Volume: 14, Issue: 1
Page: 80-92
2022

International Journal of Science and Business

Journal homepage: ijsab.com/ijsb

A Review on Internet of Things-IoT-Architecture, Technologies, Future Applications & Challenges

Md. Mahbubur Rahaman

Abstract

Internet of Things (IoT) is one of the developing innovations of this century. Its different aspects, such as infrastructure, architecture, and security, play a critical part in forming the long-term digitalized world. Connected devices, generally recognized as the Internet of Things (IoT), are expanding rapidly. The network framework has got to suit all these devices by giving a good network and conveying application-based services. With the Internet of Things (IoT) slowly escalating as the consequent stage of the advancement of the Web, it gets to be pivotal to recognize the different potential domains for the application of IoT and inquire about the challenges related to these applications. Currently, we only witness two types of communication: human to human and human to device. However, the Internet of Things (IoT) ensures a fantastic future for the web where machine to machine connectivity is the primary mode of communication (M2M). IoT appeals to us because of its inventiveness and fun factor. IoT is therefore predicted to be the Internet of Things in the future. The aim of this paper is to provide an inclusive illustration of the IoT situation, survey its empowering technologies & architectures, and focus on future applications. Also, it examines diverse challenges and critical issues of IoT.

IJSB
Accepted 4 September 2022
Published 10 September2022
DOI: 10.5281/zenodo.7066810

Keywords: *Internet of Things, Network, Architecture, Security, Challenges, IoT Application, RFID Authentication, Internet of Everything (IoE); Internet of Nano-things (IoNT).*

About Author (s)

Md. Mahbubur Rahaman, Associate Professor, Department of Tourism and Hospitality Management, Leading University, Sylhet, Bangladesh.

Introduction

The Internet of Things (IoT) can also be referred to as the Internet of everything. You can also think of it as the industrial Internet. It is considered as modern technology has proven globally with a network of interactive machines or devices. This area is the most vital to work on for future technology and is gradually gaining much attention from different users and industries (Malik et at., 2019). The Internet of Things (IoT) is a strategy that combines data from many things on any platform of already-existing internet infrastructure, as the name suggests (Nimodia & Ajankar, 2022). The primary goal of the Internet of Things is to enable digital devices to connect through multiple networks, paths, or services to other objects, and people at any time & anywhere (Hussein, 2019). The IoT promises people to live in an intelligent and highly networked world that enables diverse interactions with this environment. Phones are the key to authenticating with these connected devices and carrying content anywhere, using the concept of hyperlinks. Object hyperlinks are a coined term that usually refers to extending the Internet to real-world objects and locations (Tyagi et al., 2014). The Internet expands beyond being merely a network of computers. It develops into a network of various gadgets. The Internet of Things (IoT) functions as a network of interconnected devices, or a network of networks (Hussein, 2019). Although commercial success continues to be materialized, the IoT will offer nearly endless business and research opportunities. Therefore, the study addresses various potential areas of application in the IoT domain and research challenges related to these applications (Hussein, 2019). We cannot deny the growing significance of IoT in our life. Moreover, being innovative, IoT is integrating various modes of intelligence systems and devices as well as their frameworks (Kumar et al., 2019). IoT systems connect various sensors and intelligent devices to local or cloud-based controllers from an architecture perspective. Frequently, real-time data about their surroundings is gathered and sent through sensors. The controller then employs this data to deliver quick and long-term responses (Yaici et al., 2021). The IoT system's architecture is fairly dependable and is made up of three primary layers: i. the sensor or hardware layer, ii. the software control layer and iii. layers of an application. Physical elements with distinct identities and the capacity to transmit data over a network devoid of person-to-person or person-to-computer interactions are included in the hardware or sensor layer (Yaici et al., 2021). The global distribution of IoT devices is one difficulty. All of these globally dispersed devices must be reachable via the network architecture. This challenge is significant for a single service provider and an investment in an extensive infrastructure (Alenezi et al., 2021). Therefore, IoT security is a concern for protecting the hardware and networks of IoT systems (Mohamad Noor & Hassan, 2019). The paper will try to address the concepts of IoT, its infrastructure, and architecture with the challenges and the opportunities for future applications that will ease human life than before.

Literature Review

The Architecture of IoT

The current Internet architecture, which uses the TCP/IP protocol, was adopted in 1980, but by 2030, more than 25.4 billion people are anticipated to be connected, which is a tremendous figure (Nimodia & Ajankar, 2022). It requires a new open architecture to address numerous security and quality of service (QoS) challenges as well as support current network applications using open protocols because the IoT cannot handle it (M. Zhang et al., 2012). Without adequate privacy protection, it is unlikely that many people will adopt IoT (Suo et al., 2012). Therefore, data security and user privacy are critical IoT challenges. Several layered security architectures have been proposed for additional development of the IoT. (Chen, 2013) described an architecture with three significant layers of IoT, and (Suo et al., 2012) described an architecture with four important layers. (Wu et al., 2010) suggested a five-tier architecture that leverages the best Internet and communications management network architectures

based on the TCP / IP and TMN models. Similarly, a 6-tier architecture based on a hierarchical network structure has been proposed (Suo et al., 2012). Consequently, it is typically separated into six layers. The following describes each of the six IoT levels.

Coding layer
The IoT's coding layer, which identifies the target object, is its core. At this layer, each object is given a distinct ID, making it simple to identify between things (M. Zhang et al., 2012).

