Review Article

Artificial Intelligence Application in Cybersecurity and Cyberdefense

Yao Jun,¹ Alisa Craig,² Wasswa Shafik³,³ and Lule Sharif⁴

¹Information Network Center, Beijing Technology and Business University, China

²Department of Statistics, Pennsylvania State University, USA

³Computer Engineering Department, Intelligent Connectivity Research Laboratory, P.O. Box 89175-741, Yazd, Iran

⁴Department of Management Studies, Islamic University in Uganda, Kampala, Uganda

Correspondence should be addressed to Wasswa Shafik; wasswashafik@gmail.com

Received 15 April 2021; Revised 17 September 2021; Accepted 15 October 2021; Published 27 October 2021

Academic Editor: Zhihan Lv

Copyright © 2021 Yao Jun et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Devices are increasingly getting connected to the internet with the advances in technologies called the Internet of Things (IoT). The IoTs are the physical device in which are embedded with software, sensors, among other technologies. Linking and switching data resources with other devices, IoT has been recognized to be a trending research arena due to the world's technological advancement. Every stage of technology avails several capacities, for instance, the IoT avails any device, anyone, any service, any technological path or any network, any place, and any context to be connected. The effective IoT applications permit public and private business organizations to regulate their assets, optimize the performance of the business, and develop new business models. In this study, we scrutinize the IoT progress as an approach to the technological upgrade through analyzing traits, architectures, applications, enabling technologies, and future challenges. To enable an aging society, and optimize different kinds of mobility and transportation, and helps to enhance the effectiveness of energy, along with the definition and characteristics of the IoT devices, the study examined the architecture of the IoT that includes the perception layer, transmission layer, application layer, and network management. It discusses the enabling technologies of the IoT that include application domain, middleware domain, network domain, and object domain. The study further evaluated the role of the IoT and its application in the everyday lives of the people by making smart cities, smart agriculture and waste management, retail and logistics, and smart environment. Besides the benefits, the IoT has demonstrated future technological challenges and is equally explained within the study.

1. Introduction

The world has been exposed to smart technologies, where the favorite products and services of an individual and an organization are connected through electrical devices that include sensors. These devices are cooperative to coordinate with other people without any sort of communication. For illustration, IoTs has utilized homes security, utilities and appliances, entertainment, and health perspective. Within the transportation sectors, IoT is used in logistics, traffic, parking technologies, emergency services, and highways, in communities, business intelligence, factories, retails, environment, surveillance, and smart metering, see [1–13]. At

the national levels, the IoT expresses its capacities in the utilities too, infrastructures, smart grids, defense, remote sensing, and remote monitoring, traffic gather information about the roads, and the weathercast.

The potential benefits of the IoT are nearly limitless, and in this time, the IoT-oriented applications are transforming the way people work. To exemplify how IoT can increase on the achieved customer centricity, onsite data among others are demonstrated within Figure 1 displaying IoT application within a smart city setup.

The way people live via saving not only their time but also logistic resources. The implementation of IoT brings new chances for innovation, knowledge, and development

the current and projected advancement in technology. Lastly, Section 6 holds the conclusion.

2. Literature

In this section, distinguished studies on the IoT are presented and evaluated. The word “IoT” was initially used by Kevin Ashton, who was from the UK, in 1999. He explained “IoT” as a state of amalgamation of different objects and also the objects that are connected tangibly to the internet through sensors.

2.1. The Internet of Things. IoT was developed to express the principle of joining radiofrequency identification (RFID) tags that is used widely in different processes of the supply chain. Currently, this term is very common and extensive for defining different circumstances in which the capability of computing and connectivity of the internet spread on different sensors, objects, devices, and regular items. However, the IoT is novel; the notion of joining the networks to display computers and various devices to regulate has been for many years. In the 1970s, the information system was used in the commercial segment for a remote monitor. Also, access for electrical meters on the network through different phone lines is obtained. The industrial clarifications for tool monitoring and operation are now implemented broadly. From these fantastic initial stages, robust research and development into the field formulated the groundwork for today’s IoT [19].

