ПРОГРЕСИВНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ, ВИСОКОПРОДУКТИВНІ КОМП'ЮТЕРНІ СИСТЕМИ

UDC 62-50
DOI: 10.20535/SRIT.2308-8893.2024.1.01

POTENTIAL APPLICATIONS OF INTERNET OF THINGS: A COMPREHENSIVE ANALYSIS

M. PUNITHA, P.M. REKHA

Internet of Things (IoT) is the amalgamation of hardware, like sensors and trackers, which monitor several parameters of the environment or physical objects, and software that processes all the data gathered by hardware. Globally, the IoT market is anticipated to reach 53.8 billion USD by 2025. This enhancing demand is due to its innate ability to automate, which drives several industries to adopt IoT. In addition, minimum memory cost, processing, and storage with an increase in Big Data (BD), cloud, and conjunction of industrial networks and the internet are the added factors for the increase in IoT development. Due to this significance, IoT has applications in numerous areas like medical management, farming, wearable technology, smart energy meters, smart cities, etc. The applications are not limited to the examples mentioned above. Considering this, existing studies have considered different applications and attempted to execute them. As different applications have been focused on by these studies, the present review intends to provide a compilation of potential applications of IoT as considered by conventional research between 2018 and 2022. The study also intends to explore the advantages and disadvantages of different IoT applications (deliberated by conventional studies) through tabular analysis. Further, this review emphasizes IoT's major key challenges and countermeasures to resolve its security issues. Finally, the study affords recommendations that will assist all IoT experts in bringing IoT products with enhanced security into the market.

Keywords: Internet of Things, automation, security, potential applications.

INTRODUCTION

The contemporary universe is experiencing silent smart evolution with enhancing technological progress touching all life aspects. Smart technologies positioned as the epi-centre of DT (Digital Transformation) possess drastic result leasing to innovation towards designing IoT (Internet of Things) as the main pillar of recent Industry 4.0 [1]. IoT is defined as the network of objects embedded with circuits, sensors, electronics, and connectivity, which permits the objects for gathering and transmitting data. In IoT, the term 'thing' might be a vehicle with in-built sensors or any manmade or natural objects for which an IP (Internet Protocol) address could be assigned by which data could be transferred on a network. Consequently, it has become easy for creating chances to directly incorporate the world into computer-oriented systems that lead to efficiency, enhancements, minimized human exertion, and economic benefits. IoT definition has aroused due to the con-

junction of several technologies like ML (Machine Learning), the internet, automation, micro-electromechanical systems, and wireless technology. This conjunction has enabled to bridge of the gap between information and operational technology permitting unstructured machine-retrieved data to remain examined for insights that will bring innovation. It permits objects to get sensed and managed remotely throughout the existing infrastructure of the network creating choices to directly integrate the physical environment into computer-oriented systems. IoT is also capable of interacting with no human intervention. Few primary IoT applications already exist in transportation, automotive industries, and healthcare. By a report produced by a business insider, nearly 24-billion IoT-based devices were used by 2020. It has also been predicted that the revenue of IoT will touch 300 billion dollars in the upcoming years which will lead to numerous jobs in various industries. This vast reach is due to the significance of IoT which includes real-time monitoring and tracking, optimal decision-making, automation, and the capability of IoT for affording sensor information and permitting communication between devices.

For instance, automatic driving technology demands huge data from several sensors embedded within vehicles. These embedded sensors gather the engine's behaviour, field data, and camera feed for enhancing the self-driving method for handling any circumstance which could happen while driving. IoT also possesses several other applications. IoT finds its application in smart grids for energy management where sensors are deployed on each customer outlet and transmission line. These sensors assist in notifying failures, and irregularities in line, realizing the behavior pattern and usage nature over time. The smart meters could also alert the customers regarding the cost of peak time and non-peak time based on which cost can be reduced. In addition, IoT is applicable in fleet management. IoT logistics have been a complicated task as goods have to be dealt with better efficiency and care. Despite transmission from one place to another, the service providers must confirm that correct conditions are maintained at the transportation time. To alleviate such manual efforts, smart sensors that can connect with IoT networks persistently monitor GPS location, container's tilt angle, shock, temperature, and humidity. Data gathered from such sensors are later processed and evaluated in a central cloud server. This information could be accessed by the logistics team from anywhere through the internet. Fleet movement could also be monitored in real-time and later conveyed to customers regarding the delivery progress. Besides, IoT finds its application in the manufacturing sector where the initial IoT adopters have altered various phases of product development. IoT (Industrial IoT) will assist in optimizing several manufacturing phases through monitoring of inventory management and supply chain, quality testing, product enhancement, etc. Further, IoT could be employed in agriculture to support researchers and farmers to discover several cost-efficient and optimized manners to enhance production. Individual agriculture stages can be improved through smart-sensor technology; automation supports to minimize manual labour. Additionally, IoT is applicable in the healthcare sector for saving the lives of individuals. Initiating from the gathering of essential data from bedside devices, accessing patient information and healthcare records throughout several departments and real-time processes in diagnosing, overall patient care could be enhanced with the execution of IoT. In addition to such useful applications of IoT, there also exist certain issues due to IoT usage [2]. Hence, the present work intends to summarize the significant challenges in IoT use and countermeasures to solve the drawbacks along with the analysis of existing works about potential applications of IoT.

Objectives

The major objectives of the present work are listed below:

- To comprehensively examine the potential IoT applications as considered by traditional works ranging from (2018–2022) to bring out the drawbacks faced by these works.
- To discuss the advantages and disadvantages of different IoT applications (considered by conventional studies) through tabular analysis.
- To emphasize the major key issues of IoT and countermeasures to resolve the security challenges of IoT along with recommendations that will assist IoT experts while designing products in the future.

Paper Organization

Section 2 explores the IoT evolution and its concepts. This is followed by IoT architecture, protocols, and significance of IoT in section 3. Subsequently, the potential applications of IoT are discussed in section 4. After this, a comparative analysis is presented in section 5. Following this, major key challenges are summarized in section 6 with the countermeasures for security problems in IoT in section 7. Finally, the entire study is concluded in section 8.