Perceptual layer
Each object has a physical meaning gives by the layer. It is made up of several data sensors that may measure an object's temperature, humidity, velocity, position, and other properties (Bandyopadhyay & Sen, 2011). This layer gathers important data from the sensing devices about an object and transforms it into a digital signal. The network layer receives the digital signal to take further action.

Network layer
This layer's function is to gather useful data from the perception layer in the form of digital signals and transmit it over transmission mediums such WiFi, Bluetooth, WiMAX, Zigbee, GSM, and 3G to the middleware layer's processing system. It employs MQTT, DDS, IPv4, and IPv6 (Y. Zhang, 2011).

Middleware layer
The data sent by the sensor device is handled by this layer (Shen & Liu, 2011). It includes innovations like cloud computing and ubiquitous computing that let you store all the data you require and instantly access the database. Information is processed using some intelligent processing tools, and the results of the processing are totally automated activities.

Application layer
Based on processed data, this layer enables IoT applications for various industries. As applications support IoT development, this layer is advantageous for the broad expansion of IoT networks (Wu et al., 2010). Smart homes, intelligent transportation, and smart planets are examples of IoT-related applications.

Business layer
All IoT-related study is managed by this layer, which also oversees IoT applications and services. It provides several business models for efficient tactics (Khan et al., 2012).

The Technologies of IoT
To enable things to be identified and communicate with one another, a combination of new and efficient technologies must be developed through the creation of ubiquitous computing systems that can each uniquely identify digital objects, things and interact with other entities, and gather data to carry out automated actions (Khoo, 2011). The IoT's broad development will benefit from the linked technologies described in this section.

Radio Frequency Identification (RFID)
RFID is an important tech that allows things to be identified. Due to its reduced size and cost can be embedded in anything (Chen, 2013). Depending on the application, RFID is a transmitter microchip that resembles a sticker and can be either active or passive (Guo et al., 2011). The active tag is connected to the battery. The dynamic title is always busy, sending the data signal continuously, but the passive tag is active only when activated. Passive tags are less expensive,

yet active tags have a number of useful applications (Shen & Liu, 2011). RFID systems include RFID tags and readers that convey information about an object, such as its ID or position, when the right signal is generated (Zhang & Zhu, 2011). Using radio frequencies, the reader transmits the object-related data signal that was emitted, which is then sent on to the processor for analysis. The creation of a universal computing system where digital things may be precisely recognized and have the capacity to think and engage in interactions with other objects to gather facts depending on whether automated operations are conducted, a mix of modern, efficient technology is required, which can only be accomplished by integrating several technologies that enable object identification and communication (Khoo, 2011). In this part, essential technologies are covered that can aid in the widespread growth of IoT. RFID frequencies are divided into four different frequency ranges based on the type of application (Guo et al., 2011), including low frequency (135 kHz or less), high frequency (13, 56 MHz), ultra-high frequency (862MHz to 928MHz), and microwave frequency (2.4G, 5.80). Barcodes are an identification technique that performs much the equivalent function as RFIDs, but RFID is more effective than barcodes because of its many advantages. RFID does not need to be physically in the field of view because RFID is a wireless technology, but as an optical technology, barcodes can only function when the reader is positioned in front of them. Furthermore, RFID acts as an actuator that triggers various events, with changes that are not apparent in barcodes.

Wireless Sensor Network (WSN)

WSN is a bi-directional wirelessly related community of sensors in a multi-hop fashion, constructed from numerous nodes scattered in a sensor subject every about one or multiple sensors which could gather object-unique statistics which include temperature, humidity, velocity after which by skipping directly to the processing equipment (Atzori et al., 2010). Sensing nodes communicate using multi-hop. Each sensor is a transceiver equipped with an antenna, a microcontroller, and an interface circuit that serve as the sensors' communication, actuation, and sensing units, respectively. The power source for each sensor may be a battery or any power-harvesting technology (Tapia et al., 2007). However (Shen & Liu, 2011) has suggested a new unit, the Memory Unit, that may also be a component of the sensing node, for storing the statistics. While blended collectively, the Wireless Sensors Network era and RFID era open up opportunities for even extra clever devices to some of the answers proposed (Atzori et al., 2010). Intel Research Labs provides an example response in the form of the Wireless Identification Sensing Platform (WISP). A passive WiFi sensor community called WISP has built-in light, temperature, and other sensors (Tapia et al., 2007). WSN and RFID Sensor Networks both have advantages, although RFID Sensor Networks have a smaller selection. While WSNs have a relatively longer arr12ay and use peer-to-peer communication, their communication is asymmetric. Additionally, the majority of WSNs are wholly based on 802.15. Low-Rate Wireless Personal Area Networks (LR-WPANs) have a Physical and MAC layer (Atzori et al., 2010). A number of solutions have been proposed, including a 6LOWPAN favored (Worlu et al., 2019), which allows IPv6 packets to be communicated via the systems that are computationally managed. This technology enables the blending of WSN with the IoT. Additionally, a ROLL routing preference exists for cease-to-cease routing responses (Roman et al., 2011).

Cloud Computing

With millions of gadgets anticipated by 2020 (Kaur, 2020), the lone technology that appears to efficiently evaluate and preserve all data is the cloud. It is an advanced computer system that integrates many servers on a cloud platform to enable the mutual sharing of resources accessible anytime, anywhere (Kaur, 2020). The crucial component of the IoT is cloud

computing, consolidating servers and handling increased computing power, analyzing helpful information obtained from sensors, and providing superior storage capacity (Rekha et al., 2021). But unleashing the full potential of this technology is just getting started. Cloud computing associated with intelligent things, which can use millions of sensors, offers immense benefits and helps develop the IoT on a colossal scale. As a result, IoT is entirely dependent on cloud computing and is being researched.