According to [20], the background of emerging electronic applications and sensors, IoT is about interconnecting entrenched systems. This collaborates into two increasing technologies that include wireless connectivity and smart sensors. These linked entrenched systems of technology are established on minor microcontroller computers that do not require a border for humans. The connections and interactions of humans and the categories of schemes have discovered appliances that are technically progressive and used with various devices. The application of IoT includes smart homes and appliances, smart light technologies, vehicles, smartphones, and inflight services reveal technological growth in Figure 3.

2.2. Characteristics of the Internet of Things. The utmost common feature of the IoT is interconnectivity; anything that can be connected with local, international communication, and information substructure are recognized. The capability of providing “thing-related” facilities within the limitations of things like semantic constancy and privacy defense between tangible things and virtual things is obtained. To offer “thing-oriented” services within the boundaries of things, both types of high-tech of the information world and the physical world will be rehabilitated. The relativity to heterogeneity is based on various hardware networks and platforms. Through this, people can network with other platforms of services and devices through various networks, as demonstrated in [21]. Its state of devices that transform dynamically include sleeping and waking up, disconnected and connected, and devices relating to speed and location.

The huge nature of these devices requires to be managed, communicated with each other, and at least an instruction of magnitude bigger than procedures linked with the internet. Overlooking security and its associated challenges, the public tends to enjoy IoT advantages; it is then therefore essential to plan for security as well. This includes the security of individual data and the security of well-being. Most importantly, the IoTs and their connectivity permit network compatibility and availability. The availability is receiving to the network, while compatibility offers the mutual ability to yield and consume data; see [22].

3. Internet of Things Architecture

In this section, three-core architecture of IoT, i.e., the perception, transmission, and application layers is presented. The conception of IoT is achievable through the process of integration of different enabling technologies, like RFID, the wireless sensor networks (WSN), the machine to machine (M2M), and the low-power personal area network. To evaluate the primary role of IoT, different frameworks have been proposed. There are based on application necessities, protocols, network topology, and business models, but they are not standardized to date.

The security problems need key care to form reliable applications and systems. The architecture of IoT has capacities to discourse diverse factors that include quality of service, reliability, privacy management, and care for novel devices and services. These features endorse the development and design of schemes that offer functionality efficiently and reliably. The architecture of IoT is separated into three layers, as discussed below.

3.1. Perception Layer. The perception layer is the lowest layer of the architecture of IoT. This layer involves high-tech used for identification, identification, actuation, and communication with a minimum level of human communication. It is considered by catching the evidence from the actual world and showing it in the digital arrangement. Besides, the sub-layers of this layer include perception nodes and perception networks. There are some key technologies of IoT that include a global positioning system (GPS), WSN, and RFID.

The GPS perceives the phone’s location, and it is an essential piece to provide contextual information for smart applications [23]. The WSN is a technology used in the IoT system mainly in the gathering of sensors that can be used individually to accumulate data and transmit data with the help of a router to the internet in a system of IoT. The RFID is an automated technology that aids computers and machines to classify objects, control personal targets, and record metadata with the help of radiowaves.

3.2. Transmission Layer. The transmission layer is interrupted between the application and the perception layer. This is considered the integration for different heterogeneous legacy networks, protocols, and technologies. Likewise, this layer is aimed at transmitting the gathered data through perception nodes to the information processing unit by using wireless or wired networks of communication for

FIGURE 3: Internet of Things and its application.

analysis, data aggregation, data mining, and data encoding [24]. This layer also has the responsibility of giving functionality for network management. Based on its functionality, this layer can be further segregated into three sublayers that include access network, local and wide area network, and core network.

There are some key technologies under this layer that include general packet radio service (GPRS) and ad hoc network. The ad hoc network is a kind of local area network (LAN) that is made instinctively when the devices get connected. The ad hoc networks are configurable and deployable networks for industrial use. As an alternative, the architecture of GPRS has some extra entities that permit a data transmission package.

3.3. Application Layer. This is one of the highest layers of the architecture of IoT that is noticeable to the end-user. The layer is aimed at regulating and providing the application internationally based on the collected info that is administered by the unit of info processing. It gives access to personalized facilities to users through the network based on their requirements through the use of different terminal equipment and handheld devices.