EVOLUTION OF IOT (INTERNET OF THINGS) AND ITS SIGNIFICANT CONCEPTS

The arrival of smart concepts has made the globe become completely connected. These concepts create a network of several devices. Its fundamental role involves the connection of several devices for transmitting and receiving data. Kevin Ashton was the one who invented the term “IoT” in 1999. Following this, LG established the first smart fridge in 2000. After 7 years, 1st iPhone was introduced. IoT has accomplished significant influence on the globe in its initial phase and will also persist to evolve with time. The concept of IoT has also bought numerous applications ranging from fiction to statistics permitting the 4IR (Fourth Industrial Revolution). This has caused a significant impact on social, technical, and economic aspects. Scientists have stated that probable merits attained from IoT technology will develop a predictable future where smart things sense, contemplate and act. It is a trending technology that embodies several concepts like edge computing, electronic devices, geo-location of the sensor, fog computing, etc. A basic IoT concept is the things that have aroused to encompass several device kinds from wireless sensors and RFID tags to intricate systems like consumer devices and many more basic facilities. IoT possesses diverse names which expand or refine its overall possibility. Examples include IoE (Internet of Everything-things like processes, people, data, and connection), and IIoT (Industrial IoT-explaining how IoT employs in the manufacturing and industrial sector) [3]. IoT comprises huge interconnected devices as a network. Such devices transmit and gather huge data amounts regarding how they function and describe the information stored by the devices. These devices also possess sensors embedded within them which continuously emit information about the environment along with the functionality of the devices. Thus, IoT acts as a medium for dumping all the information gathered by IoT devices.

This platform examines data completely for gathering significant information which is later sent back by the data afforded. Lastly, gathered data is shared among other devices to achieve better performance to enhance the experience of users [4]. In the past era, IoT has multiplied its attention in numerous areas. Accordingly, numerous researchers have tried to afford a glimpse of the IoT landscape. The study [5] intended to realize the evolvement of IoT and its diversified technologies, applications, services, and concepts. It has been explored that, AI (Artificial Intelligence), CC (Cloud Computing), and BDA (Big Data Analytics) have a crucial contribution as IoT has been advancing its vision of smart services by the use of connected devices. Though the notion of the IoT concept has been prevailing for a long time, numerous technologies have made this concept practical. Reliable and affordable sensors have been making this technology probable for several manufacturers. Different network IPs (Internet Protocols) have made it ease in connecting sensors to the cloud for effective transmission of data. With the progress in ML (Machine Learning), analytics, and access to huge data stored in the cloud, businesses could gain fast and easy insights. The advent of such allied technologies persists to drive IoT boundaries, the overall evolution of IoT is tabulated in Table 1.

Table 1. IoT Evolution

S. no	References	IoT-Paradigms	Ahead of 2010	2010 to 2015	2015 to 2020	After 2020
1	[6]	Network	Sensor-networks	Self-organized and self-aware networks Transparency in locating sensor network Delay tolerant network Power network and storage network Hybrid networking	Awareness of network context	Self-learning and self-restoring networks Cognitive network
2	[3]	Hardware	Some sensors and RFID tags Construction of sensors into mobile NFC (Near Field Communication) in mobile Cheap and small MEMs technology	Multi-standard and multi-protocol readers More actuators and sensors Low-cost and secure tags (For example-silent-tags)	Biochemical (smart sensors) Tiny sensors (actuators and numerous sensors)	New materials and nano-technology
3	[7]	Data-processing	Processing serial data Processing parallel data QoS (Quality of Services)	Energy, frequency, and spectrum-aware processing of data Context-adaptable data processing	Context-aware processing of data and responses	Cognitive processing and cognitive optimization
4	[8]	Algorithms and Software	Integrating relational database IoT concerned with RDBMS Event oriented platforms Sensor-middleware Sensor network-middleware Localization or proximity algorithms	Open and large-scale semantic software components Assembly algorithms Social software based on NextGen (Next Generation) IoT Enterprise applications based on NextGen IoT	Goal oriented software Problem-solving and distributed intelligence Things to Things collaborative environment	User-oriented software Invisible IoT Easy to deploy IoT Things to Human Collaboration IoT-for-all

IoT-ARCHITECTURE AND PROTOCOLS

No single agreement of IoT architecture exists which is approved universally. Varied architectures have been endorsed by different investigators. For instance, the study [9] suggests a decentralized framework relying on SDN (Software Defined Networking) integrated with block chain for IoT in a smart city. The recommended framework depends on three major SDN technologies namely mobile computing, fog computing, and edge computing for detecting the attack existence in IoT networks.

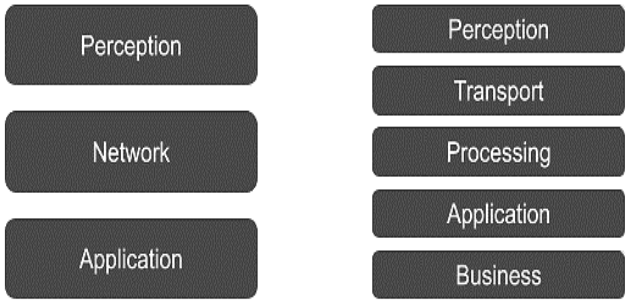
After the accomplishment of initial research on IoT, 3-layered architecture remained the central model for the applications based on IoT. These 3-layers include the perception layer, network layer, and application layer.

Perception layer: sensors stay in this layer and this is the area from where the data arrives. Data might be collected from numerous sensors on the connected device. The actuators which work on their surrounding also exist in this layer.

Network layer: this layer explores how huge data are moving in the application. It also connects several devices and transfers the data to suitable back-end services.

Application layer: it is the layer that the users view. It could be a dashboard exploring device status that is the system's part or an application for controlling a device.

The 3-layered model is a good manner of explaining an IoT-based project. However, it is restricted in possibility. Due to this reason, several proposed models possess additional or different layers and this renowned model is termed a 5-layered model. It includes the perception layer, transport layer, processing layer, application layer, and business layer. In this case, the role of the perception layer and application layer seems to be similar to 3-layered architecture. On contrary, the transport layer performs sensor data transformation from the perception layer to the processing layer and inversely through networks like 3G, Bluetooth, NFC, RFID, wireless, and LAN. Following this, the processing layer (also termed as middleware layer stores, evaluates, and processes many data which arrive from the transport layer. This layer could manage and afford diverse service sets to lower layers which apply numerous technologies like databases, CC, and BD processing modules. Lastly, the business layer maintains the entire IoT system which includes business, applications, and profit frameworks along with the privacy of users. The 3-layered and 5-layered models are shown in Figure taken from source [10].



3-layered architecture 5-layered architecture

3-layered and 5-layered architecture [10]

Further, IoT devices utilize network protocols and standards for permitting physical objects for interacting with one another and the cloud. Standards and network protocols are policies that include certain rules which explain the communication amongst many devices throughout the network. Moreover, single devices namely personal computers and smartphones also utilize network protocols to perform communication. However, general protocols which are utilized by these devices might seem to be unfit for specific necessities like latency, range, and bandwidth of solutions based on IoT. Thus, a few enhanced versions of a few prevailing protocols and new IoT protocols have arouse to satisfy the needs of IoT devices. These standards and IoT protocols are extensively categorized into two distinct divisions. This includes IoT data protocols and IoT network protocols.