Network Technology:
Due to their responsibility for the connections between objects, these technologies are essential to the growth of the IoT. In order to manage a large number of potential devices, you need a quick and efficient network. Networks for long-distance transmission often employ 3G, 4G, etc. However, as you are aware, mobile data traffic is predictable because it is only required for everyday operations like placing calls and sending texts. 5th generation wireless systems must be extremely quick, extremely efficient, unexpected, and able to supply far more bandwidth in the present era of ubiquitous computing (Vermesan & Friess, 2014). Similar to long-range networks, short-range networks rely on technologies like Bluetooth and WiFi.

Nanotechnology
This technology offers a more compact and enhanced version of what is linked. By allowing the development of nanometer-scale devices, system consumption can be reduced that can be used as sensors and actuators like regular devices. Such nanodevices are manufactured from nano components, and the network model establishes a new network structure for the Internet of Nano Things (Atlam et al., 2018).

Micro-Electro-Mechanical Systems (MEMS) technologies
MEMS is a combination of electric and mechanical components that work together to provide a number of applications, including sensing and actuating. MEMS come in the form of transducers, accelerometers, and other devices. MEMS, a low-cost option, is also paired with nanotechnologies to create the IoT communication network and other advantages such combined ubiquitous computing devices, advanced range of frequencies, and size minimization of sensors and actuators (Iannacci, 2015).

Optical Technologies
The rapid advancement of optical technologies like LiFi and Cisco's BiDi optical technology may represent a significant IoT development innovation. For the devices that are mutually connected with the idea of IoT, superior connectivity on a larger bandwidth will be provided by LiFi, a revolutionary Visible Light Communication (VLC) technology. Similarly, Bi-Directional (BiDi) technology, which offers a 40G ethernet for huge data from several IoT devices, is applicable (Aleksic, 2019).

IoT Applications
Given that Internet of Things affects virtually every aspect of people's, organizations', and civilizations' daily lives, and has a vast range of possible uses. According to (Patel et al., 2016) IoT applications span a wide range of industries, including manufacturing or industrial sectors, healthcare sectors, agriculture, smart cities, security, and emergencies.

Smart Cities
The Internet of Things (IoT) would enhance the overall infrastructure and cities' smartness (Zanjal & Talmale, 2016). Areas of IoT applications in the creation of smart cities include sophisticated transportation infrastructure (Jain, 2018), innovative construction, traffic

congestion and waste management (Bellini et al., 2022), bright lighting, smart parking, and city maps. Monitoring municipal parking spots, keeping tabs on building vibration and physical condition, placing noise-monitoring equipment in sensitive places, and keeping an eye on pedestrian and vehicle activity are just a few features that may be added. Traffic congestion in smart cities can be tracked, managed, and reduced with IoT powered by artificial intelligence (AI) (Zanjal & Talmale, 2016). In addition, you can use the IoT to install smart weather-adaptive streetlights and track debris collection schedules to detect debris and debris. Smart roadways may deliver important information and alerts. In response to environmental factors and unforeseen occurrences like traffic congestion and casualties, you have access to detours. For a smart city using IoT, it is necessary to utilize RFID and sensors. Aware Home and Smart-Santander characteristics are existing applications in this field. Many prominent American cities, like Boston, are preparing to integrate the Internet of Things into most of their systems, including parking meters, street lights, sprinklers, and sewage grates. These are all linked together and have access to the Internet. These programs have advanced significantly in terms of cost and energy savings.

Healthcare

The majority of healthcare systems worldwide are ineffective, cumbersome, and invariably prone to mistakes. The healthcare industry depends on a wide range of processes and equipment, so technology automation and expansion are readily modifiable. The healthcare industry will undergo a massive transformation thanks to new technologies that make a variety of tasks more manageable, such as exchanging reports with numerous individuals and places, storing records, and distributing medications (Mano et al., 2016). IoT applications for health may provide many advantages that can be broadly grouped into the following areas: patient, staff, and asset monitoring, personal identity and authentication, automated data collecting and processing, and tracking. Monitoring patient flow may dramatically enhance medical facility operations. Additionally, authentication and identity are decreased by record keeping, newborn mismatch situations, and accidents that might injure the patient. The administration of medical inventories, process automation, faster form processing, automated procedure evaluations, and other functions depend on automated data collection and submission. The sensor device enables patient-focused capabilities, especially in diagnosing conditions and using real-time information on patient health indicators (Zanjal & Talmale, 2016). Monitoring patient adherence to prescriptions, telemedicine solutions, and patient health warnings are some of the application areas for this sector. The sensor may offer information after use and after patient monitoring and can be utilized with outpatients and inpatients, dental Bluetooth devices, and toothbrushes. RFID, Bluetooth, and WiFi are further IoT components that can be used in this situation. These greatly advance methods for measuring and keeping track of vital parameters like blood pressure, body temperature, heart rate, blood sugar, and cholesterol levels. The deployment of the Internet of Nano-things (IoNT) further improves the Internet of Things (IoT) and Internet of Everything (IoE) applications (Miraz et al., 2015). The word "IoNT" was created by integrating nano sensors into diverse objects utilizing nanonetworks, as the name suggests. One of the primary focuses of IoNT deployments is the medical industry. When IoNT is used on the human body for therapeutic reasons, data from in situ body components that were previously inaccessible utilizing large sensor-sized medical equipment may now be accessed. Therefore, IoNT enables the collection of new medical data that leads to discoveries and better diagnoses.

