2022): 28.

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume: 4 Issue: 1
October 2025
Impact Factor: 10.2
Subject: Computer science

Author's Declaration

I as an author of the above research paper/article, here by, declare that the content of this paper is prepared by me and if any person having copyright issue or patent or anything otherwise related to the content, I shall always be legally responsible for any issue. For the reason of invisibility of my research paper on the website /amendments /updates, I have resubmitted my paper for publication on the same date. If any data or information given by me is not correct, I shall always be legally responsible. With my whole responsibility legally and formally have intimated the publisher (Publisher) that my paper has been checked by my guide (if any) or expert to make it sure that paper is technically right and there is no unaccepted plagiarism and hentriacontane is genuinely mine. If any issue arises related to Plagiarism/ Guide Name/ Educational Qualification /Designation /Address of my university/ college/institution/ Structure or Formatting/ Resubmission /Submission /Copyright /Patent /Submission for any higher degree or Job/Primary Data/Secondary Data Issues. I will be solely/entirely responsible for any legal issues. I have been informed that the most of the data from the website is invisible or shuffled or vanished from the database due to some technical fault or hacking and therefore the process of resubmission is there for the scholars/students who finds trouble in getting their paper on the website. At the time of resubmission of my paper I take all the legal and formal responsibilities, If I hide or do not submit the copy of my original documents (Andhra/Driving License/Any Identity Proof and Photo) in spite of demand from the publisher then my paper maybe rejected or removed from the website anytime and may not be consider for verification. I accept the fact that as the content of this paper and the resubmission legal responsibilities and reasons are only mine then the Publisher (Airo International Journal/Airo National Research Journal) is never responsible. I also declare that if publisher finds Any complication or error or anything hidden or implemented otherwise, my paper maybe removed from the website or the watermark of remark/actuality maybe mentioned on my paper. Even if anything is found illegal publisher may also take legal action against me.

Dr. Jaya Sharma

******