3.4. Network Management. Network management is a topological element and effective resource management. Some current approaches of resource and network management in the environment of IoT include extensible messaging and presence protocol, software-defined networking, and game-theoretic mechanisms. Information security and physical management deal with the protection of interconnected physical devices that secure information transmission and storage among devices. Besides, the more quantity of smart devices increases the necessity of techniques of management of transparent security that deals with the network, web interface. The security of software and mobile services that

safeguard the integrity, confidentiality, and user privacy of information are considered.

Trust management significantly helps in IoT growth by giving consistent services to users to enhance their privacy of users. Minimizing uncertainties and risks that are linked with the IoT applications enhances the approval of users for these requests [9]. The layers (the perception, transmission, and application) are illustrated in Figure 4.

3.5. Internet of Things Enabling Technologies. The systems of IoT encompass functional chunks that enable different utilities to the systems that include sensing identification, communication, actuation, and administration. Technologies of IoT can be reduced into different groups that include recognition technologies and identification technologies, software, hardware, communication networks, algorithms, and positioning technologies among others.

The platforms of IoT allow an informal combination of different IoT technologies. These types of platforms are a layer that attaches the possessions to the network. Nonconcrete requests from the things having a goal that allows the growth of facilities [25]. These platforms offer a framework for associating things with different applications and networks. Different IoT platforms include cloud platforms and hardware used to enhance flexibility, productivity, and usability for different IoT applications that reduce cost and time in the developing process.

IoT technologies are measured from different features including utility features to offer perceptions for open challenges and issues of the currently used domains. The main IoT-enabling technologies do include sensor technologies, wireless communications, and networking RFID, and smart technology and computing and nanotechnology are demonstrated in Figure 3, in considering cost-effectiveness, the embedded system including security and privacy, software-based, data and signal processing, cloud computing identification, data and signal processing, among others.

Layers	Sub-layers	Key Features	Key Technologies
Application layer	IoT applications	Handheld devices, Terminals and User Interface	Cloud computing, Middleware, M2M, Service support platform
	Application support layer		
Transmission layer	Local & Wide Area Network	Connectivity establishment and Information transmission	Internet, GPRS, Wi-Fi, Ad hoc Network
	Core network		
	Access network		
Perception layer	Perception network	Sensing, Identification, Actuation and Communication technologies	RFID, WSN, GPS, Bluetooth
	Perception nodes		
Network management	Physical and information security management		Trust management

FIGURE 4: The Internet of Things architecture.

3.5.1. Sensor Technologies. The innovation of IoT helps to connect things every day to the internet. The sensors play a key role in identifying solutions through IoT. The sensors are devices that perceive external information and replace it through a signal that machines and humans can differentiate.

3.5.2. Wireless Communication and Networking. The devices of IoT use wireless communication for making communication with other devices, and it supports to empower the communication between system and sensor. It also works as a communication capability for sharing and transferring data with other devices [26].

3.5.3. Smart Computing. Smart computing serves as a new generation of integrated software, hardware, and network technologies that offer information technology systems through awareness of real time in the real world. Correspondingly, it provides advanced analytics that help people to make intelligent decisions. It enables the network power to devolve processing abilities to various parts of networks.

3.5.4. Nanotechnology. Massive data of the IoT data is created by different interconnected nanodevices. In this regard, nanotechnology is relevant for the processing of data of the IoT. These technologies are implemented to form powerful supercomputers and processors that help to collect, report, and analyze data that are formed by devices of IoT.

3.6. IoT Domains. The IoT has more potential for enhancing intelligent requests in every straight market like smart homes, smart transportation, and smart healthcare. For instance, several IoT applications are implemented successfully for systems of smart traffic, regulation of chain of logistics, fleet tracking solutions, smart cities, and smart metering, energy efficiency, etc.

3.6.1. Application Domain. The IoT requests offer a regular of capabilities and functionalities that can be gathered as

per the domain of application into four different areas that include monitoring, control, optimization, and autonomy. The domain of application regulates the services of applications that are typically given through the middleware layer of IoT.

The application programming interfaces (API) and technologies can be plotted to the middleware domain or application. For allowing functionalities of the domain of application, there is some shared entrenched operating system (OS) in use that includes TinyOS, LiteOS, and the OS like Riot OS. These types of arrangements are helpful to support the low-power communication of the internet, and they need a rare kilobyte of random access memory.