Smart Agriculture and Water Management

According to (Badran & Kashmoola, 2020), the agriculture industry may benefit from and be improved by the IoT by examining soil moisture and monitoring the diameter of the stem in

the case of vineyards. Thanks to the Internet of Things (IoT) we will be able to manage microclimate conditions, maximize the production and quality of vegetables and fruits, and monitor and preserve the number of vitamins in agricultural goods. Studying weather patterns can also manage temperature, and humidity levels to minimize fungal and other microbial contamination as well as anticipate ice information, droughts, wind changes, rain, and snow. The Internet of Things (IoT) assists with livestock identification and the detection of hazardous gases in animal waste on farms and improves health and survival potential by controlling the growth conditions of offspring increase. Additionally, via effective monitoring methods and administration of the whole agricultural sector, IoT applications in agriculture may help prevent significant waste and corruption. It also leads to better force and water control. As (Badran & Kashmoola, 2020) explains, the role of IoT in water management is to study sea and river water compatibility for both drinking and agricultural use, and pressure fluctuations in pipes and out of tanks. It also involves the detection of liquid as a way of monitoring changes in water levels in dams, rivers, and reservoirs. Wireless sensor networks are used in these IoT applications. The IoT apps SiSviA, GBROOS, and SEMAT are a few examples in this field.

Retail and Logistics

There are many benefits to implementing IoT in supply chain or retail management. Observing parking lot conditions throughout the delivery chain is one. Other examples include product monitoring for traceability considerations, price processing based on the region or hobby length in public transportation, theme parks, gyms, etc. IoT can operate in a variety of ways inside retail locations, including directing customers through the store based entirely on a pre-selected list, quickly learning with biometrics, identifying high-capacity allergen products, and managing the rotation of inventory on shelves and warehouses to automate replenishment processes (Sivakumar et al., 2020). WiFi sensor networks and radio frequency identification are examples of IoT components utilized in this setting. There might be a modern application for SAP (Systems Applications and Products). Several examples include acceptable consignment situations, object regions, detecting garage incompatibility issues, and fleet monitoring in logistics. In the enterprise domain, IoT enables in detection degrees of fuel line and leakages in the enterprise and its environs, maintaining tune of poisonous gases in addition to the oxygen degrees in the confines of chemical plant life to make sure the protection of products and people, and gazing degrees of oil, gases, and water in cisterns and garage tanks. The utility of IoT additionally assists in the preservation and restoration because structures may be installed vicinity to expect system malfunctions and on the equal routinely agenda periodic protection offerings earlier than there may be a failure withinside the system. The process may be executed by setting up sensors, internal systems, or equipment to screen their capability and ship reports.

Smart Living

In this domain, IoT may be carried out in faraway manipulated gadgets wherein you'll be able to transfer home equipment remotely and stale to stop injuries and save energy (Miraz et al., 2018). Other clever domestic home equipment consists of fridges outfitted with LCD (Liquid Crystal Display) screens, allowing one to recognize what's to be had interior, what has overstayed and is nearly expiring, and what wishes to be restocked. This data can also be related to a phone utility allowing one to get the right of entry to it whilst out of the residence's doors and consequently purchase what's needed. Additionally, washing machines allow for remote laundry screening. A range of kitchen appliances can be connected to via a phone, making it possible to change the temperature, for example inside an oven. It may not be difficult to monitor some ovens that have a self-cleaning feature. The home security provision of the IoT

can be used to operate an alarm system, and you can configure the camera to watch and detect window and door openings to repel attackers (Miraz et al., 2015).

Smart Environment

The surroundings have a crucial position in all elements of lifestyles, from humans to animals, birds, and flowers, and all suffer from bad surroundings in a single manner or another. There were several efforts to create healthful surroundings in phrases of getting rid of pollutants and decreasing the wastage of resources; however, irresponsible and harmful human behavior along with industrial waste and transportation habits are typical elements that continue to affect the environment. Consequently, the surroundings call for clever and modern approaches to assist in tracking and coping with the waste, which offers a vast quantity of facts that forces governments to install vicinity structures to shield the surroundings. Smart surroundings techniques integration with IoT generation have to be created for sensing, monitoring, and evaluating gadgets that provide capability advantages in reaching a sustainable lifestyle and an inexperienced world. The IoT generation permits staring at and coping with air first-rate thru facts series from far-off sensors throughout towns and presenting spherical clock geographic insurance to perform higher approaches of dealing with site visitors jams in the important cities. Additionally, you can implement IoT generation in measuring water pollutants tiers and therefore enlighten water usage choices. One can implement IoT in waste control, which includes numerous sorts of waste, like chemical substances and pollution being harmful to the surroundings and humans, animals, and flowers. Environmental safety can be done by controlling business pollutants through on-spot tracking and control structures blended with supervision, similar to decision-making networks, and reducing waste (Ruggeri et al., 2020). In climate forecasting, IoT may supply a vast accuracy and excessive decision for tracking the climate using record sharing and facts exchange. Climate structures can acquire records through IoT generation, including barometric pressure, humidity, temperature, light, movement, and different records, from motors in action and transmit the forms wirelessly to climate stations. The documents are attained by putting sensors on engines or even on homes, and then their miles are saved and analyzed to help in climate forecasting. Radiation is likewise a hazard to the surroundings, the fitness of people and animals, and agriculture output. In order to identify leakage and spread deterrence, IoT sensor networks may manage radiation by continuously tracking its levels, particularly in the vicinity of nuclear plant premises.

