International Journal of Religion
2024
Volume: 5| Number 2 | pp. 436 – 451
ISSN: 2633-352X (Print) | ISSN: 2633-3538 (Online)
ijor.co.uk
DOI: https://doi.org/10.61707/awg31130

Gravitating towards Internet of Things: Prospective Applications, Challenges, and Solutions of Using IoT

Zahidul Islam[1], Mohammad Rakibul Islam Bhuiyan[2], Tahmina Akter Poli[3], Rashed Hossain[4] and Lisa Mani[5]

Abstract

In the contemporary world, the Internet of Things has been utilized enormously in individual and business sectors. The purpose of the paper is to determine the prospective areas for utilizing IoT. Moreover, it also identifies the challenges and solutions of using IoT in different sectors. The study mostly employs qualitative methodologies, utilizing secondary data and articles to conduct this review article. The researcher employed the PRISMA 2020 platform to discern and select pertinent studies and reports from indexed publications such as Scopus, Web of Science, PubMed, DOAJ, and others. The study used primarily secondary methods of data collection because the idea of Internet of Things technology is still relatively new and not yet used by all sectors of Bangladesh's economy. The review paper might not include pertinent research that was published in other languages or in publications that were not indexed, which could potentially introduce a bias stemming from language and ordering. From the point of implication portion, IoT would be the driving force behind the development of future wireless sensor networks, which will feature enhanced connection, intelligence, and application diversity in different sectors.

Keywords: *Internet of Things, PRISMA-Based Systematic Review, Prospective Application, Challenges, Solutions*

INTRODUCTION

There is significant technological progress going forward concurrently with the beginning of human-machine interfaces, or HMIs, becoming increasingly popular in the context of Industry 4.0, the fourth industrial revolution (Mourtzis & Panopoulos, 2023). Some examples of these advancements include the Internet of Things (IoT), the Industrial Internet of Things (IIoT), hyper-automation, and distributed cloud computing, amongst others (Ashima et al., 2022). The approach of digital modeling has a favorable influence on the creative talents of the designer, which provides the opportunity for intelligent and compassionate machine integration (Kabanda, 2021).

IoT, which stands for the Internet of Things, has fundamentally altered the way in which we perceive and interact with the environment that surrounds us (Singh, 2023). Through the process of connecting a multitude of devices and objects to the internet, it establishes a massive and interconnected network of both digital and physical entities (Vermesan & Friess, 2022). This game-changing technology has not only remodeled entire industries but also made our day-to-day lives better, and it holds the prospect of having even more dramatic effects in the future (Hodgson et al., 2022). It is the Wireless Sensor Networks (WSNs) that are at the core of Internet of Things-based systems (Ali, 2021). These networks play an essential role in the implementation of important energy-saving strategies. However, because of the gadgets' quick development, there are now issues with energy usage throughout the information transmission process (Amin & Rahman, 2018). Increasing levels of communication and data interchange have resulted in increases in energy consumption and carbon emissions that are not conducive to long-term sustainability (Lili & Caiyun, 2021). In a variety of applications, including environmental control, agriculture, and border surveillance, sensor nodes are required to function well for extended periods of time (Ghamari et al., 2022). These periods might range anywhere from months to years, depending on the requirements of the application (Sussex & Grant, 2020).

[1] Senior Lecturer, School of Business, Uttara University, Dhaka, Bangladesh. Email: zahid@uttarauniversity.edu.bd
[2] Department of Management Information Systems, begum Rokeya University, Rangpur, Bangladesh. Email: rakib@mis.brur.ac.bd
[3] Joint Commissioner of Customs , National Board of Revenue: Dhaka, Bangladesh Email: mtahminapoli@gmail.com
[4] MBA Student, Accounting & Information Systems, University of Dhaka, Dhaka. Bangladesh. Email: rashedhbs@gmail.com
[5] Research Assistant, Department of Accounting & Information Systems, Begum Rokeya University, Rangpur, Rangpur 5004, Bangladesh. Email: lisamoni00@gmail.com

In the Internet of Things (IoT) ecosystem, real-time modules, such as sensors, are networked with one another to transport important data to centralized repositories (Sundas & Panda, 2021). Data is stored and accumulated in these repositories, which then make it readily available to users who have been authorized to access it (Dowaidar, 2021). Considering that the sheer number of communication devices involved in IoT-based networking systems is substantially greater than that of traditional wired or wireless systems (Pahuja & Kumar, 2023). It is fascinating to compare and contrast the two types of systems. Nevertheless, despite the huge volume of traffic generated by the Internet of Things (IoT), it is not significantly affecting the effectiveness of the network that is being used (Charyyev & Gunes, 2021). IoT devices are able to perceive and communicate data to their respective IoT servers, which is the reason for this phenomenon (Mazher, 2022). The network's overall efficiency is impacted by the data produced by a large number of objects, although this impact is often acceptable. Internet of Things networks are able to function without interruption and sustainably for extended periods of time, even when there is no intervention from humans (Chekati et al., 2020). One of the most attractive aspects of the Internet of Things is its capacity to operate independently, thereby ensuring the security and effectiveness of interconnected systems without the need for ongoing human supervision (Trivedi & Patel, 2022). Within the context of applications that require constant monitoring or control, this particular element is especially advantageous (Łuszczyńska, 2021).

Research Gap

The Internet of Things (IoT) is a swiftly progressing domain with a wide range of applications spanning multiple industries. There is a potential research gap in investigating the possible uses of IoT in various fields, including healthcare, smart cities, agriculture, manufacturing, transportation, and others (Mourtzis & Panopoulos, 2023). Examining the potential advantages, difficulties, and remedies unique to each application domain could yield interesting observations. There are numerous studies conducted on IoT from emerging technologies and diverse perspectives (Mourtzis & Panopoulos, 2023). No studies are conducted through a PRISMA-based systematic review of world-wide perspectives (Dowaidar, 2021). The fundamental research gap is using PRISMA 2020 to describe the potential usages, challenges, and solutions of utilizing IoT in the individual and business sectors.

Research Objective

Overall, this study offers professionals and scholars a comprehensive understanding of a highly promising development in the realm of new technology research, such as IoT (Vermesan & Friess, 2022). Researchers can obtain vital insights into optimizing the utilization of these tools for developing advanced IoT devices that can mimic human behavior by comprehending the internal mechanisms and possible applications of these technologies (Mourtzis & Panopoulos, 2023). The following objectives were established to conduct this review paper:

Assessing the potential applications of using emerging technologies, especially IoT,

Determining the challenges and optimal solutions to utilizing IoT in different sectors.

MATERIALS

In an intelligent Internet of Things transportation system, the endorsed individual is able to monitor the existing area and development of a vehicle (Thamaraimanalan et al., 2018). The Internet of Things has made it practical to amass sizable contemporary structures and applications, which has enabled this capability. The individual who has been confirmed is also able to forecast future traffic patterns in the zone and on the roads (Villiers, 2023). When we were in the beginning stages, we used the term Internet of Things to refer to one of the kinds of items that had RFID. In the past, the researchers have associated the phrase "Internet of Things" (IoT) with things like sensors, mobile phones, gadgets that use the Global Positioning System (GPS), and actuators (Shackelford, 2020). The assurance and organization of new developments in the Internet of Things are primarily dependent on the protection of data for the same reason that information security is important (Bolognini & Balboni, 2019). Therefore, the Internet of devices enables a variety of devices to be connected, monitored, and checked, which results in the accumulation of significant information as well as private data (Bell, 2021). In the Internet of Things (IoT) environment, security assurance is an extremely crucial concern

when compared to older frameworks. This is due to the relatively high number of assaults that are launched against IoT (Cheruvu et al., 2019).