IoT data protocols [11]: these are utilized for connecting IoT devices of low power. They afford communication with the hardware on the user's side without requiring an internet connection. Connectivity in these standards and protocols exists through cellular or wired networks. Some IoT data protocols are listed below.

HTTP (Hypertext Transfer Protocol). HTTP (Hypertext Transfer Protocol): is an application layered protocol that transmits hypermedia documents like HTML. It was framed for communication amongst web servers and browsers. However, it could also be utilized for several other purposes. It is a segment of the IP suite and states the services and commands utilized to transfer the data of the webpage. It exists as a basis for the exchange of any data on the web and is a client and server protocol that indicates that requests are started by the recipient (typically a web browser).

CoAP (Constrained Application Protocol). CoAP (Constrained Application Protocol): is an application layer protocol that is designed for addressing the requirements of IoT systems relying on HTTP. It is ideal for usage in devices having limited resources like WSN nodes or IoT microcontrollers.

AMQP (Advanced Message Queuing Protocol). AMQP (Advanced Message Queuing Protocol): is an open-standard application layered protocol utilized for the transaction of messages amongst the servers. It permits interoperable and encrypted messaging amongst applications and organizations. The main operation of this protocol involves: receiving and positioning messages (in queues), setting an interaction amongst the messages, and storing the messages. With its reliability and security level, it is generally applied in settings that need analytical environments based on the server like the banking sector. Nevertheless, it is not extensively utilized elsewhere.

MQTT (Message Queuing Telemetry Transport). MQTT (Message Queuing Telemetry Transport): is a lightweight protocol and features a publisher and subscriber model that permits the simple flow of data amongst varied devices. Despite the wide adoption of this protocol as an IoT standard especially with industrial applications, it seems to not assist defined device management and data representation.

DDS (Data Distribution Service). DDS (Data Distribution Service): is an ascendable IoT protocol that permits high-quality interaction in IoT. Alike MQTTT, it also operates with the publisher and subscriber model and could be installed in numerous settings from cloud to small devices which makes it ideal for embedded and real-time systems.

IoT network protocols [12]: are utilized for connecting devices to a network. Typically, these protocols are used over the internet. A few of the network protocols of IoT are listed below.

Bluetooth. It is a widely utilized protocol for communicating within a specific range. It remains a standard communication protocol of IoT which is optimal for low-powered, short-range, and low-cost wireless transmission amongst electronic devices. Besides, BLE (Bluetooth Low Energy) remains a version of Bluetooth which minimizes the consumption of power and has a crucial part in connecting IoT devices.

Zigbee. These networks are identical to Bluetooth in the aspect that, it already possesses a significant base for the user in the IoT world. Nevertheless, its specifications marginally conceal the use of Bluetooth. It consumes low power and possesses a low range of data, a long communication range, and high security. It is a simple protocol for exchanging data and is frequently executed in devices having minimum needs like sensors and microcontrollers.

RFID (Radio Frequency Identification). RFID (Radio Frequency Identification): utilizes radio waves for transmission of fewer data packets upon network within the low range. It seems to be easy for embedding the RFID chip into IoT devices. After embedding, the RFID readers could read the corresponding tags and afford information regarding the product which is attached to the tags. Common RFID applications include inventory management. Through the attachment of RFID tags to products and then connecting them with IoT devices, businesses could track the available product count.

Wi-Fi (Wireless Fidelity). It is a renowned IoT protocol utilized for connecting neighbouring devices existing within a particular range by broadcasting a signal or hotspot. Generally, this connection makes use of several radio waves which are meant in broadcasting information upon specific frequencies namely 2.4GHz, 5GHz, or 6GHz. Presently, 6GHZ is probable to evolve as the biggest novelty in the past twenty years. It remains the core of this DT (Digital Transformation) which will permit reliable and fast interactions from the next device generation.

Significance of IoT

Tracking and Monitoring in Real-Time. The potential of a web-based system for monitoring and tracking is numerous. IoT tracking affords effective means for monitoring and tracking everything from stolen goods, and shipping containers to vehicle fleets. Distinct devices could also detect alterations in climatic conditions. Multiple industries exist where IoT trackers could immensely enhance the company's efficacy. For instance: IoT devices find their significance in determining COVID-19 by following individual infected persons and taking suitable actions for reducing its spread. Through the data gathered from several tracking devices, it is possible to find the area affected with the maximum number of victims. Additionally, the individuals who are absconding from the isolation wards or clinics could also be found. It is also probable to monitor the suspects. Conclusively, with the assistance of IoT devices, the exposure rate could be effectively controlled with the enhancement of patient health [13].

Optimal Decision Making. IoT devices possess numerous sensors based on which they could gain considerable data from several sources, affording them additional information for working with the data obtained. For instance, the study

[14] has explored an integrative agricultural monitoring system through the use of IoT and smartphone application. Through the use of this system, farmers could remotely observe the farm for determining the soil's pH level, wetness duration of the leaf, humidity, temperature, and soil moisture. The system quickly evaluates the soil and weather conditions in the specific region where the plant exists and affords new insights for manipulating the decision process. For instance, the article [15] intended to outline and progress control through the sensor modes in crop areas with the management of data through web applications and smartphones. This permits manual or automatic management by users. Automatic control utilizes data from the sensors used to monitor the soil moisture for watering. Nevertheless, the user could opt for manual management of crop watering in functional mode. The system could also send notifications by LINE API for line applications. Outcomes have explored the execution to be valuable in agriculture.

Automation. The main reason behind the IoT invention is convenience. The smart devices which automate day-to-day tasks permit humans for performing other activities. Such devices lessen the workload of people. For instance, the research [16] has explored that home automation methods are moving to mechanization techniques wherein machinery equipment manages varied systems in houses with less effort from humans. It also forces the automatic management of home appliances by several technologies. A Bluetooth kit used for automating homes is cheap and versatile. However, it could be used only within a limited range. Moreover, an automation solution utilized a zigbee-RF module for creating a wireless network that permits users for remote monitoring of the appliances at home. GSM-based automation outline is also under consideration wherein consumers could monitor and manage the home appliances by transferring messages from the corresponding devices.

POTENTIAL APPLICATIONS

Generally, day-to-day applications work smart. However, they are not able to interact with one another. To permit them for communicating with one another for sharing valuable information, IoT comes into origin with wide applications. These evolving applications with autonomous abilities would certainly enhance the lives of individuals. IoT is bringing technological modifications to the daily lives of people which assists in creating and comfortable and simple life through several applications and technologies. There are innumerable IoT applications in almost all domains inclusive of industry, medicine, education, mining, transportation, governance, manufacturing, etc. Some common and recent applications of IoT are discussed in this section.