Challenges of IoT

For each of the aforementioned possible IoT applications, the success of some applications and their capabilities must have practical feasibility in different domains. The IoT faces issues and implications that must be addressed before it can be widely adopted, just like other technologies and innovations. While present IoT technology has improved significantly in recent years, many topics remain unresolved, providing the path for a new research dimension. The Internet of Things notion is derived from disparate technologies used to gather, exchange, process, generate, transmit, inform, manage, and store data, which unavoidably creates several research difficulties. As a result, these research agendas that need to be addressed have extended across a variety of study disciplines (Rehman et al., 2018).

Privacy and Security

Internet of Things (IoT) features need to be completely taken into account as Internet usage increases and the IoT emerges as a crucial part of the Internet's future. Many modern IoT devices have weaknesses, which researchers are aware of. Additionally, because the Internet of Things (IoT) is based on already-existing wireless sensor networks (WSNs), it shares WSNs' privacy and security flaws (Alansari et al., 2018). IoT system vulnerabilities and threats show

the need for many security measures to completely secure data and systems. Many assaults often take use of weaknesses in certain devices to obtain access to the system and, as a result, being vulnerable to secure devices (Abu Daia et al., 2018; Chaudhry et al., 2018). The vulnerability consists of cryptographically efficient research applied to data and system security, unencrypted security technology, and a framework that helps developers build secure systems on heterogeneous devices. Further, motivate a comprehensive security solution. Further research is needed on cryptographic security services on resource-constrained IoT devices. Cryptographic security enables users of varying skill levels to properly utilize and install IoT systems, despite the insufficient user interface accessible on practically any IoT device. In addition to the safety and security features of IoT, areas such as communication secrecy, dependability, connectivity partner reliability, message integrity, and additional security requirements must be included. Preventing communication between different parties can also be included. For example, smart objects need to prevent competitors from accessing sensitive information on their devices and using it maliciously in business transactions.

Processing, Analysis, and Management of Data

Processing, analysis, and data management are key issues due to the heterogeneity of the IoT and the vast amount of data generated, particularly in the age of big data (Alansari et al., 2018). The majority of systems rely on centralized systems to offload data and compute-intensive operations to overseas cloud platforms. There are also worries that standard cloud architectures would not be successful in transferring enormous volumes of data created and consumed by IoT-enabled devices and increasing support for accompanying computing demands while adhering to time limitations (Belkeziz & Jarir, 2017). As a result, the majority of systems rely on existing mobile cloud computing and fog computing technologies. To address this issue, both rely on edge processing. Another area of study in data management is the use of information-centric networks (ICNs) in the Internet of Things. As they allow content retrieval and fast access to services, these information-centric systems appear to be of considerable use in access, distribution, and control of created material and its delivery. This method, however, poses a number of issues, including how to correctly extend the ICN paradigm over Fixed Network Edge, enable IoT static and mobile devices, and separate ICN functionality into resource-constrained devices (Belkeziz & Jarir, 2017). Data analytics and its context play an essential role in the success of the IoT and pose significant challenges. The data collected must be used intelligently to implement innovative IoT capabilities. The creation of machine learning and artificial intelligence algorithms derived from neuronal activity, genetic algorithms, evolutionary algorithms, and many more artificial intelligence systems is essential to achieve automated decision-making.

Monitoring and Recognition

Surveillance and detection technology has made great strides but is constantly evolving with a focus on energy conservation and shape considerations. Detectors and trackers are usually expected to be always active to receive instant data. Because of this, they are critical for energy efficiency, significantly when extending life. Simultaneously, recent breakthroughs in nanotechnology/biotechnology and downsizing have allowed for the development of nanoscale actuators and sensors (Nikhat Akhtar & Yusuf Perwej, 2020).

M2M (Machine to Machine) Communication and Communication Protocols

Constrained application protocol (COAP) and message queue telemetry transport (MQTT) are examples of communication protocols geared for the Internet of Things, however there isn't an open IoT standard as of yet. All objects must be connected, although they are not all dependent on the Internet to send data to a particular gateway. Additionally, there are wireless

technologies like LORA, IEEE 802.15.4, and Bluetooth that are available, although it is uncertain whether these technologies must continue to provide a wide range of IoT connection options (Dwivedi, 2021). The device's communication protocol is the driving force in the settlement of the IoT application, which forms the primary support of the data stream between the sensor and the physical object or the external world. For traffic collision frequencies, multi-access, time division multiple connections, and carrier sense multiple MAC protocols for various domains (FDMA, TDMA, and CSMA) are used (FDMA, TDMA, and CSMA). The transport layer's primary tasks include assuring end-to-end dependability and providing end-to-end congestion control. In this regard, most protocols are incapable of providing proper end-to-end dependability (Bilal et al., 2018).