The Internet of Things is being used on a daily basis in the medical and health care sectors, both by doctors and patients. For instance, electrocardiograms and ultrasounds are being used to monitor patients' health (Jaques, 2012). When it comes to the Internet of Things (IoT), Kaa is an open-source middleware platform that allows for the monitoring, collection, analysis, and monitoring of specific parts of communications between connected devices (Jasmin, 2023). It is feasible to build executioner applications for buying items surprisingly fast instead of weeks because of the way that Kaa gives different pluggable highlights. Out of the container, Kaa is viable with essentially any advanced purchaser item or chip, including shrewd TVs, innovative home apparatuses, air conditioning systems, wearables, and more limited-size PC sheets (Joshi & Solanki, 2022).

Savvy City is yet another remarkable application of the Internet of Things that generates interest among the general population. Sensitive reconnaissance, automated transportation, more intelligent energy management systems, water transportation, urban security, and ecological monitoring are all examples of applications that can be made possible through the use of the internet of things for urban communities that are technologically sophisticated (Udendhran & Balamurugan, 2020). The Internet of Things will solve severe problems that people living in urban neighborhoods face, including contamination, transportation congestion, and a lack of vitality supplies, among other problems (Omeke et al., 2022). Whenever a container has to be emptied, SmartBelly rubbish will send notifications to city authorities with the help of devices such as mobile phone communication-enabled garbage (Koley & Acharjya, 2022).

Digitalization

Digitalization is the process of converting various forms of information, such as pictures, text, data, sound, and speech, into a binary code. This code is then stored in a way that is ideal for transmission, as well as for computer processing and analysis (Sogam, 2023). The process of digitalization has a significant impact on various facets of life. The digital revolution is a prominent trend in the current era, resulting in the emergence of IoT-based companies that exclusively deal with digital data (Lin, 2023). Digitalization consolidates, evaluates, and disseminates vast quantities of data to prospective users. Modern digital technology and information systems produce immense quantities of data, which are then stored as Big Data (Blann, 2018). The process of digitalization and the utilization of Big Data can be employed to generate digital profiles of clients. Algorithms have the capability to combine consumers' transactional data with other sources, such as online behavior and digital data shared by users with other financial and non-financial businesses (Gürkan et al., 2022).

IoT

The Internet of Things (IoT) is a term that describes the process of linking physical objects to the internet (Herrero, 2022). This enables the devices to quickly gather, analyze, and share data with one another. There are a wide range of organizations that are reliant upon the IoT, including transportation, medical care, farming, and savvy urban communities (Drinkwater & Kai, 2018). As a consequence, it leads to an increase in productivity, a broader capacity to make well-informed decisions, and a larger degree of automation in processes and oversight, with the end result being a dramatic transformation of our living and working situations (Lazarus et al., 2020). Nonetheless, regardless of the way that the IoT contains a wide assortment of conceivable outcomes that are both mind-boggling and huge, the development of this innovation and its application are not without their difficulties (Yang et al., 2023).

Worldwide Scenario of Internet of Things

The size of the global Internet of Things (IoT) market is anticipated to reach $806.3 billion by the year 2027 (Figure 1), expanding at a compound annual growth rate (CAGR) of 17.6% during the period where the prediction is being made (Focus on Catalysts, 2021). In the Internet of Things (IoT) innovation, there are brilliant gadgets that are associated with the web and can get, break down, and cycle the information that is accumulated from their environmental elements (Arora & Baliyan, 2019). These devices are equipped with embedded systems that include sensors, processors, and communication hardware. IoT technology is being

gradually adopted by organizations across a wide variety of industries in order to improve their organizational performance and gain a deeper understanding of their customers (Santos, 2022). This allows them to provide superior customer service, enhance their decision-making processes, and increase the value of their company (Nasution et al., 2022).

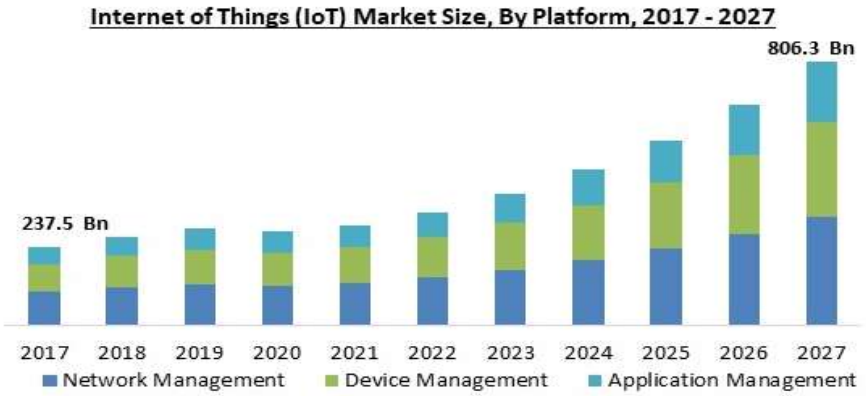

Figure 1: Present Worldwide Scenario of IOT Market Size

Source: kbvresearch.com

Applications of IoT

Smart Home Automation

A network that enables the linking of devices and the remote monitoring of those devices through the use of the Internet is referred to as the Internet of Things (IoT). The IoT is a concept that has witnessed significant expansion in recent years and is currently being applied in a variety of fields, including smart homes, telemedicine, and industrial settings, among others (Auwal, 2023). The introduction of wireless sensor network technologies into the IoT makes it possible for a global interconnection of intelligent devices with improved features. One of the fundamental technologies that underpins smart homes is a wireless home automation network (Zhang, 2021). It is made up of sensors and actuators that are connected to a network and collaborate with one another to share resources. A "smart home" is an essential component of the IoT concept, which is aimed at incorporating home automation into the existing infrastructure (Domb, 2019). The inclusion of Internet connectivity into the devices and appliances that are found within a household gives users the ability to remotely monitor and control those items and devices. Intelligent irrigation systems that can be programmed to start at specific times and follow a customized monthly schedule in order to reduce water waste are among the features that are included in this category (Aleshkin & Lesko, 2019). Other features include light switches that can be activated by a smartphone or voice, and thermostats that can automatically control the temperature inside the home and provide reports on the amount of energy (Petrovski & Seviour, 2018). In recent years, there has been a significant increase in the number of people interested in developing smart home solutions. The illustration in Figure 1 depicts a smart home that makes use of a number of IoT-connected utilities.

Figure 2: Smart Home Automation

Source: Author Work

Academic researchers have proposed numerous home automation solutions related to the IoT in the past decade. Various technologies have been utilized in wireless home automation systems, each with its own advantages and disadvantages. The IoT is widely utilized in smart home automation. Home automation is the interconnection of several gadgets and appliances in a household with a centralized network, allowing for remote control, automation, and seamless integration (Moreno et al., 2019). This integration enhances comfort, convenience, efficiency, and security. Below are several crucial elements and advantages of smart home automation (Jatolia & Patil, 2022).

IoT-empowered smart home arrangements let property holders remotely oversee and robotize a great many gadgets, for example, lighting, indoor regulators, entryway locks, surveillance cameras, and theater setups (Desai & Modi, 2019). These systems offer heightened security by means of remote monitoring, motion detection, entrance sensors, and video surveillance. Additionally, they enhance energy efficiency by adjusting energy usage according to user preferences and environmental factors (Marabissi et al., 2021). IoT solutions facilitate the smooth integration and compatibility of devices, resulting in a cohesive user experience. They streamline everyday routines by simplifying tasks like scheduling appliances and managing lighting. Remote monitoring and management enable homeowners to remotely monitor security, energy usage, and gadget performance (Khanna, 2022). Furthermore, smart home automation systems have the capability to acquire user preferences and adjust accordingly to meet their requirements (Tai et al., 2022).