IoT based smart-city

IoT possesses good importance in constructing smart cities. It also holds positive implications in enhancing the progress of urban trade which includes the industry throughout the city with commercial progress in the city's central area. In a huge sense, realizing IoT is of huge importance to re-alter the city's industrial structure that encompasses the features of centralized use of resources and optimizing a smart city's structure. The direct influence of executing IoT is to minimize the cost of information management. As IoT relies on a network, it quickly processes, stores and transfers huge information. As a new technology, the physical network

not only creates new opportunities for the economic development of urban areas but also improves the creation of new management and production techniques. An IoT model relying on fog-computing has been endorsed in the study [17] that efficiently resolves the network scalability and BD processing issues. This model has been suggested to create efficient, harmonious, and coordinated operations of the city through several information processing, network transmission and intelligent perception means. Analytical outcomes have explored that, the recommended scheme has been suitable for fog-environment having numerous computing resources. Additionally, IoT could be utilized in several ways for making the cities highly effective ranging from the management of traffic, air pollution control, waste management, early planning for environmental disasters, creation of smart buildings, etc. For providing traffic solutions, IoT makes use of varied sensor kinds and fetches GPS location from the smartphone of drivers to find the location, vehicle speed, and number. Concurrently, traffic lights based on IoT connected with cloud platforms permit the monitoring of timings of the green light and automatically modify the lights relying on the current circumstance of traffic to avoid congestion. In addition, the use of historical data and smart solutions to manage the traffic could forecast where traffic might go and undertake measures for preventing probable congestion. Further, for monitoring air pollution, an IoT-based system has been considered for observing the quality of air upon the server through the internet. This will prompt an alarm if the quality of air exceeds a certain level indicating that, there are enough quantity of detrimental gases existing in the air namely smoke, benzene, etc. general use of IoT is managing waste through route optimization. It minimizes the consumption of fuel thereby emptying the dustbins all over the city. Moreover, IoT also assists in determining natural disasters before their occurrence. The sensors and IoT devices gather real-time information on things namely volcanic activity, barometric readings, and water levels. The sensors could detect tornadoes, earthquakes, cloudbursts, etc, and alerts through initial warnings. Thus, with its minimum energy consumption, great connectivity, low cost, and strong coverage, IoT has turned out to be a key expertise in smart-city creation. Nevertheless, faced with numerous terminals, non-uniformity in smart buildings, rational assignment of restricted resources, and integration of heterogeneous data have become significant trends in the IoT study area. Consequently, the study [18] has suggested a method to process the heterogeneous data gathered by IoT networks in smart-building thereby converting them into standardized homogeneous data which could be taken as input to monitor and manage the procedures in smart buildings to optimize its performance.

IoT-based smart home

Using IoT for home automation has become a modern lifestyle to comfort the citizens of smart cities. The person who is employing applications for home automation at the time of construction of the home could manage, monitor as well as regulate the use of energy in all probable manners. It lessens the manual work. For instance, a lamp in a bedroom glows automatically once an individual enters the room. Moreover, lights in a specific area in the home could be programmed to automatically switch on or off. Such home automation comes with several advantages: they bring safety through the appliance, enables light control, enhances awareness through cameras, and improvises convenience through automatic temperature adjustments, alarm control, smartphone alerts, energy management, etc. Some significant applications of IoT in automating homes are emphasized in the study [19]. It has been claimed that IoT manages home automation devices from

any place throughout the globe by managing them from tablets, smartphones, and personal computers. Monitoring has been another factor of IoT for affording how things could be known in advance in terms of water distribution, security alarms, and energy management. User-friendliness has been a significant factor of IoT for managing home utilizations with less interface, limited range of wireless transmission, and easy opera table through tablets and smartphones. Similarly, the research [20] has suggested a system with interconnecting sensors, data sources, and actuators to accomplish multi-purpose home automation. This system has been termed a toggle which works by holding the ability for powerful and flexible API (Application Program Interface) that indicates the basis of a common and simple communication mechanism. Most devices utilized by qToggle rely on raspberry-pi boards or ESP8266 or ESP8285. Besides, an application has also been developed which permits users for managing the sequence of sensors and home appliances. In such cases, qToggle has been utilized for several purposes like controlling temperature and lights, security alarms, garden sprinklers, concurrent opening and closing of doors, and observing energy and power. Suggested qToggle has been flexible, and user-friendly and could be developed through the use of varied devices.

IoT for smart-energy

IoT has become a boundless ally in managing energy consumption and smart distribution in smart system cases. With the enhancement of IoT networks for optimal energy, a smart meter comes with additional operations namely bidirectional communication which permits the integration of networks and users, controlling smart equipment, etc. Smart meters remain the basic component of a smart grid. Moreover, meters utilized with a management system could be used to monitor and control the appliances of the home and other devices by the requirements of users. In a contemporary smart home, IoT and smart meters have been hugely deployed for altering the conventional analog meters which digitalize the meter readings and data gathered. Data could be transmitted wirelessly which significantly lessens the manual efforts. Nevertheless, the smart home community has been susceptible to the theft of energy. These attacks could not be detected effectively as the conventional methods need specific device installation to make it work. This levies an issue for such theft detection to be executed despite the deficiency in devices for energy monitoring. To resolve this, the study [21] has developed SETS (Smart Energy Theft System) which relies on statistical models and ML (Machine Learning). Three stages of decision taking modules exist. The initial stage involves the prediction framework that utilizes a multi-model prediction system. The such system integrates several ML models into a forecast system to determine the rate of power consumption. This has been followed by the primary decision-making model which makes use of SMA (Simple Moving Average) to filter the abnormality. The final phase includes a secondary decision-making framework which creates the final decision stage on energy stealing. Simulation outcomes have represented that; the endorsed system could perform successful detection at a rate of 99.6% which improves IoT security in a smart home for saving energy. It has also been found that SETS has improved IoT security from energy theft and could be further executed in industrial and commercial sectors. The solution of the single integrated system has to be economical and effective. Smart computation systems permit the monitoring of energy consumption thereby af-

fording valuable information regarding the quality of energy. The information afforded by such systems has been utilized by operators for enhancing the energy supply. Varied methodologies could also be employed on this end like charge scheduling, demand side management, and non-intrusive monitoring of load. The intention of the research [22] has been to design, construct, explore and validate the solution for a cheap smart meter to monitor energy consumption based on IoT. It transfers the gathered data by wireless communication utilizing IoT protocols. The collected data by IoT middleware has been capable of managing and affording users with information for energy use on the internet. The smart meter operates online where all the data has been attained in real-time. For easy integration with any tracking software solution, the meter possesses a multi-protocol link. Zigbee, 6LoWPAN, and Bluetooth have been permitted for this process. Wi-Fi has also been utilized for validating the ability of the smart meter to interact with IoT middleware. Lastly, the solution has been validated in real-world settings and is also used recently.