Blockchain of Things (BCoT)

Since 2018, blockchain technology has grown in popularity due to its integration with the Internet of Things (IoT). The Blockchain was developed primarily as the underpinning technology for Bitcoin currency, but it is currently employed in a variety of non-monetary applications (Ganapathy et al., 2020). Miraz contends that the IoT and Blockchain may empower each other by reducing their respective architectural constraints (Miraz, 2019). Because WSN is the IoT's key technology, it has security and data protection flaws. On the other hand, inherent security, immutability, dependability, and transparency are the main drivers of the blockchain deployment trend in non-monetary applications. Blockchain's consensus algorithm and Distributed Ledger Technologies (DLT), which both largely rely on participating nodes, make it possible for these properties to exist. The Blockchain of Things is a new term created by fusing the Blockchains of these two technologies with the Internet of Things (IoT) (BCoT). In this sense, the Blockchain augments the IoT by adding an extra layer of security, and "things" may be part of the IoT and operate as participating nodes in the blockchain ecosystem (Miraz, 2019). Therefore, the blockchain-enabled IoT ecosystem improves overall security (Abdelmaboud et al., 2022) and benefits each other.

Interoperability

Traditionally, interoperability is the fundamental core of the Internet. The essential requirement for an Internet connection requires that "connected" systems be able to "speak similar languages" concerning cryptography and protocols. It's valued, and it's still essential. Currently, different things are used in various industries.

Conclusion

The Internet of Things may be characterized as a dynamic network of interactions to adapt, requiring new and revolutionary software program engineering, structures engineering, task management, and several disciplines to broaden its development process and manipulate it in the coming years. Five-layer structure for the Internet of Things has been introduced. All companies that intend to apply the ability of the Internet of Things, in the first stage, must broaden a codified approach to this issue and must have a framework to address the vulnerabilities that arise. Drawing up a strategy focusing on the architecture can significantly thrive the achievement of the implementation. As a result, it minimizes the safety holes that will help understand Internet of Things applications. The main difficulty is that safety takes precedence above the convenience of Internet of Things devices or the network that connects those devices. Future research initiatives will embellish the IoT environment with statistical fingerprinting and blockchain technologies. This emerging networking paradigm will impact every aspect of our lives, from smart homes to health and environmental tracking, by embedding intelligence into the objects around us. Individuals, society, groups, and institutions are served by technology. Its wide range of adoption is already being researched; yet, without

resolving the challenging conditions in its development and providing secrecy of privacy and safety to the user, it is extremely unlikely to be a ubiquitous technology. Using IoT successfully is required to deal with safety and privacy threats and offer solutions. Researcher expects that more studies in the future will lead to IoT trends.

References

1. Abdelmaboud, A., Ahmed, A. I. A., Abaker, M., Eisa, T. A. E., Albasheer, H., Ghorashi, S. A., & Karim, F. K. (2022). Blockchain for IoT Applications: Taxonomy, Platforms, Recent Advances, Challenges and Future Research Directions. Electronics, 11(4), 630. https://doi.org/10.3390/electronics11040630.
2. Abu Daia, A. S., Ramadan, R. A., & Fayek, M. B. (2018). Sensor networks attacks classifications and mitigation. Annals of Emerging Technologies in Computing, 2(4), 28–43. https://doi.org/10.33166/AETiC.2018.04.003.
3. Alansari, Z., Anuar, N. B., Kamsin, A., & Soomro, S. (2018). ' S. August. https://doi.org/10.1007/978-3-319-95450-9.
4. Aleksic, S. (2019). A survey on optical technologies for IoT, smart industry, and smart infrastructures. Journal of Sensor and Actuator Networks, 8(3). https://doi.org/10.3390/jsan8030047.
5. Alenezi, M., Almustafa, K., & Meerja, K. A. (2019). Cloud-based SDN and NFV architectures for IoT infrastructure. Egyptian Informatics Journal, 20(1), 1–10. https://doi.org/10.1016/j.eij.2018.03.004.
6. Ali, O., Ishak, M. K., & Bhatti, M. K. L. (2021). Emerging IoT domains, current standings and open research challenges: a review. PeerJ Computer Science, 7, 1–49. https://doi.org/10.7717/peerj-cs.659.
7. Atlam, H. F., Walters, R. J., & Wills, G. B. (2018). Internet of nano things: Security issues and applications. ACM International Conference Proceeding Series, August, 71–77. https://doi.org/10.1145/3264560.3264570.
8. Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. Computer Networks, 54(15), 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010.
9. Badran, A., & Kashmoola, M. (2020). Smart Agriculture Using Internet of Things: A Survey. January. https://doi.org/10.4108/eai.28-6-2020.2298249.
10. Bandyopadhyay, D., & Sen, J. (2011). Internet of things: Applications and challenges in technology and standardization. Wireless Personal Communications, 58(1), 49–69. https://doi.org/10.1007/s11277-011-0288-5.
11. Belkeziz, R., & Jarir, Z. (2017). A survey on Internet of Things coordination. Proceedings - 2016 3rd International Conference on Systems of Collaboration, Sysco 2016, May. https://doi.org/10.1109/SYSCO.2016.7831328.
12. Bellini, P., Nesi, P., & Pantaleo, G. (2022). IoT-Enabled Smart Cities: A Review of Concepts, Frameworks and Key Technologies. Applied Sciences (Switzerland), 12(3). https://doi.org/10.3390/app12031607.
13. Bilal, D., Rehman, A.-U., & Ali, R. (2018). Internet of Things (IoT) Protocols: A Brief Exploration of MQTT and CoAP. International Journal of Computer Applications, 179(27), 9–14. https://doi.org/10.5120/ijca2018916438.
14. Chaudhry, J., Saleem, K., Haskell-Dowland, P., & Miraz, M. H. (2018). A survey of distributed certificate authorities in manets. Annals of Emerging Technologies in Computing, 2(3), 11–18. https://doi.org/10.33166/AETiC.2018.03.002.
15. Chen, W. (2013). An IBE-based security scheme on the Internet of Things. Proceedings - 2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems, IEEE CCIS 2012, 3, 1046–1049. https://doi.org/10.1109/CCIS.2012.6664541.
16. Dabbagh, M., & Rayes, A. (2019). Internet of Things Security and Privacy. Internet of Things From Hype to Reality, July, 211–238. https://doi.org/10.1007/978-3-319-99516-8_8.
17. Dwivedi, J. N. (2021). Internet of Things (IoT) and Machine to Machine (M2M) Communication Techniques for Cyber Crime Prediction. Intelligent Data Analytics for Terror Threat Prediction, January, 31–55. https://doi.org/10.1002/9781119711629.ch2.
18. Ganapathy, A., Rahaman, M., & Khan, W. (2020). Artificial Intelligence-Driven Crypto Currencies. 9(2), 107–118.
19. Guo, L. G., Huang, Y. R., Cai, J., & Qu, L. G. (2011). Investigation of architecture, key technology and application strategy for the Internet of things. Proceedings of 2011 Cross-Strait Quad-Regional Radio Science and Wireless Technology Conference, CSQRWC 2011, 2, 1196–1199. https://doi.org/10.1109/CSQRWC.2011.6037175.
20. Hussein, A. R. H. (2019). Internet of Things (IOT): Research challenges and future applications. International Journal of Advanced Computer Science and Applications, 10(6), 77–82. https://doi.org/10.14569/ijacsa.2019.0100611.