Industrial Internet of Things (IIoT)

The IoT is widely employed in several industries to optimize processes, enhance efficiency, and improve safety. IIoT applications encompass many functions, such as remote monitoring and control of machinery, predictive maintenance, asset tracking, optimization of the supply chain, and real-time data analytics (Robertson, 2020). The IIoT is the implementation of IoT technology and principles in industrial environments. IIoT refers to the process of linking industrial devices, equipment, sensors, and systems to a network infrastructure (Gupta, 2021). This connection allows for the gathering, analysis, and automation of data, leading to enhanced operational efficiency, productivity, and decision-making capabilities (Ragazou et al., 2023). Below are a few crucial elements and advantages of IIoT:

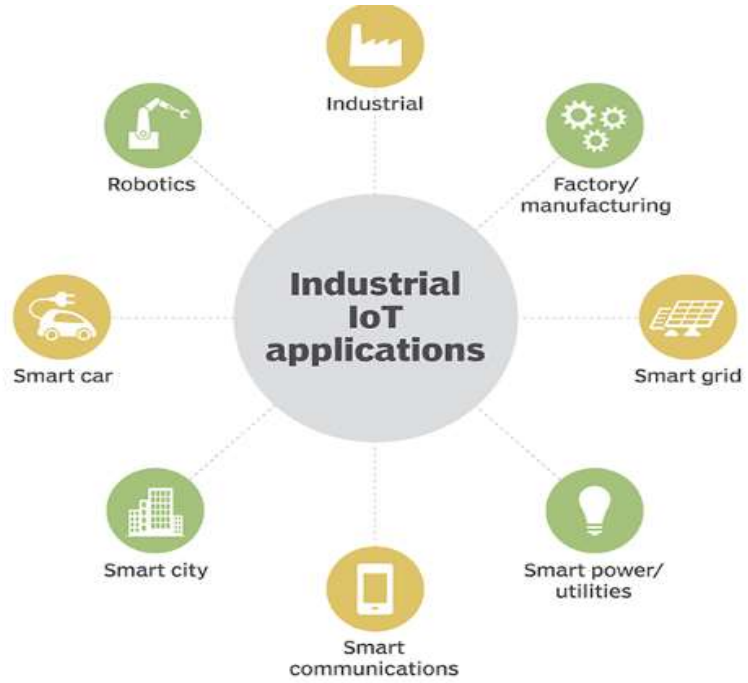

Figure 3: Industrial IoT Applications

Source: Author Work

IoT-enabled smart home systems allow homeowners to remotely control and automate a range of devices, including thermostats, lighting, door locks, security cameras, and entertainment-related systems (Figure 3. These systems offer improved security, energy efficiency, and seamless integration and compatibility between devices and platforms (Ragazou et al., 2023). Smart devices streamline everyday tasks, offer remote surveillance and control, and have the ability to acquire human preferences through machine learning. The use of IIoT allows for the immediate monitoring of industrial equipment and processes, which in turn enables the prediction of maintenance needs and enhances operational efficiency (Cakir, 2020; Guvenc & Mistiko, 2021). It can improve supply chain management by offering immediate visibility and monitoring of goods and commodities. The implementation of IIoT technology enhances worker safety through the continuous monitoring of environmental conditions and the provision of immediate notifications (Viehmann et al., 2022). The utilization of data analytics and insights derived from the IIoT can result in enhancements in quality control, production planning, and resource allocation (Figure 3. IIoT solutions have the capability to seamlessly interact with pre-existing systems, hence improving the exchange of data, interoperability, and coordination (Yang & Shami, 2023). They are specifically engineered to have the capability to adapt and expand, effectively meeting the changing requirements of industrial settings (Figure 3. Through the utilization of IoT technology in industrial environments, firms can achieve heightened levels of efficiency, production, and competitiveness (Fan & Du, 2023).

Healthcare and Remote Patient Monitoring

IoT devices can be utilized for the purpose of remotely monitoring patients, gathering essential health indicators, and transferring the data to healthcare providers in order to facilitate prompt intervention and individualized medical attention (Chidambaram, 2023). It facilitates the ongoing surveillance of patients with chronic ailments, elderly folks, and individuals in the process of recuperating following surgical procedures (Witwer et al., 2019). The IoT has achieved substantial advancements in healthcare and remote patient monitoring (RPM), leading to a transformative impact on patient care and enhancing health outcomes. The following are the essential elements and advantages of IoT in healthcare and remote patient monitoring (Table 1):

Table 1: IoT Applications in Healthcare Industry

Focus Area	Application
Disease management system to improve reliability	A guide for IoT healthcare service providers
Healthcare monitoring for chronic diseases like depression and diabetes	Battery energy efficiency approach using a machine learning technique
Healthcare monitoring system which uses low-cost sensors and ensures a lower energy consumption	New architecture and paradigm of monitoring
Mobile medical home monitoring system to improve the rapidity of factor measurements and ensure a low energy consumption	A new paradigm for mobile medical home monitoring
Adaptive security management based on metrics to enhance security	Adaptive security management standard
Synthesis method for e-health to ensure high availability	A new structure for e-health
IEEE 802.15.4 transceiver with a low error rate and a higher probability	Framework
An efficient protocol to counter PUEA attacks	Algorithm and structure protocol

Source: Author Work

The utilization of IoT technology enables healthcare providers to remotely check the health state of patients through remote patient monitoring (Table 1. This technique is especially beneficial for the management of long-standing illnesses such as diabetes, cardiovascular disease, and respiratory problems (Zamanifar, 2021). The utilization of IoT devices empowers patients to actively participate in their healthcare, thereby promoting healthier behaviors. Automated warnings and notifications can be activated, enabling healthcare providers to swiftly intervene. IoT data analytics can detect recurring trends in patient health data, facilitating early intervention and diminishing healthcare expenses (Jayashankara et al., 2021). The IoT likewise empowers far-off discussions and telemedicine administrations, empowering patients to speak with medical care experts through video conferencing or virtual stages (Table 1. The implementation of IoT can optimize the coordination of care across various healthcare facilities, minimizing the repetition of tests and enhancing the smoothness of care transitions (Liau & Ho, 2019). Additionally, it holds significant worth in the realm of aged care and the concept of aging in place, as it fosters self-sufficiency and ensures the well-being of individuals. In outline, the execution of IoT in medical services has the ability to alter the arrangement of medical care administrations by working with customized, proactive, and patient-centered care (Jolles & Thomas, 2018).

Smart Cities

The term "smart city" refers to a metropolitan area that collects data through the utilization of a variety of modern systems and sensors. With the goal of enhancing the effectiveness of municipal operations and services, the notion of a smart city merges information and communication technology with a wide variety of physical items that are connected to IoT networks (Meah & Hossain, 2023). The growing demand for intelligent living, which has become a popular trend, is primarily driving the market's increased prominence of the concept of smart cities. Smart living encompasses technological breakthroughs that significantly influence individuals' lives, empowering them to adopt a novel lifestyle. Smart city innovations promote the adoption of cutting-edge

technologies, including IoT, AI, big data, data analytics, and cloud storage technologies. These technologies are utilized to gather and analyze data, enabling effective management of assets, services, and resources. Smart cities are metropolitan regions that are meticulously planned to improve sustainable economic growth and quality of life. This is achieved by advancements in several sectors, such as the economy, technology, environment, people, mobility, and government (Bhuiyan et al., 2024). The main objective of smart city initiatives is to enhance energy efficiency and decrease reliance on non-renewable fuel sources. Smart cities provide advanced public safety and security measures by promptly identifying and addressing issues at an early stage. The key advocates of smart city development encompass the existence of strong sustainable property, infrastructure, intelligent transportation, cutting-edge communications, citizen safety, and enhanced market feasibility (Bhuiyan et al., 2023). Smart cities are designed to incorporate several elements, such as intelligent transportation, smart housing, smart buildings, security and sustainability, and energy management. These features aim to provide optimal development options for authorities and decision-makers.