IoT in medical management

The influence of IoT on the medical industry has attained extensive attention in recent years. Digitalization has been rapidly occurring in hospitals. Numerous firms have been developing platforms to connect numerous devices in clinics. For instance, Philip's health suite (an open platform) permits medical devices for sharing data with the specific platform which could later process and evaluate these data which could then be generated by medical workers inclusive of nurses and physicians. This process assists the physicians in taking decisions. An eICU program has also been developed by Philips, which integrates audio technology with visual technology in addition to data visualization and predictive analytics. This lays a centrally observed intense care in clinics by use of connected devices which afford data in real-time [23]. Another research area in IoT in healthcare involves the networked data produced and retrieved from healthcare devices in serious care settings, analysis and observance of patients in the clinics from X-ray, MRI, and CT scanners and mammography with integrated EMR (Electronic Medical Records) with imaging results that could assist in fast medical decisions. Moreover, digital pathology represents a term utilized for explaining actionable information produced using AI (Artificial Intelligence) algorithms on diseased tissue images including tumours, other diseases, and wounds. Various primary MedTech companies like Philips have created products of digital pathology for the market. Likewise, other global organizations like Siemens possess products of digital pathology [24]. Another evolving sector where IoT has initiated to make an impact includes prosthetics and the implantation of medical devices like defibrillators, robotic surgeries, hip joints, etc. Measurement of heart rate, computation of intake or calorie burn, automatic patient monitoring, etc. includes a few tasks accomplished by the IoT devices integrated with healthcare sensors. IoT with fig-computing, mobile edge-computing, and cloud computing exists as promising technologies to build a digital, smart, and advanced medical management system. An enhanced block chain framework based on IoT has been suggested in the study [25] to access and maintain EMR with reliability, efficiency, transparency, and security. In this case, block chain resolves the privacy limitations of IoT through the use of cryptographic algorithms. Reliability issues have also been focussed through the use of tamper-resistant ledgers. Similarly, the research [26] has used SHA (Saskatchewan Health Authority) which includes

several medical areas as case-study. The concept of the study has been to execute IoT in SHA. It has been assumed that this will be sufficient in consolidating to assure the interoperability and interconnectivity among medical areas through network designs which will enable wide communication in a health area. It has been argued that using IoT will give huge merits like enhance workforce productivity, enhanced business models, and cost savings with enhanced cooperation with patients and medical practitioners in all the segments of medical delivery. The smart solution has also been accomplished by concentrating on certain medical services like cloud services, emergency services, operational services, and cancer-care services by IoT, particularly with WSNs and other devices through the full mesh-hierarchical network configuration.

IoT-wearable

IoT-based wearable technology has been associated with ubiquitous computing. It is a technology with smart devices and microcontrollers. The device could be worn on the human body as an accessory or an implant. Such wearable devices could perform numerous identical computing similar to laptops and mobile phones. Nevertheless, in certain conditions, wearable technology could perform better than handheld devices. For instance: smart-belt, smart-shoes, smart-ring, fitness trackers, smart jewellery, etc. Wearable devices based on IoT are not restricted to these instances alone. While wearable technology inclines to indicate the items that could be put on with ease and taken off with ease, there exist invasive types of concepts as in implanted device cases like smart tattoos or microchips. No matter if a device has been incorporated into a human body or is worn, the wearable device has intended to develop convenient, portable, handy, and constant free access for computers and electronics. The study [27] has presented a HAR (Human Activity Recognition) system relying on DL (Deep Learning) methods and a Wi-Fi sensor conceived to use the wearable and smart devices for recognizing the day-to-day activities of users prevailing within AAL (Ambient Assisted Living). Generally, the proposed model exploits neural networks and Wi-Fi connections to be utilized on the cloud to perform demand tasks and on embedding components or low-cost devices for regular activity recognition. By this, connection to cloud services has been vital only when any individual initiates to get monitored affording trivial training for creating an entire dataset to fit into the use case. The intention of the work has not been real-time, however, it exists as a personalized activity monitoring in the long-term for the activity accomplished during the day by old people to infer any unwanted behaviours often associated with emergency or unhealthy cases. Obtained outcomes have been positive in comparison with other research works. Furthermore, the study [28] has introduced a smartwatch and data pipeline based on the cloud to develop a user-friendly medicine intake observation system that could contribute for enhance medication adherence. The introduced smartwatch gathers sensor data through a gyroscope or accelerometer. With the suggested sensor data retrieval, preprocessing and ML algorithms, the research has accomplished a maximum F1-score of 0.977. Outcomes have revealed that spark-cluster with numerous storage, memory, and CPU could construct ML models quicker by the use of several computing resources simultaneously.

IoT in farming

IoT in farming utilizes drones, computer imaging, remote sensors, and robots integrated with persistent progress of analytical tools and ML to monitor the crops, surveying as well as field mapping with the provision of suitable data to the farmers for better management plans of a farm for saving money and time. Employing IoT in farming targets traditional farming functionalities to satisfy the enhancing demands with limited production losses. Accordingly, the research [29] has developed an algorithm based on image processing to detect and observe the infected fruits from cultivation to harvesting. To accomplish this, ANN (Artificial Neural Network) has been employed. Four tomato crop diseases have been chosen for the research. Two databases have been used for training infected images and execution of query images. Weight has been adjusted for training through the backpropagation concept. Empirical outcomes have presented the mapping and classification of respective image categories. Images have been categorized as texture, morphology, and colour. Practical execution of methodology has been accomplished using MATLAB. Morphology has afforded results at a rate of 93%. The suggested algorithm is better at determining the disease's spread. Similarly, the article [30] has executed services based on IoT for the farming sector. The main intention has been to gather data from several spots in farmland. This data later is accessed by farmers in a mobile application through a cloud platform. Data gets represented in graphical form. The mobile application also affords several beneficial services for farmers. Application users could also manage the fundamental functions of environmental, irrigation, fertilization, and soil data. These data have been automatically correlated with the invalid data filtered out from a view of evaluating the crop performance. Suggested application has also forecasted crops and recommended crops based on a specific farm. A farm could possess numerous crops in its fields. Thus, individual crops will possess varied parameters that have to be controlled. For this, a cluster has been needed that will gather data individually. To undertake this, nodes have been installed on several field areas relying on parameters. The individual node includes a sensor and raspberry pi connected with it. The sensors might be humidity sensors, soil moisture, or temperature sensor. As the soil moisture sensor has been analog, it needs an analog-to-digital converter. Data from the sensor remains in an analog form that has to be transmitted in digital format. Thus, raw data has been supplied to the analog-to-digital converter which gets converted to digital (in voltage value format). Based on this value, the percentage of soil moisture has been considered. Thus, through clustering technology, accurate decisions can be made by farmers about detecting the particular area in which soil moisture gets reduced, the particular period in which motor pumps can be turned on/off and device parameters to be managed. All this data transferred to the cloud has been stored in a cloud database. These data could be viewed by farmers after logging into their corresponding accounts. Data from the cloud has been afforded to the mobile application by which farmers could easily control several devices and maintain all the readings retrieved from sensors.