21. Iannacci, J. (2015). RF-MEMS: an enabling technology for modern wireless systems bearing a market potential still not fully displayed. Microsystem Technologies, 21(10), 2039–2052. https://doi.org/10.1007/s00542-015-2665-6.
22. Jain, R. (2018). A congestion control system based on vanet for small length roads. Annals of Emerging Technologies in Computing, 2(1), 17–21. https://doi.org/10.33166/AETiC.2018.01.003.
23. Kaur, C. (2020). The Cloud Computing and Internet of Things (IoT). International Journal of Scientific Research in Science, Engineering and Technology, January, 19–22. https://doi.org/10.32628/ijsrset196657.
24. Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012). Future Internet: The Internet of things architecture, possible applications and key challenges. Proceedings - 10th International Conference on Frontiers of Information Technology, FIT 2012, 257–260. https://doi.org/10.1109/FIT.2012.53.
25. Khoo, B. (2011). RFID As an enabler of the Internet of things: Issues of security and privacy. Proceedings - 2011 IEEE International Conferences on Internet of Things and Cyber, Physical and Social Computing, IThings/CPSCom 2011, October 2011, 709–712. https://doi.org/10.1109/iThings/CPSCom.2011.83.
26. Kumar, S., Tiwari, P., & Zymbler, M. (2019). Internet of Things is a revolutionary approach for future technology enhancement: a review. Journal of Big Data, 6(1). https://doi.org/10.1186/s40537-019-0268-2.
27. Malik, A., Magar, A. T., Verma, H., Singh, M., & Sagar, P. (2019). A detailed study of the internet of things (Iot). International Journal of Scientific and Technology Research, 8(12), 2989–2994.
28. Mano, L. Y., Faiçal, B. S., Nakamura, L. H. V., Gomes, P. H., Libralon, G. L., Meneguete, R. I., Filho, G. P. R., Giancristofaro, G. T., Pessin, G., Krishnamachari, B., & Ueyama, J. (2016). Exploiting IoT technologies for enhancing Health Smart Homes through patient identification and emotion recognition. Computer Communications, 89–90, 178–190. https://doi.org/10.1016/j.comcom.2016.03.010.
29. Mazayev, A., Martins, J. A., & Correia, N. (2017). Interoperability in IoT Through the Semantic Profiling of Objects. IEEE Access, 6(December), 19379–19385. https://doi.org/10.1109/ACCESS.2017.2763425.
30. Miraz, M. H. (2019). Blockchain of Things (BCoT): The Fusion of Blockchain and IoT Technologies. In SSRN Electronic Journal (Issue September). https://doi.org/10.2139/ssrn.3464085.
31. Miraz, M. H., Ali, M., Excell, P. S., & Picking, R. (2015). A review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT). 2015 Internet Technologies and Applications, ITA 2015 - Proceedings of the 6th International Conference, September, 219–224. https://doi.org/10.1109/ITechA.2015.7317398.
32. Miraz, M. H., Ali, M., Excell, P. S., & Picking, R. (2018). Internet of Nano-Things, things and everything: Future growth trends. Future Internet, 10(8). https://doi.org/10.3390/fi10080068.
33. Mohamad Noor, M. binti, & Hassan, W. H. (2019). Current research on the Internet of Things (IoT) security: A survey. Computer Networks, 148, 283–294. https://doi.org/10.1016/j.comnet.2018.11.025.
34. Nikhat Akhtar, & Yusuf Perwej. (2020). The Internet of nano things (IoNT) existing state and future Prospects. GSC Advanced Research and Reviews, 5(2), 131–150. https://doi.org/10.30574/gscarr.2020.5.2.0110.
35. Nimodiya, A. R., & Ajankar, S. S. (2022). A Review on Internet of Things. International Journal of Advanced Research in Science, Communication and Technology, 113(1), 135–144. https://doi.org/10.48175/ijarsct-2251.
36. Patel, K. K., Patel, S. M., & Scholar, P. G. (2016). Internet of Things-IoT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges. International Journal of Engineering Science and Computing, 6(5), 1–10. https://doi.org/10.4010/2016.1482.
37. Rehman, H. U., Asif, M., & Ahmad, M. (2018). Future applications and research challenges of IoT. 2017 International Conference on Information and Communication Technologies, ICICT 2017, 2017-December (December 2017), 68–74. https://doi.org/10.1109/ICICT.
38. Rekha, S., Thirupathi, L., Renikunta, S., & Gangula, R. (2021). Study of security issues and solutions in Internet of Things (IoT). Materials Today: Proceedings, August. https://doi.org/10.1016/j.matpr.2021.07.295.
39. Roman, R., Alcaraz, C., Lopez, J., & Sklavos, N. (2011). Key management systems for sensor networks in the context of the Internet of Things. Computers and Electrical Engineering, 37(2), 147–159. https://doi.org/10.1016/j.compeleceng.2011.01.009.
40. Ruggeri, G., Loscrí, V., Amadeo, M., & Calafate, C. T. (2020). The Internet of things for smart environments. Future Internet, 12(3), 10–11. https://doi.org/10.3390/fi12030051.
41. Shen, G., & Liu, B. (2011). The visions, technologies, applications and security issues of the Internet of things. 2011 International Conference on E-Business and E-Government, ICEE2011 - Proceedings, 1867–1870. https://doi.org/10.1109/ICEBEG.2011.5881892.
42. Sivakumar, V., Ruthramathi, R., & Leelapriyadharsini, S. (2020). Internet of things: Benefits and challenges of logistics service providers in India. International Journal of Scientific and Technology Research, 9(2), 1949–1953.
43. Suo, H., Wan, J., Zou, C., & Liu, J. (2012). Security in the Internet of things: A review. Proceedings - 2012 International Conference on Computer Science and Electronics Engineering, ICCSEE 2012, 3(March), 648–651. https://doi.org/10.1109/ICCSEE.2012.373.