Figure 4: IoT application in Smart City

Source: Author Work

The implementation of IoT technology enables healthcare providers to remotely check the health status of patients through remote patient monitoring. This technique is especially beneficial for the management of chronic illnesses such as diabetes, cardiovascular disease, and respiratory problems (Bhuiyan et al., 2023). The utilization of IoT devices enables patients to actively participate in managing their healthcare, hence encouraging the adoption of better practices (Figure 4. Automated warnings and notifications can be activated, enabling healthcare providers to swiftly intervene. IoT data analytics can detect recurring trends in patient health data, facilitating early intervention and diminishing healthcare expenses (Bhuiyan, 2017). The IoT additionally empowers far-off interviews and telemedicine administrations, empowering patients to speak with medical care experts through video conferencing or virtual stages. The implementation of IoT can optimize the coordination of care across various healthcare facilities, minimizing the repetition of tests and enhancing the smoothness of care transitions (Figure 4. Furthermore, it is highly beneficial for providing care to the elderly and facilitating the process of aging in one's own home, thereby encouraging self-sufficiency and ensuring safety. In summary, the execution of IoT in medical care has the ability to upset the arrangement of medical service administrations by working with customized, precautionary, and patient-centered care (Fan & Du, 2023).

METHODOLOGY

This study primarily focuses on the application of qualitative techniques. The data sources employed in this study predominantly comprise secondary sources, encompassing various scholarly journals, papers, televised

news broadcasts, and online platforms (Khanom et al., 2022). The present study aims to uncover the crucial criteria required for the development of IoT applications that are efficient and have a significant impact in the setting of a developing economy such as Bangladesh. Furthermore, it encompasses the difficulties and possible remedies of implementing IoT in many domains (Fan & Du, 2023).

The search was conducted using global databases such as Science Direct, Scopus, Web of Sciences, PubMed, and DOAJ, following the PRISMA statement of 2020. PRISMA is a standardized collection of essential elements for documenting findings in systematic reviews and meta-analyses based on solid evidence (Molla et al., 2023). PRISMA primarily emphasizes the reporting of reviews that assess randomized trials. However, it can also serve as a framework for reporting systematic reviews of other forms of research, especially evaluations of therapies. It is important to provide a thorough and comprehensive account of the techniques and outcomes of systematic reviews so that consumers can evaluate the reliability and relevance of the review's conclusions (Molla et al., 2023).

The research approach involved the use of certain phrases, such as IoT, characteristics, possible areas, and challenges, that are relevant to the main purpose of the investigation in figure 5. Any records that do not match the chosen keywords or study subjects are excluded (Molla et al., 2023). Additional factors that should be considered when determining whether to reject publications and reports include insufficient data availability, papers written in multiple languages, varied outcomes, and disconnected impacts and findings (Fan & Du, 2023). The researchers discovered an additional 140 papers and 10 reports during the examination, as shown in Figure 5.

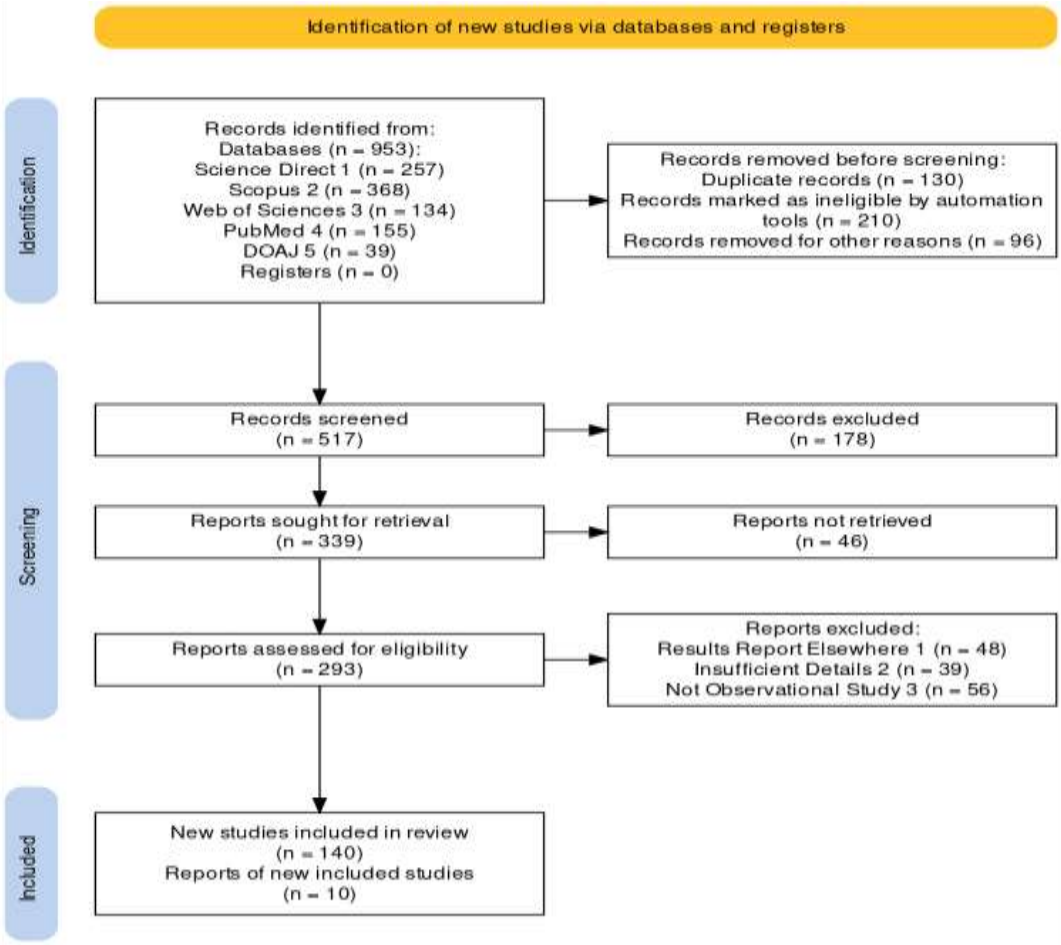

Figure 5: Flow Diagram of PRISMA 2020

Source: (Haddaway et al., 2022) [Access on December 24, 2023]

RESULTS AND DISCUSSION

Challenges of Using IoT

IoT presents various issues that should be appropriately addressed, notwithstanding the way that it achieves various advantages. There have been critical worries raised over administration, protection, and security because of the quick development of innovation and the explosion in the quantity of gadgets that are associated with each other. As a result, large amounts of data are gathered, processed, and transmitted by Internet of Things devices as a result. This information can range from individual data, for example, wellbeing records from brilliant wearables to essential business information from modern hardware. They are habitually of a delicate sort (Mani, 2019). Due to the tremendous volume and assortment of information that these gadgets produce, the board presents various significant issues. The interaction involves not just the stockpiling and handling of this information, but also the ensuring of its legitimacy, trustworthiness, and accessibility consistently.

The growing amount of personal data that Internet of Things devices are gathering and transmitting also raises privacy concerns. In reality, as we know it, where information has turned into a significant product, it is extremely vital to safeguard people's very own data appropriately (Bhuiyan, 2019). However, the utilization of the Internet of Things necessitates the continuous generation and transmission of data from a variety of areas of a user's life, which presents the possibility of users being subjected to privacy violations. IoT is also confronted with one of the most serious problems, which is security (Bhuiyan et al., 2024). Internet of Things devices are naturally susceptible to cyberattacks due to the fact that they are interconnected at their core (Fan & Du, 2023). To gain access to the organization and compromise other associated gadgets, hackers can take advantage of a device's security flaws in order to acquire access to the network. The implications of such breaches can be catastrophic, particularly in applications that are considered to be of crucial importance, such as healthcare or infrastructure (Bhuiyan et al., 2023). Therefore, it is necessary to address these issues by developing solutions that are both strong and inventive. These solutions should be able to protect the data, bring about an increase in privacy, and guarantee the safety of the IoT ecosystem. Because of this, blockchain technology is becoming increasingly important.