COMPARATIVE ANALYSIS – ADVANTAGES AND DISADVANTAGES

The reviewed articles have been comparatively evaluated to bring out their advantages and disadvantages. The tabular analysis is shown in Table 2.

Table 2. Tabular analysis – advantages and disadvantages

S.no	Reference	IoT applications	Objective	Outcome/ Advantages	Disa dvantages
1	[17]	Smart-city	An IoT model relying on fog-computing has been endorsed to create coordinated operations of the city through intelligent perception means	Minimize processing delay, and reduce running time and violation rate. Resource allocation maintains stability	Competition for several resources might possess a negative impact on resource allocation due to limited communication and storage resources
2	[19]	Smart home	A significant application of IoT in automating homes is emphasized in the study	The researcher has claimed that IoT manages home automation devices from any place throughout the globe by managing them from tablets, smartphones, and personal computers	IoT has been limited in privacy, confidentiality, and over-dependence on technology
3	[22]	Energy meters based on IoT	The study has aimed to design, construct, explore and validate the solution for a cheap smart meter to monitor energy consumption based on IoT	For easy integration with any tracking software solution, the meter possesses a multi-protocol link	Limited with respect to standardization of communication protocols, lack of plug & play support, and inefficiency in BD management.
4	[25]	Medical management	An enhanced block chain framework based on IoT has been suggested to access and maintain EMR with reliability, efficiency, transparency, and security	Block chain has resolved the privacy limitations of IoT through the use of cryptographic algorithms. Reliability issues have also been focussed on by considering the tamper-resistant ledgers	A highly compact system has to be considered in the future to alleviate the security issues in EMR
5	[27]	IoT wearables	The research has presented a HAR (Human Activity Recognition) system relying on DL (Deep Learning) methods and Wi-Fi sensors conceived to use wearable and smart devices for recognizing the day-to-day activities of users	Obtained results have been positive	Real-time execution has not been undertaken
6	[30]	Agriculture	The main intention has been to gather data from several spots in farmland based on IoT	Application users could also manage the fundamental functions of environmental, irrigation, fertilization, and soil data	Data has to be centralized in the future
7	[31]	Industry	The basic objective has to predict the motor vibration measurements	The working of system compared with other ML techniques has stated better results	A unified system for maintenance planning in industry has to be built

Continued table 1

S.no	Reference	IoT applications	Objective	Outcome/ Advantages	Disa dvantages
8	[32]	Industry	To develop an IoT architecture to detect motor faults	The results has projected better accuracy in monitoring induction machines using IoT system with ML algorithms	The study has to emphasize by applying the methodology in other machine types
9	[33]	Industry	The main objective of the study has to remove noise and preserving anomalies in IIoT data	The study has detected the noise in presence of significant anomalies and has distinguished the abnormal patterns and sensor noise caused by equipment failure	It is not completely automatic detection and temporary change in noise has resulted in sensor alteration

From comparative analysis, a few disadvantages faced by conventional works have been explored which include limitations in terms of privacy, confidentiality, over-dependence on technology, lack of real-time execution, data to be centralized, need of high compact system, and limited communication, lack of plug & play support, inefficiency in BD management and storage resources. Major Key challenges of IoT are discussed below,

MAJOR KEY ISSUES AND CHALLENGES OF IOT

IoT has interconnected several physical devices through the internet for exchanging data amongst them. Data is maintained in the cloud. Despite its extensive popularity, it is facing several issues as listed below [34]:

Regarding technological challenges, IoT lacks standards, and a deficiency in intelligent analysis, and connectivity.

Standards: IoT organizations lack in adopting a standard which is the reason for their deficiency in planning, implementing, and managing the IoT devices.

Deficiency in intelligent analysis: Sometimes the data gathered by the sensor might be inaccurate which might lead to wrong results.

Connectivity: With the increase in the evolution of IoT devices, connecting numerous devices have become a challenge.

Regarding societal challenges, IoT is encountering numerous issues to meet up with customer demands that change frequently. New devices also grow rapidly, hence, time is required. As the users have partial knowledge regarding IoT devices, they might get concerned when the interface seems to be complex which might lead to averting the product use. Inventing new IoT devices and integrating them with previous ones requires time and money.

IoT also faces challenges in design where battery life seems to be a limitation. Challenges are also involved in packing and including microchips with minimum power consumption and weight. Designers have to resolve the design timing issue and deliver the device to market at the correct time. In addition, IoT faces issues due to deployment concerning connectivity, data collection and processing, and capability cross-platform. In IoT, scalability has become another concern which is of 2 kinds-vertical and horizontal scalabilities. In this case, vertical

scalability indicates the removal or inclusion of computing-resources corresponding to the IoT node, while, horizontal scalability indicates the removal or inclusion of the IoT node. Though the study [35] has attempted to solve scalability issues of IoT using a cloud-based model, it still faces several challenges IoT nodes demanding enhancing services like functional scalability, data storage, privacy, security, etc. Moreover, IoT has lacked end-to-end security solutions and privacy standards which is a prevailing concern to deploy IoT. Deficiencies in encryption, scarce testing, and updating are a few instances of lack of security in IoT. All these challenges have to be solved for maintaining IoT devices reliable and secure.

COUNTERMEASURES FOR SECURITY ISSUES IN IOT

Few countermeasures exist using which IoT security challenges could be mitigated [36]. This includes data encryption, access control, certification, communication security, etc.

Data encryption strategies. Encryption involves the procedure of converting PT (Plaintext) into CT (Cipher text). The IoT network layer accepts the hop-by-hop encryption strategy for securing nodes at the network layer. In this way, information gets encrypted during transmission. However, it has to maintain PT in the individual node by encryption process and decryption process. On contrary, IoT's application layer accepts end-to-end encryption for the secure transfer of information from the sender to the receiver. By business needs, one could select any encryption approach. In addition, with security management and the exchange of keys, one could avoid attacks namely fabrication records, eavesdropping, etc.