3.6.2. The Middleware Domain. The IoT middleware is a scheme that is controlled through infrastructure and software, planned to be midway between the application layer and IoT objects. In this domain, the technologies are grouped that offer functionalities like filtering, aggregating, and processing acquired information from the devices of IoT, machine learning, information unearthing, projecting modeling, and offering access regulators to the application devices. The common solutions of the functionalities of IoT middleware depend on cloud computing. The cloud platforms allow data processing and IoT services development self-sufficiently of the platform of hardware. There are different open sources and commercial stages that can be assessed through gateway provision, programming language, and application protocol support [27].

3.6.3. The Network Domain. This contains technologies, hardware, and protocols that allow connectivity between global and object infrastructure. The system of IoT uses an exciting variety of different technologies of communication that require to be interoperable to cater to supplies of IoT. These include location-based capabilities, autonomic networking, autonomic services providing, plug and play, security, manageability, privacy, and quality [28].

FIGURE 5: Enabling technologies of the internet of things.

There exist open issues associated with this domain that include scalability, interoperability, reliability, management, mobility, coverage, routing, resource usage control, and energy efficiency. Enabling technologies of the IoT are presented within Figure 5, entailing thread, platform, ZigBee, wifi, and others.

3.6.4. Object Domain. This shows the endpoint layer that comprises tangible things and effective things. These objects have different competencies such as actuation, sensing, recognizing, data processing and storage, linking with other different objects, and combination into networks of communication. The objects of IoT include entrenched software and hardware. Also, the sensors are objects that measure and detect some changes and events in their situation that include air pressure, temperature, quickening, light, and movement. They execute actions to deliver output for prospective handling. Different sensors are entrenched in different objects that enable value-added services related to IoT [29].

4. Internet of Things Application Domains

In this section, the application of IoT is broadly explained from diverse perspectives. The applications of the IoT are frequent and different, and they pervade virtually all elements of the daily life of people, society, and institutions. The IoT applications encompass wider areas comprising the industrial and manufacturing sector, agriculture, health sector, smart cities, emergencies, security, and other areas, detailed in [30]. The application of IoT in some key areas is explained below. Corresponding-enabling-technologies as demonstrated within Figure 6 are classified as data acquisition and sensing, data transmissions, data processing, and information management, and lastly, utilization and actions as depicted.

4.1. Smart Cities. Some areas of application of IoT for forming smart cities include systems of intelligent transportation, traffic congestion, smart building, waste management, smart lighting, urban maps, and smart parking. Artificial intelligence enables IoT to be used effectively to assess, mitigate, and regulate traffic overcrowding in Smart Cities [31].

Additionally, IoT permits the connection of weather-oriented street lighting and finding of waste containers by possessing flaps of schedules of trash gathering. Moreover, intellectual highways offer essential information and warning messages that include access to alterations depending on unexpected occurrences and climatic conditions like accidents and traffic jams.

4.2. Smart Agriculture and Waste Management. The IoT can enhance and promote the agriculture sector by assessing the soil moisture and monitoring trunk width. IoT permits to regulate and reserve the measure of vitamins present in products of agriculture and also manage the circumstances of a microclimate to make more manufacture of fruits and quality vegetables, see [32].

By evaluating weather conditions, IoT permits predicting ice information, wind alterations, drought, snow, and rain and regulates humidity and temperature levels that avert fungus and other bacterial pollutants.

4.3. Retail and Logistics. The execution of the IoT in the retail and supply chain has numerous benefits, and some of the benefits include assessing the conditions of storage in the entire supply chain and also product tracking that help in payment processing while relying on the activity period and location in gyms, public transport, and theme parks, see [33].

Moreover, in the retail locations, IoT is smeared to different applications that include fast processes of payments like automatically examining out through the assistance of biometrics, detection of possible allergen products, and

FIGURE 6: Enabling technologies of the Internet of Things.

control of the spin of products in warehouses as early demonstrated in [34].