Table 2: Challenges of Using IoT

Challenges Issues	Explanation	Source
Object Identification	The abundance of devices makes validation in IoT a prominent concern. Verifying each and every device is not a task that can be completed by a single individual. Due to the rapid computational capabilities and energy efficiency of private key cryptography, a few security strategies have been recommended.	(Kollolu, 2020)
Data Management	The noticeable presence of billions of gadgets and their transmission can be seen as a key worry in the IoT. As indicated by projections, constantly 2020, in excess of 50 billion gadgets will be associated with the internet. Despite the implementation of IPv6, managing and transmitting gadgets will still be inconvenient. There are ways that can be employed to ensure clear and unmistakable verification of the objects in the Internet of Things (IoT). Examples of this include bar code identification and vision-based product recognition. RFID and NFC technologies are employed for distinct applications.	(Yang et al., 2023)
Authentication	The proliferation of devices in IoT makes verification the most prominent challenge. Verifying each and every contraption requires a collective effort, rather than being a task that can be completed by a single individual. Given the factors of fast computation and energy efficiency, several security methods have been suggested for the consideration of private key cryptographic individuals.	(Ragazou et al., 2023)
Heterogeneity	The heterogeneity of devices is the most serious security concern in the Internet of Things. Due to the fact that every category of device has its own specific security requirements, it is difficult to implement a single solution. This heterogeneity can have an effect on a variety of factors, including combination problems, security, and differentiating proof, which makes it difficult to govern and monitor.	(Kollolu, 2020)
Bulk Data	Data is the fundamental element in the Internet of Things. The Internet of Things (IoT) associates different machines to cloud server ranches, where all devices are connected to cloud models and store and recover tremendous measures of data and information in cloud server farms. Managing scattered data centres can be challenging, particularly when it comes to maintaining and securing essential and private information stored within them.	(Ragazou et al., 2023)
Encryption and Data Privacy	Sensor gadgets independently identify or gauge information and communicate it to the information taking care of unit through the transmission structure. Data encryption is necessary for sensor devices in order to safeguard data at the data processing unit. Multiple internet-enabled devices exist. Determining the presence of an illegal device that intercepts critical data	(Yang et al., 2023)

	during an internet exchange can be challenging. The primary obstacle faced by security measures is the preservation of secrecy.	
Internet Connection	The Trap of Things interfaces different savvy gadgets through the Web, empowering brought together checking and control of interconnected gear. In order for the Internet of Things to function, it relies on reliable web services. If any issues arise, they must be promptly resolved to prevent more complications in the system without the assistance of responsive devices.	(Aleshkin & Lesko, 2019)
Sharing of Data	The sharing of data between IoT devices and entities raises privacy concerns. Third-party entities may access user data without consent. IoT devices must restrict data sharing and provide consumers control over it to solve this problem. Companies should have clear data sharing procedures and get user agreement before sharing personal data.	(Nandalal & Anand Kumar, 2021)
Collection of Data	A significant protection issue related with the IoT is the broad gathering of information by different gadgets. The data may encompass personal details, like name, address, and payment card information, as well as behavioral data like location, browsing history, and search queries. In order to safeguard privacy, IoT devices should exclusively gather data that is essential for their designated purpose. Organizations should additionally demonstrate transparency regarding the data they gather and the intended purposes for its utilization.	(Nandalal & Anand Kumar, 2021)
Transparency	Ensuring privacy in the Internet of Things (IoT) relies heavily on the principle of transparency. Organizations must to exhibit transparency regarding the data they gather, the intended purposes for its utilization, and the entities with whom it will be shared. IoT devices should be designed to offer users unambiguous and succinct information regarding data collection, utilization, and dissemination.	(Meah & Hossain, 2023; Ragazou et al., 2023)
Control of End User	Exerting control over user data is a crucial element of maintaining privacy in the Internet of Things (IoT). Users should possess authority over the info amassed by IoT gadgets, encompassing the capability to eradicate or alter their data. IoT devices should additionally furnish users with unambiguous and succinct information regarding the collection, utilization, and dissemination of their data.	(Yang et al., 2023)

Source: Author's Work

Possible Solutions of IoT

Due to the interconnected nature of devices and the possible consequences that could result from security breaches, the Internet of Things (IoT) is a significant necessity for security. For the purpose of protecting Internet of Things devices, networks, and data from unauthorized access, data breaches, and other security threats, it is essential to implement these security standards through implementation. An approach to security that is both comprehensive and layered is required in order to address the ever-changing threat landscape and to keep people's faith in Internet of Things (IoT) systems. Internet of Things (IoT) security requirements include the following:

Device Authentication: IoT gadgets should be serious areas of strength for incorporating methods to ensure that the main approved gadgets might establish an association with the organization. This may encompass secure boot procedures, distinctive device identifiers, and secure communication protocols for verifying the authenticity of the device. For secure association, IoT gadgets should utilize strong correspondence conventions like Vehicle Layer Security (TLS) or Datagram Transport Layer Security (DTLS). These protocols guarantee the confidentiality, integrity, and authenticity of data sent between devices and the IoT infrastructure. Encryption and digital signatures are essential for safeguarding data during transmission.

Data Encryption: It is imperative to encrypt sensitive data obtained by IoT devices, including personal information and health data, both when it is being transmitted and when it is being stored. Data should be safeguarded from illegal access or interception by implementing robust encryption techniques.

Access Control: It is necessary to build access control techniques in order to limit illegal access to IoT devices, networks, and data. Enforcing access limits requires the implementation of role-based access control (RBAC), robust passwords, multi-factor authentication, and user privilege management (Akter et al., 2023). IoT devices must possess the means to receive and implement security updates and fixes in order to resolve vulnerabilities. Regular updates to firmware and software are essential for safeguarding devices against known security vulnerabilities and maintaining their long-term security (Bhuiyan, 2023).

Secure Storage: IoT gadgets have the ability to store secret information locally. It is crucial to guarantee that data stored on devices is sufficiently safeguarded using encryption and access control techniques. It is essential to implement physical security measures to deter unauthorized individuals from gaining physical access to equipment. IoT systems should possess strong monitoring capabilities to identify security issues and

abnormalities in a reliable manner. Using IDS, security occasion logging, and ongoing checking empowers the opportune distinguishing proof and reaction to potential security dangers.

Privacy Protection: IoT devices frequently gather and analyze personal data. To ensure compliance with data protection rules and uphold user privacy, it is imperative to include privacy protection mechanisms such as data anonymization, consent management, and privacy by design principles. Robust security measures should be implemented in the backend infrastructure that supports IoT systems, including cloud platforms and data centers (Akter et al., 2023). This includes the implementation of access controls, encryption techniques, periodic security audits, and intrusion prevention systems in order to protect data and deter unlawful access. IoT devices and systems must undergo comprehensive security testing and validation prior to deployment (Bhuiyan et al., 2023). Conducting autonomous security evaluations, performing penetration testing, and adhering to established security standards in the market will guarantee the security and resilience of IoT systems against potential assaults (Meah & Hossain, 2023).