44. Tapia, E. M., Intille, S. S., & Larson, K. (2007). Portable wireless sensors for object usage sensing in the home: Challenges and practicalities. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 4794 LNCS, 19–37. https://doi.org/10.1007/978-3-540-76652-0_2.
45. Tyagi, S., Darwish, A., & Khan, M. Y. (2014). Managing Computing Infrastructure for IoT Data. Advances in Internet of Things, 04(03), 29–35. https://doi.org/10.4236/ait.2014.43005.
46. Vermesan, O., & Friess, P. (2014). Internet of things applications: From research and innovation to market deployment. Internet of Things Applications: From Research and Innovation to Market Deployment, June, 1–371.
47. Worlu, C., Jamal, A. A., & Mahiddin, N. A. (2019). Wireless Sensor Networks, Internet of Things, and Their Challenges. International Journal of Innovative Technology and Exploring Engineering, 8(12S2), 556–566. https://doi.org/10.35940/ijitee.l1102.10812s219.
48. Wu, M., Lu, T. J., Ling, F. Y., Sun, J., & Du, H. Y. (2010). Research on the architecture of Internet of Things. ICACTE 2010 - 2010 3rd International Conference on Advanced Computer Theory and Engineering, Proceedings, 5(September 2010). https://doi.org/10.1109/ICACTE.2010.5579493.
49. Yaïci, W., Krishnamurthy, K., Entchev, E., & Longo, M. (2021). Recent advances in Internet of things (IoT) infrastructures for building energy systems: A review. In Sensors (Vol. 21, Issue 6). https://doi.org/10.3390/s21062152.
50. Yun, M., & Yuxin, B. (2010). Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid. 2010 International Conference on Advances in Energy Engineering, ICAEE 2010, 69–72. https://doi.org/10.1109/ICAEE.2010.5557611.
51. Zanjal, S. V., & Talmale, G. R. (2016). Medicine Reminder and Monitoring System for Secure Health Using IoT. Physics Procedia, 78(August), 471–476. https://doi.org/10.1016/j.procs.2016.02.090.
52. Zhang, H., & Zhu, L. (2011). Internet of Things: Key technology, architecture and challenging problems. Proceedings - 2011 IEEE International Conference on Computer Science and Automation Engineering, CSAE 2011, 4, 507–512. https://doi.org/10.1109/CSAE.2011.5952899.
53. Zhang, M., Sun, F., & Cheng, X. (2012). Architecture of Internet of Things and its key technology integration based-on RFID. Proceedings - 2012 5th International Symposium on Computational Intelligence and Design, ISCID 2012, 1, 294–297. https://doi.org/10.1109/ISCID.2012.81.
54. Zhang, Y. (2011). Technology framework of the Internet of Things and its application. 2011 International Conference on Electrical and Control Engineering, ICECE 2011 - Proceedings, 4109–4112. https://doi.org/10.1109/ICECENG.2011.6057290.

Cite this article:

Md. Mahbubur Rahaman (2022). A Review on Internet of Things-IoT- Architecture, Technologies, Applications & Future Challenges. *International Journal of Science and Business, 14*(1), 80-92. doi: https://doi.org/ 10.5281/zenodo.7066810

Retrieved from http://ijsab.com/wp-content/uploads/958.pdf

Published by