4.4. Smart Environment. The strategies of the smart environment are effective through the integration of the technology of IoT and must be formulated for sensing, assessing, and tracking objects in an environment that provides possible advantages in accomplishing a green and ecological life. Moreover, the IoT technology permits managing and observing air quality through the process of data gathering from different remote sensors in different cities by offering topographical exposure to achieve better means of regulating traffic blockages in big cities [35, 36].

5. Future Challenges of the Internet of Things

In this section, we present identified future challenges of IoT. Not only IoT in particular but also as the technology advances, business, and society at large as discussed below:

5.1. Technology. Within the technological aspect, there do exist a number of issues that call for focal analysis. This section mainly entails issues. This includes security, connectivity, compatibility and longevity, technological standards, intelligent actions, and analysis as IoT is concerned, see Figure 7.

5.1.1. Security. The IoT has been a key element for the future of the internet as it has enhanced usage that necessitates the requirement to sufficiently address trust and security functions. Moreover, the basis of IoT is laid down on the current WSN, and it architecturally receives a similar level of security and privacy issues as WSN possesses. The different weaknesses and attacks of systems of IoT show that there is a requirement for broad-ranging projects of security that will defend systems and data from end to end [37].

5.1.2. Connectivity. The IoT has some challenges regarding connectivity and the major ones include bandwidth and power consumption. These challenges are faced by people because people want easier connectivity and usability of devices [38].

5.1.3. Longevity and Compatibility. The IoT has a vast research paradigm due to various advanced high-tech that are contending to achieve a certain standard. There exist a number of compatibility factors that range from nonunified cloud services to other standards like a shortage of homogeneous machine to machine diversities and protocols in firm-ware, see [39].

5.1.4. Technological Standards. The challenges of IoT regarding technological standards include actions of machines for different impulsive circumstances, privacy and information security, mean-reverting human performances, and slower implementation of new technologies [40].

5.1.5. Intelligent Actions and Analysis. The challenges regarding intelligent analysis and actions within the Internet of Things include erroneous analysis because of faults in the model and data, the ability of legacy systems to examine unstructured data, and also the ability of legacy systems to manage and regulate real-time data [41].

5.1.6. Use of Weak and Default Credentials. Numerous IoT companies are selling devices and giving consumers default credentials, just like an admin username. The hackers require a password and username to attack the device. When hackers know the username, they conduct brute force attacks to contaminate the devices.

5.2. Business

5.2.1. Consumer Internet of Things. Though the consumers are getting the benefits and advantages from IoT, however, some challenges are posed to consumers related to the security and privacy that IoT poses. Moreover, the consumers also face the problem of malware, data loss, unauthorized access to personal data, illegal surveillance, and intrusive uses which are some risks posed to consumers.

5.2.2. Commercial Internet of Things. There are some of the commercial issues that are faced by companies regarding IoT include interoperability and compatibility of various Internet of Things systems. The authentication and identification of technologies also led to merges of IoT products

FIGURE 7: Internet of Things-based technological challenges.

with IoT-based platforms, data capturing capabilities, and intelligent analytics.

5.2.3. Industrial Internet of Things. The primary challenges of industrial IoT include the high investment cost, secure data management and storage, and connectivity outages that the companies and organizations must be aware of in their daily operations.

5.3. Social and Legal Challenges

5.3.1. Privacy. The major challenges of IoT regarding privacy are regarding awareness of tracing on the face of passive data gathering, the control of communal data location in indoor environments.

5.3.2. Internet of Things Data. IoT data relates to the information collected from sensors found in connected devices. There are two main challenges of IoT data in the cloud. The first challenge is about the quick growth of data, and the second one is regarding the lack of data security of IoT.

5.3.3. Technology for Security. There are various challenges related to the technology of security of IoT that include the out-of-date wares (like software and hardware), the use of default, and weak identifications. The prediction and prevention of attacks, the difficulty in finding a device that is affected, and other security and data protection challenges are demonstrated explicitly within.

5.3.4. Business Procedures and Policies. Some business-related challenges include technical expertise, security, connectivity and workload, and support. The businesses might face these challenges, and proper training is required for proper implementation of IoT considering policies and procedures [42, 43].