CONCLUSION

The process of digitalization has become an essential component of contemporary human existence, influencing all facets of our everyday endeavors (Bhuiyan et al., 2023). In the 21st century, our dependence on advanced innovations for correspondence, work, medical services, schooling, and diversion is growing. In this digital age, technology has become more than simply a tool; it is now an essential element of our civilization, enabling unparalleled levels of accommodation, effectiveness, and worldwide interconnectedness (Islam & Bhuiyan, 2022). Out of this large number of innovations, the IoT has emerged as a groundbreaking power. The IoT is vital in various enterprises like transportation, medical services, horticulture, and brilliant urban communities (Bhuiyan et al., 2023). It results in increased productivity, an expanded ability to make informed choices, and a greater degree of automated processes and oversight, significantly reshaping our living and working conditions. Although the IoT encompasses a complex and extensive range of possibilities, the wider implementation and growth of this technology are not without difficulties (Akter et al., 2023). The most important challenges are mostly concerned with security, privacy, and data integrity. With the proliferation of IoT devices, the volume of data generated experiences exponential growth. Nevertheless, these gadgets frequently possess insufficient processing capabilities and are thus susceptible to a wide range of cyber assaults. Moreover, the widespread adoption of IoT also raises concerns surrounding privacy (Molla et al., 2023). Due to the extensive collection, processing, and storage of personal data by IoT devices, concerns are increasing over the abuse and unauthorized access to data.

LIMITATIONS OF THE STUDY

This research is exhaustive, yet it does have several shortcomings that need to be addressed. To begin, because the PRISMA-based approach is a powerful tool for topic modeling, it is possible that it does not fully differentiate between subjects. This is especially true in situations where the topics are closely related to one another or overlap. It is plausible that this will bring about an absence of accuracy in the recognizable proof of subjects. In the subsequent spot, our survey was restricted to exploring articles written in the English language that were recorded by the most prestigious data sets. As a consequence of this, the review might not include pertinent research that was published in other languages or in publications that were not indexed, which could potentially introduce a bias stemming from language and ordering. Furthermore, the time span of the study only runs up until the beginning of 2023, which means that it is possible that the most recent events and trends will not be covered. In conclusion, due to the rapid pace of development of Internet of Things technologies, it is possible that certain emergent subjects and unique applications have not been fully incorporated into the review that is now being presented. Because of this, there is a requirement for ongoing evaluation and revision of the information.

FUTURE SCOPE OF THE STUDY

In future, remote sensor networks that depend on the IoT will introduce an abundance of choices. The possibilities are without limit, ranging from the implementation of cutting-edge networks such as 5G to the incorporation of artificial intelligence, blockchain technology, and quantum computing. IoT-based wireless

sensor networks will alter industries, improve human-machine interaction, and pave the way for a future that is more connected and sustainable as technology continues to move toward its full potential. The Internet of Things will be the driving force behind the development of future wireless sensor networks, which will feature enhanced connection, intelligence, and application diversity. These networks will have a tremendous impact on the manner in which we engage with our surroundings, the businesses we run, and our personal lives. As the technology continues to advance, we may anticipate even more revolutionary solutions and paradigm-shifting shifts in the landscape of the IoT.

CONFLICT OF INTEREST

There is no conflict of interest among the authors in conducting and publishing this research paper. No funding has been received to conduct the study. Authors have not any potential conflict of interest to publish it.

DECLARATION OF GENERATIVE AI

For conducting this research, there is no usages of AI for writing. Authors have agreed to this statement.

ACKNOWLEDGEMENT

The researchers would like to acknowledge Dr. Md. Rakibul Hoque, Professor in the Management Information Systems department at the University of Dhaka, Bangladesh, for his invaluable help in this work. All authors have contributed equivalent contributions to the implementation of this research study.

REFERENCES

Akter, M. S., Bhuiyan, M. R. I., Poli, T. A., & Hossain, R. (2023). Web-based Banking Services on E-Customer Satisfaction in Private Banking Sectors: A Cross-Sectional Study in Developing Economy. Migration Letters, 20(S3), 894-911. https://doi.org/10.59670/ml.v20iS3.3976

Akter, M. S., Bhuiyan, M. R. I., Tabassum, S., Alam, S. A., Milon, M. N. U., & Hoque, M. R. (2023). Factors Affecting Continuance Intention to Use E-wallet among University Students in Bangladesh. https://doi.org/10.14445/22315381/IJETT-V71I6P228

Aleshkin, A., & Lesko, S. (2019). Predicting the growth of total number of users, devices and epidemics of malware in internet based on analysis of statistics with the detection of near-periodic growth features. 2019 XXI International Conference Complex Systems: Control and Modeling Problems (CSCMP). https://doi.org/10.1109/cscmp45713.2019.8976674

Ali, I. (2021). Data collection in studies on Internet of things (IoT), wireless sensor networks (WSNs), and sensor cloud (SC): Similarities and differences. https://doi.org/10.36227/techrxiv.14039486.v1

Amin, S. B., & Rahman, S. (2018). LNG and LPG market development in Bangladesh. Energy Resources in Bangladesh, 67-71. https://doi.org/10.1007/978-3-030-02919-7_13

Arora, S., & Baliyan, N. (2019). Extraction and analysis of information in news domain using Semantic Web. 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU). https://doi.org/10.1109/iot-siu.2019.8777502

Ashima, R., Haleem, A., Javaid, M., & Rab, S. (2022). Understanding the role and capabilities of Internet of Things-enabled Additive Manufacturing through its application areas. Advanced Industrial and Engineering Polymer Research, 5(3), 137-142.

Auwal, A. M. (2023). IoT integration in telemedicine: Investigating the role of Internet of things devices in facilitating remote patient monitoring and data transmission. https://doi.org/10.21203/rs.3.rs-3419693/v1

Bell, C. (2021). Project 4: Using MySQL to store data. Windows 10 for the Internet of Things, 455-493. https://doi.org/10.1007/978-1-4842-6609-0_13

Bhuiyan, M. R. I. (2017). UNDP-a2i: Citizens' Awareness Survey on E-Service and Service Simplification through the Digital Innovation Fair. Available at SSRN 4341799. https://dx.doi.org/10.2139/ssrn.4341799

Bhuiyan, M. R. I. (2019). An Analysis of Non-Performing Loan of Janata Bank from the Perspective of Bangladesh. Available at SSRN 4341827. https://dx.doi.org/10.2139/ssrn.4341827

Bhuiyan, M. R. I. (2019). An Analysis of Non-Performing Loan of Janata Bank from the Perspective of Bangladesh. Available at SSRN 4341827. https://dx.doi.org/10.2139/ssrn.4341827

Bhuiyan, M. R. I. (2023). The Challenges and Opportunities of Post-COVID Situation for Small and Medium Enterprises (SMEs) in Bangladesh. PMIS Review, 2(1), 141-159.

Bhuiyan, M. R. I., Islam, M. T., Alam, S. A., & Sumon, N. S. (2023). Identifying Passengers Satisfaction in Transportation Quality: An Empirical Study in Bangladesh. PMIS Review, 2(1), 27-46.