CC (Cloud Computing). Huge data are stored in the cloud and its performance seems to be more with minimum cost. IoT could adopt CC for storing, processing, and gathering data from numerous sensor nodes that are also capable of affording 3rd party security for IoT systems.

Communication Security in IoT. IoT devices include small devices having low power that results in weak communication security. Hence, a secure and strong communication protocol is needed for accomplishing communication security.

Access Control and Certification. Through the use of PKI (Public Key Infrastructure), one could accomplish authentication with public key certification to preserve the confidentiality and authenticity of IoT. It also seems to be a secure manner of determining the parties involved in transferring information. Identifying parties could also be performed by a trusted 3rd party termed notarization. Besides, access control affords secure IoT through the limitation of device access and person or things that are not legal for IoT resource access. For correct, IoT access control, the system has to afford a certification system for security.

Recommendations

The efficient approach to secure IoT is to concentrate on fundamentals. IoT device manufacturers, architects, developers, application developers, service developers, and experience designers have to work collaboratively to bring security in the initial phases of designing and ensure that it seems to be consistent throughout the entire IoT phase. It is vital for individuals contributing to the development of IoT for including security features at the design stage of solution development for IoT. Efforts for preventing attacks involve designing security, embedding features of the firewall to integrate additional defence layers, affording encryption abili-

ties, and including capabilities of tamper detection. When manufacturers fail to completely test their IoT devices, safety and consumer trust might be at risk. Hence, it is significant to assure that security has a purpose, constructed in all the ecosystem aspects which are implementing specific IoT devices, services, or products. When constructing IoT products, the vendors must always apply optimal strategy and intend for integrity, availability, and confidentiality.

CONCLUSION

The study reviewed the potential applications of IoT from existing works that ranged from 2018 to 2022. It also discussed the IoT evolution, its concepts, architecture, and protocols. Additionally, the significance of IoT was highlighted. The advantages and disadvantages of different IoT applications (considered by conventional studies) were also discussed through tabular comparative analysis. Through this comparative assessment, a few issues in considering IoT was determined which comprised of limitations in terms of privacy, confidentiality, overdependence on technology, lack of real-time execution, data to be centralized, lack of plug & play support, inefficiency in BD management and storage resources, need of high compact system and limited communication. After this, the study summarized the major key challenges of IoT technological challenges, societal challenges, and design and deployment challenges. Issues due to scalability and security were also emphasized. Finally, the study provided countermeasures for resolving the security challenges of IoT with recommendations that will act as a guideline for researchers and IoT experts in resolving the unsolved gaps to attain a better vision in adopting IoT products with enhanced security.

REFERENCES

1. P. Balaganesh, M. Vasudevan, R. Rameswari, and N. Natarajan, “Recent Trends in IOT-Enabled Composter for Organic Wastes,” in *Sustainable Cities and Resilience*, ed: Springer, 2022, pp. 445–457.
2. P. Gokhale, O. Bhat, and S. Bhat, “Introduction to IOT,” *International Advanced Research Journal in Science, Engineering and Technology*, vol. 5, pp. 41–44, 2018.
3. N. Sharma, M. Shamkuwar, and I. Singh, “The history, present and future with IoT,” in *Internet of Things and Big Data Analytics for Smart Generation*, ed: Springer, 2019, pp. 27–51.
4. R. Román-Castro, J. López, and S. Gritzalis, “Evolution and trends in IoT security,” *Computer*, vol. 51, pp. 16–25, 2018.
5. B.K. Chae, “The evolution of the Internet of Things (IoT): A computational text analysis,” *Telecommunications Policy*, vol. 43, p. 101848, 2019.
6. J. Wang, M.K. Lim, C. Wang, and M.-L. Tseng, “The evolution of the Internet of Things (IoT) over the past 20 years,” *Computers & Industrial Engineering*, vol. 155, p. 107174, 2021.
7. R. Krishnamurthi, A. Kumar, D. Gopinathan, A. Nayyar, and B. Qureshi, “An overview of IoT sensor data processing, fusion, and analysis techniques,” *Sensors*, vol. 20, p. 6076, 2020.
8. R. Nawaratne, D. Alahakoon, D. De Silva, P. Chhetri, and N. Chilamkurti, “Self-evolving intelligent algorithms for facilitating data interoperability in IoT environments,” *Future Generation Computer Systems*, vol. 86, pp. 421–432, 2018.
9. S. Rathore, B.W. Kwon, and J.H. Park, “BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network,” *Journal of Network and Computer Applications*, vol. 143, pp. 167–177, 2019.
10. M. El-Hajj, A. Fadlallah, M. Chamoun, and A.J.S. Serhrouchni, “A survey of internet of things (IoT) authentication schemes,” *Sensors*, vol. 19, p. 1141, 2019.