Bhuiyan, M. R. I., Uddin, K. S., & Milon, M. N. U. (2023). Prospective Areas of Digital Economy: An Empirical Study in Bangladesh. doi:10.20944/preprints202307.1652.v1

Bhuiyan, M. R. I., Uddin, K. S., & Milon, M. N. U. (2023). Prospective Areas of Digital Economy in the Context of ICT Usages: An Empirical Study in Bangladesh. FinTech, 2(3), 641-656. https://doi.org/10.3390/fintech2030035

Blann, A. D. (2018). Handling quantities: Mass, volume, and concentration. Data Handling and Analysis. https://doi.org/10.1093/hesc/9780198812210.003.0002

Bolognini, L., & Balboni, P. (2019). IoT and cloud computing: Specific security and data protection issues. Internet of Things Security and Data Protection, 71-79. https://doi.org/10.1007/978-3-030-04984-3_4

Cakir, M., Guvenc, M. A., & Mistikoglu, S. (2021). The experimental application of popular machine learning algorithms on predictive maintenance and the design of IIoT based condition monitoring system. Computers & Industrial Engineering, 151, 106948. https://doi.org/10.1016/j.cie.2020.106948

Charyyev, B., & Gunes, M. H. (2021). Locality-sensitive IoT network traffic fingerprinting for device identification. IEEE Internet of Things Journal, 8(3), 1272-1281. https://doi.org/10.1109/jiot.2020.3035087

Chekati, A., Riahi, M., & Moussa, F. (2020). Data classification in Internet of things for smart objects framework. 2020 International Conference on Software, Telecommunications and Computer Networks (SoftCOM). https://doi.org/10.23919/softcom50211.2020.9238186

Cheruvu, S., Kumar, A., Smith, N., & Wheeler, D. M. (2019). IoT frameworks and complexity. Demystifying Internet of Things Security, 23-148. https://doi.org/10.1007/978-1-4842-2896-8_2

Chidambaram, S. (2023). IoT-based ECG monitoring system for smart health-care data applications. Recent Advancement of IoT Devices in Pollution Control and Health Applications, 109-125. https://doi.org/10.1016/b978-0-323-95876-9.00007-0

De Los Santos, H. J. (2022). Understanding MEMS/NEMS devices. Understanding Nanoelectromechanical Quantum Circuits and Systems (NEMX) for the Internet of Things (IoT) Era, 81-111. https://doi.org/10.1201/9781003339939-4

De Villiers, B. (2023). Regaining what has been lost. Indigenous Rights in the Modern Era, 371-396. https://doi.org/10.1163/9789004545663_010

Desai, P., & Modi, N. (2019). IoT based smart lighting system using PIR sensors, Arduino UNO and Thingspeakcloud + chat bot and dashboard to monitor home remotely. International Journal of Engineering and Advanced Technology, 8(5s3), 379-382. https://doi.org/10.35940/ijeat.e1081.0785s319

Dingbang, C., Cang, C., Qing, C., Lili, S., & Caiyun, C. (2021). Does new energy consumption conducive to controlling fossil energy consumption and carbon emissions?-evidence from China. Resources Policy, 74, 102427. https://doi.org/10.1016/j.resourpol.2021.102427

Bhuiyan, M. R. I., Akter, M. S., & Islam, S. (2024). How does digital payment transform society as a cashless society? An empirical study in the developing economy. *Journal of Science and Technology Policy Management*. Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/JSTPM-10-2023-0170

Domb, M. (2019). Smart home systems based on Internet of things. IoT and Smart Home Automation [Working Title]. https://doi.org/10.5772/intechopen.84894

Dowaidar, M. (2021). Gene therapy can target mutations such as BRAF, which have been shown to make tumors more susceptible to autophagy suppression. https://doi.org/10.31219/osf.io/3gwra

Drinkwater, C., & Kai, J. (2018). Making surprising things happen: Building primary care in urban disadvantaged communities. Primary Care in Urban Disadvantaged Communities, 1-12. https://doi.org/10.1201/9781315379241-1

Focus on Catalysts, 2021(5), 2, Gas sensor market size to reach $1.3 bn by 2027 at CAGR 6.4%. (2021).. https://doi.org/10.1016/j.focat.2021.04.009

Ghamari, M., Rangel, P., Mehrubeoglu, M., Tewolde, G. S., & Sherratt, R. S. (2022). Unmanned aerial vehicle communications for civil applications: A review. IEEE Access, 10, 102492-102531

Gupta, V. P. (2021). Smart sensors and industrial IoT (IIoT): A driver of the growth of industry 4.0. Internet of Things, 37-49. https://doi.org/10.1007/978-3-030-52624-5_3

Gürkan, M., Bozkaya, B., & Balcisoy, S. (2022). Financial datasets: Leveraging transactional big data in mobility and migration studies. Data Science for Migration and Mobility, 211-238. https://doi.org/10.5871/bacad/9780197267103.003.0010

Haddaway, N. R., Page, M. J., Pritchard, C. C., & McGuinness, L. A. (2022). PRISMA2020: An R package and Shiny app for producing PRISMA 2020-compliant flow diagrams, with interactivity for optimised digital transparency and Open Synthesis Campbell Systematic Reviews, 18, e1230. https://doi.org/10.1002/cl2.1230

Hanney, S. R., Wooding, S., Sussex, J., & Grant, J. (2020). From COVID-19 research to vaccine application: Why might it take 17 months No. 17 years and what are the wider lessons? Health Research Policy and Systems, 18(1). https://doi.org/10.1186/s12961-020-00571-3

Herrero, R. (2022). Ultrasonic physical layers as building blocks of IoT stacks. Internet of Things, 18, 100489. https://doi.org/10.1016/j.iot.2021.100489

Hodgson, A., Maxon, M. E., & Alper, J. (2022). The US Bioeconomy: Charting a Course for a Resilient and Competitive Future. Industrial Biotechnology, 18(3), 115-136.

Islam, M. A., & Bhuiyan, M. R. I. (2022). Digital Transformation and Society. Available at SSRN: https://ssrn.com/abstract=4604376 or http://dx.doi.org/10.2139/ssrn.4604376

Jaime Moreno Escobar, J., Morales Matamoros, O., Quintana Espinosa, H., Tejeida Padilla, R., & Gabriela Ramírez Gutiérrez, A. (2019). Optimizing a centralized control topology of an IoT network based on Hilbert space. IoT and Smart Home Automation [Working Title]. https://doi.org/10.5772/intechopen.87206

Jaques, H. (2012). International medical students being used as "cash cows," say doctors. BMJ, e4554. https://doi.org/10.1136/bmj.e4554

Jasmin, N. (2023). Internet of things (IoT): The IoT refers to the growing network of devices that are connected to the internet. https://doi.org/10.31219/osf.io/thuxw

Jatolia, S., & Patil, H. (2022). Using IoT for smart home automation & Applications. Journal of IoT Security and Smart Technologies, 1(2), 15-21. https://doi.org/10.46610/jisst.2022.v01i02.003

Jayashankara, M., Udmale, S. S., Pandey, A. K., & Singh, R. S. (2021). IoT healthcare architecture. IoT-Based Data Analytics for the Healthcare Industry, 9-29. https://doi.org/10.1016/b978-0-12-821472-5.00011-9

Jha, S., Tariq, U., Joshi, G. P., & Solanki, V. K. (Eds.). (2022). Industrial Internet of Things: technologies, design, and applications. CRC Press.

Kabanda, P. (2021). Creative natives in the digital age: How digital technology has revolutionized creative work. https://doi.org/10.33774/coe-2021-3b9c1

Khanna, S. (2022). Can electricity demand management drive the transition to clean and affordable energy in poor economies? AEA Randomized Controlled Trials. https://doi.org/10.1257/rct.9118

Khanom, K., Islam, M. T., Hasan, A. A. T., Sumon, S. M., & Bhuiyan, M. R. I. (2022). Worker Satisfaction in Health, Hygiene and Safety Measures Undertaken by the Readymade Garments Industry of Bangladesh: A Case Study on Gazipur. Journal of Business Studies Pabna University of Science and Technology ISSN 2410-8170 2022, 3(1), 93–105. https://doi.org/DOI:10.58753/jbspust.3.1.2022.6

Koley, S., & Acharjya, P. P. (2022). Concepts and Techniques in Deep Learning Applications in the Field of IoT Systems and Security. Convergence of Deep Learning In Cyber-IoT Systems and Security, 303-348.

Kollolu, R. (2020). A Review on wide variety and heterogeneity of iot platforms. *The International journal of analytical and experimental modal analysis, analysis*, *12*, 3753-3760. https://dx.doi.org/10.2139/ssrn.3912454

Lazarus, P. J., Overstreet, S., & Rossen, E. (2020). Building a foundation for trauma-informed schools. Fostering the Emotional Well-Being of our Youth, 313-337. https://doi.org/10.1093/med-psych/9780190918873.003.0016

Li, M., Liang, S., Fan, Y., & Du, W. (2023). Can firms achieve collaborative governance of airborne pollution and greenhouse gases? Evidence from Chinese industrial sector. https://doi.org/10.2139/ssrn.4326108

Liau, J., & Ho, C. (2019). Intelligence IoT(Internal of things) telemedicine health care space system for the elderly living alone. 2019 IEEE Eurasia Conference on Biomedical Engineering, Healthcare and Sustainability (ECBIOS). https://doi.org/10.1109/ecbios.2019.8807821

Lin, Y. (2023). IoT-based enhanced decision-making and data mining for digital transformation of tobacco companies. https://doi.org/10.21203/rs.3.rs-3018868/v1

Łuszczyńska, M. (2021). Ageing within the context of a particular society. Ageing as a Social Challenge, 15-43. https://doi.org/10.4324/b22775-3

Mani, L. (2019). An Analysis of loan portfolio of Janata Bank Limited. Available at SSRN 4644687. or http://dx.doi.org/10.2139/ssrn.4644687

Marabissi, D., Mucchi, L., & Morosi, S. (2021). User-cell association for security and energy efficiency in ultra-dense heterogeneous networks. Sensors, 21(2), 508. https://doi.org/10.3390/s21020508

Mazher, N. (2022). Radio access network to communicate with IoT devices in edge network. https://doi.org/10.31219/osf.io/3gaed

Meah, M. R., & Hossain, R. (2023). Ownership Structure and Auditor Choice in Emerging Economy: An Empirical Study. Indonesian Journal of Business, Technology and Sustainability, 1(1), 12-22. https://orcid.org/0000-0003-4793-1462

Molla, C., Mani, L., Bhuiyan, M. R. I., & Hossain, R. (2023). Examining the Potential Usages, Features, and Challenges of Using ChatGPT Technology: A PRISMA-Based Systematic Review. Migration Letters, 20(S9), 927-945. https://doi.org/10.59670/ml.v20iS9.4918

Mourtzis, D., Angelopoulos, J., & Panopoulos, N. (2023). The Future of the Human–Machine Interface (HMI) in Society 5.0. Future Internet, 15(5), 162.

Nandalal, V., & Anand Kumar, V. (2021). Internet of Things (IoT) and Real Time Applications. *Artificial Intelligence for COVID-19*, 195-214.

Nasution, M., Siregar, O., & Ardian, M. (2022). The influence of customer value and E-service quality on the purchase decision of service products through PLN mobile in Medan Baru customer service unit. Proceedings of the 4th International Conference on Social and Political Development. https://doi.org/10.5220/0011928200003460

Omeke, K. G., Abubakar, A. I., Zhang, L., Abbasi, Q. H., & Imran, M. A. (2022). How reinforcement learning is helping to solve internet-of-Underwater-Things problems. IEEE Internet of Things Magazine, 5(4), 24-29. https://doi.org/10.1109/iotm.001.2200129

Pahuja, M., & Kumar, D. (2023). Energy-efficient stable election protocol for IoT-based healthcare systems using wireless sensor networks. 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT). https://doi.org/10.1109/icccnt56998.2023.10307041

Pérez Jolles, M., & Thomas, K. C. (2018). Disparities in self-reported access to patient-centered medical home care for children with special health care needs. Medical Care, 56(10), 840-846. https://doi.org/10.1097/mlr.0000000000000978

Petrovski, S., & Seviour, R. (2018). Activated sludge foaming: Can phage therapy provide a control strategy? Microbiology Australia, 39(3), 162. https://doi.org/10.1071/ma18048

Ragazou, K., Passas, I., Garefalakis, A., Galariotis, E., & Zopounidis, C. (2023). Big Data Analytics Applications in Information Management Driving Operational Efficiencies and Decision-Making: Mapping the Field of Knowledge with Bibliometric Analysis Using R. Big Data and Cognitive Computing, 7(1), 13.

Robertson, P. W. (2020). Using supply chain analytics to enhance supply chain design processes. Supply Chain Analytics, 99-147. https://doi.org/10.4324/9781003084020-5

Shackelford, S. J. (2020). How can we do better? Finding cyber peace in the Internet of things. The Internet of Things. https://doi.org/10.1093/wentk/9780190943813.003.0007

Singh, D. (2023). Internet of Things. *Factories of the Future: Technological Advancements in the Manufacturing Industry*, 195-227.

Sogam, R. K. (2023). Secure data transmission using cryptography, image processing and steganography (Doctoral dissertation, Dublin Business School).

Sundas, A., & Panda, S. N. (2021). Real-time data communication with IoT sensors and ThingsSpeak cloud. Wireless Sensor Networks and the Internet of Things, 157-173. https://doi.org/10.1201/9781003131229-12

Suresh, A., Udendhran, R., & Balamurugan, M. (2020). Internet of things based solutions and applications for urban planning and smart city transportation. Internet of Things in Smart Technologies for Sustainable Urban Development, 43-62. https://doi.org/10.1007/978-3-030-34328-6_3

Tai, C. S., Hong, J. H., Hong, D. Y., & Fu, L. C. (2022). A real-time demand-side management system considering user preference with adaptive deep Q learning in home area network. Sustainable Energy, Grids and Networks, 29, 100572.

Thamaraimanalan, T., Mohankumar, M., Dhanasekaran, S., & Anandakumar, H. (2018). Experimental analysis of intelligent vehicle monitoring system using Internet of things (IoT). EAI Endorsed Transactions on Energy Web, 169336. https://doi.org/10.4108/eai.16-4-2021.169336

Trivedi, R. S., & Patel, S. J. (2022). Security and privacy aspects in the Internet of things (IoT) and cyber-physical systems (CPS). Handbook of Research of Internet of Things and Cyber-Physical Systems, 453-490. https://doi.org/10.1201/9781003277323-23

Vermesan, O., & Friess, P. (Eds.). (2022). Digitising the Industry Internet of Things Connecting the Physical, Digital and VirtualWorlds. CRC Press.

Viehmann, S., Johannsen, M., & Entrop, D. (2022). How international logistics service providers counter supply chain disruptions through increased visibility and mitigate risk through technology. Supply Chain Resilience, 69-85. https://doi.org/10.1007/978-3-031-16489-7_5

Witwer, M., Miller, K., Pocklington, T., & McFarren, M. D. (2019). Increase in post-coronary artery bypass Graft surgical site infections (SSIs) following cease of active surveillance demonstrates need for continued active surveillance for SSIs following cardiac procedures. American Journal of Infection Control, 47(6), S49. https://doi.org/10.1016/j.ajic.2019.04.123

Yang, L., & Shami, A. (2023). A multi-stage automated online network data stream analytics framework for IIoT systems. IEEE Transactions on Industrial Informatics, 19(2), 2107-2116. https://doi.org/10.1109/tii.2022.3212003

Yang, Z., Liu, Y., Zhang, S., & Zhou, K. (2023). Personalized federated learning with model interpolation among client clusters and its application in smart home. World Wide Web, 26(4), 2175-2200. https://doi.org/10.1007/s11280-022-01132-0

Zamanifar, A. (2021). Remote patient monitoring: Health status detection and prediction in IoT-based health care. IoT in Healthcare and Ambient Assisted Living, 89-102. https://doi.org/10.1007/978-981-15-9897-5_5

Zhang, H. (2021). A survey on energy saving technology of wireless sensor network. Wireless Technology, Intelligent Network Technologies, Smart Services and Applications, 93-99. https://doi.org/10.1007/978-981-16-5168-7_12