11. O. Mnushka, *IOT architecture patterns and data protocols*, 2018.
12. A. Triantafyllou, P. Sarigiannidis, and T.D. Lagkas, "Network protocols, schemes, and mechanisms for internet of things (iot): Features, open challenges, and trends," *Wireless Communications and Mobile Computing*, vol. 2018, 2018. doi: 10.1155/2018/5349894.
13. S. Ketu, P.K. Mishra, "Enhanced Gaussian process regression-based forecasting model for COVID-19 outbreak and significance of IoT for its detection," *Applied Intelligence*, vol. 51, pp. 1492–1512, 2021.
14. M.A. Patil, A.C. Adamuthe, and A. Umbarkar, "Smartphone and IoT based system for integrated farm monitoring," in *Techno-Societal 2018*, ed: Springer, 2020, pp. 471–478.
15. J. Muangprathub, N. Boonnam, S. Kajornkasirat, N. Lekbangpong, A. Wanichsombat, and P. Nillaor, "IoT and agriculture data analysis for smart farm," *Computers and Electronics in Agriculture*, vol. 156, pp. 467–474, 2019.
16. G. Arun Francis, M. S. Manikandan, V. Sundar, and E. Gowtham, "Home Automation Using Iot," *Annals of the Romanian Society for Cell Biology*, pp. 9902–9908, 2021.
17. C. Zhang, "Design and application of fog computing and Internet of Things service platform for smart city," *Future Generation Computer Systems*, vol. 112, pp. 630–640, 2020.
18. R. Casado-Vara, A. Martin-del Rey, S. Affes, J. Prieto, and J. M. Corchado, "IoT network slicing on virtual layers of homogeneous data for improved algorithm operation in smart buildings," *Future Generation Computer Systems*, vol. 102, pp. 965–977, 2020.
19. T. Alsharari, S. Alresheedi, A. Fatani, and I. Maolood, "Significant role of internet of things (IoT) for designing smart home automation and privacy issues," *International Journal of Engineering & Technology*, vol. 9, pp. 515–519, 2020.
20. C. Stolojescu-Crisan, C. Crisan, and B.-P. Butunoi, "An IoT-based smart home automation system," *Sensors*, vol. 21, p. 3784, 2021.
21. W. Li, T. Logenthiran, V.-T. Phan, and W. L. Woo, "A novel smart energy theft system (SETS) for IoT-based smart home," *IEEE Internet of Things Journal*, vol. 6, pp. 5531–5539, 2019.
22. D.B. Avancini, J.J. Rodrigues, R.A. Rabêlo, A.K. Das, S. Kozlov, and P. Solic, "A snew IoT based smart energy meter for smart grids", *International Journal of Energy Reserch*, vol. 45, pp. 189–202, 2021.
23. V. Herasevich, S. Subramanian, "Tele-ICU technologies," *Critical Care Clinics*, vol. 35, pp. 427–438, 2019.
24. *Medtech and the Internet of Medical Things*. 2018. Available: https: //www2.deloitte.com/content/dam/Deloitte/global/Documents/Life-Sciences-Health-Care/gx-lshc-medtech-iomt-brochure.pdf
25. P.P. Ray, D. Dash, K. Salah, and N. Kumar, "Blockchain for IoT-based healthcare: background, consensus, platforms, and use cases," *IEEE Systems Journal*, vol. 15, pp. 85–94, 2020.
26. A. Onasanya, S. Lakkis, and M. Elshakankiri, "Implementing IoT/WSN based smart Saskatchewan healthcare system," *Wireless Networks*, vol. 25, pp. 3999–4020, 2019.
27. V. Bianchi, M. Bassoli, G. Lombardo, P. Fornacciari, M. Mordonini, and I. De Munari, "IoT wearable sensor and deep learning: An integrated approach for personalized human activity recognition in a smart home environment," *IEEE Internet of Things Journal*, vol. 6, pp. 8553–8562, 2019.
28. D. Fozoonmayeh et al., "A scalable smartwatch-based medication intake detection system using distributed machine learning," *Journal of Medical Systems*, vol. 44, pp. 1–14, 2020.
29. H. Pang, Z. Zheng, T. Zhen, and A. Sharma, "Smart farming: An approach for disease detection implementing IoT and image processing," *International Journal of Agricultural and Environmental Information Systems (IJAEIS)*, vol. 12, pp. 55–67, 2021.
30. A. Aher, J. Kasar, P. Ahuja, and V. Jadhav, "Smart agriculture using clustering and IOT," *International Research Journal of Engineering and Technology (IRJET)*, vol. 5, pp. 2395–0056, 2018.

31. G. Scalabrini Sampaio, A. R. de A. Vallim Filho, L. Santos da Silva, and L. Augusto da Silva, "Prediction of motor failure time using an artificial neural network," *Sensors*, vol. 19, p. 4342, 2019. doi: 10.3390/s19194342.
32. M.-Q. Tran, M. Elsisi, K. Mahmoud, M.-K. Liu, M. Lehtonen, and M.M. Darwish, "Experimental setup for online fault diagnosis of induction machines via promising IoT and machine learning: Towards industry 4.0 empowerment," *IEEE Access*, vol. 9, pp. 115429–115441, 2021.
33. Y. Liu, T. Dillon, W. Yu, W. Rahayu, and F. Mostafa, "Noise removal in the presence of significant anomalies for industrial IoT sensor data in manufacturing," *IEEE Internet of Things Journal*, vol. 7, pp. 7084–7096, 2020.
34. A. Čolaković, M. Hadžialić, "Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues," *Computer Networks*, vol. 144, pp. 17–39, 2018.
35. C. MacGillivray, D. Reinsel, and M. Shirer*, The growth in connected iot devices is expected to generate 79.4 zb of data in 2025, According to a New IDC Forecast*. Available: https://www.businesswire.com/news/home/20190618005012/en/The-Growth-in-Connected-IoT-Devices-is-Expected-to-Generate-79.4ZB-of-Data-in-2025-According-to-a-New-IDC-Forecast
36. .A. Abdul-Ghani, D. Konstantas, "A comprehensive study of security and privacy guidelines, threats, and countermeasures: An IoT perspective," *Journal of Sensor and Actuator Networks*, vol. 8, p. 22, 2019.

Received 05.12.2022

INFORMATION ON THE ARTICLE

Punitha Mahadevappa, ORCID: 0000-0003-3567-5537, JSS Academy of Technical Education, India

Rekha Puranic Math, ORCID: 0000-0003-0866-9502, JSS Academy of Technical Education, India, e-mail: rpmresearch22@gmail.com

ПОТЕНЦІЙНЕ ЗАСТОСУВАННЯ ІНТЕРНЕТУ РЕЧЕЙ: ВСЕБІЧНИЙ АНАЛІЗ / Пуніта Махадеваппа, Ріка Пуранік Мет

Анотація. Інтернет речей (IoT) — це об'єднання апаратного забезпечення, наприклад датчиків і трекерів, які відстежують кілька параметрів середовища або фізичних об'єктів, і програмного забезпечення, яке обробляє всі дані, зібрані апаратним забезпеченням. Очікується, що глобальний ринок IoT зросте на 53,8 мільярдів доларів США до 2025 року. Такий зростальний попит пояснюється його вродженою здатністю до автоматизації, яка спонукає кілька галузей до впровадження IoT. Крім того, мінімальна вартість пам'яті, оброблення та зберігання зі збільшенням великих даних (BD), хмари та поєднання промислових мереж та Інтернету є додатковими факторами для збільшення розвитку IoT. Завдяки цій важливості IoT застосовується у багатьох сферах, таких як управління медициною, сільське господарство, носимі технології, розумний лічильник енергії, розумне місто тощо. Застосування не обмежуються наведеними прикладами. Із урахуванням цього існуючі дослідження розглядали різні програми та намагалися їх реалізувати. Оскільки ці дослідження зосереджувалися на різних додатках, метою цього огляду є надання компіляції потенційних застосувань IoT за результатами звичайних досліджень у період з 2018 по 2022 рік. Дослідження також має на меті вивчити переваги та недоліки різних IoT додатків (розглянутих традиційними дослідженнями) за допомогою табличного аналізу. Крім того, у праці наголошується на основних ключових проблемах IoT включно з контрзаходами для вирішення проблем безпеки IoT. Дослідження дає рекомендації, які допоможуть усім експертам з Інтернету речей вивести на ринок продукти Інтернету речей із підвищеною безпекою.

Ключові слова: Інтернет речей, автоматизація, безпека, потенційні застосування.