5.3.5. Internet of Things: Laws and Regulation. There might also be some challenges, particularly legal and ethical. The legal laws are related to cybersecurity, and ethical laws and regulations are related to privacy, access, and integrity of information, and the compliance of these laws might be a challenge [44].

6. Conclusion

In this study, an examination of the IoT progress in approaching the technological upgrade through analyzing traits, architectures, applications, enabling technologies, and future challenges. To enable an aging society and optimize different kinds of mobility and transportation and help

enhance the effectiveness of energy, along with the definition and characteristics of the IoT, are the aim of this study. This study has also analyzed the architecture of the IoTs that includes the perception layer, transmission layer, application layer, and network management. More still, it discusses the enabling technologies of the IoTs that include application domain, middleware domain, network domain, and object domain. This study has also analyzed the role of the IoTs and their application in the everyday lives of the people by making smart cities, smart agriculture and waste management, retail and logistics, and a smart environment. Apart from all these benefits, the IoTs also have some future challenges and these are also discussed in this study. IoT is the latest revolution on the internet and it is a major topic of research. The researchers are embedded to research this domain because it encompasses a varied application area and a combination of different communications based on entrenched technology and its planning.

Data Availability

All the datasets are provided within the main body of the paper.

Conflicts of Interest

There are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This research is supported by the Department of Computer Engineering, Yazd University, Iran.

References

- [1] S. Smys, "A survey on internet of things (IoT) based smart systems," *Journal of ISMAC*, vol. 2, no. 4, pp. 181–189, 2020.
- [2] M. Sarma, T. Matheus, and C. Senaratne, "Artificial intelligence and cyber security: a new pathway for growth in emerging economies via the knowledge economy," in *Business Practices, Growth and Economic Policy in Emerging Markets*, pp. 51–67, Series in Business and Emerging Markets, 2021.
- [3] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (IoT): a vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.
- [4] M. Yildirim, "Artificial intelligence-based solutions for cyber security problems," in *Artificial Intelligence Paradigms for Smart Cyber-Physical Systems*, pp. 68–86, IGI Global, 2021.

- [5] F. Ihsan and N. K. Bintarsari, "Internet governance forum analysis on artificial intelligence in cyber security," *Insignia: Journal of International Relations*, vol. 35, pp. 32–47, 2021.
- [6] K. K. Patel and S. M. Patel, "Internet of things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges," *International Journal of Engineering Science and Computing*, vol. 6, no. 5, 2016.
- [7] A. Mathew, "Artificial intelligence for offence and defense-the future of cybersecurity," *Educational Research*, vol. 3, no. 3, pp. 159–163, 2021.
- [8] Y. Jia, B. Fang, A. Li, and Z. Gu, "Artificial intelligence enabled cyberspace security defense," *Strategic Study of Chinese Academy of Engineering*, vol. 23, no. 3, pp. 98–105, 2021.
- [9] G. Misra, V. Kumar, A. Agarwal, and K. Agarwal, "Internet of things (iot)—a technological analysis and survey on vision, concepts, challenges, innovation directions, technologies, and applications (an upcoming or future generation computer communication system technology)," *American Journal of Electrical and Electronic Engineering*, vol. 4, no. 1, pp. 23–32, 2016.
- [10] G. Cybenko and R. Hallman, "Resilient distributed adaptive cyber-defense using blockchain," *Game Theory and Machine Learning for Cyber Security*, vol. 22, pp. 485–498, 2021.
- [11] Z. R. Khan, S. Venugopal, and F. Oroumchian, "Tracking changing perceptions of students through a cyber ethics course on artificial intelligence," in *Advances in Software Engineering, Education, and e-Learning*, pp. 287–302, Springer, Cham, 2021.
- [12] P. Sethi and S. R. Sarangi, "Internet of things: architectures, protocols, and applications," *Journal of Electrical and Computer Engineering*, vol. 2017, Article ID 9324035, 2017.
- [13] S. K. Sahay, N. Goel, M. Jadhwal, and S. Upadhyaya, "Advances in secure knowledge management in the artificial intelligence era," *Information Systems Frontiers*, vol. 23, no. 4, pp. 807–810, 2021.
- [14] M. Taylor, D. Reilly, and C. Wren, "Internet of things support for marketing activities," *Journal of Strategic Marketing*, vol. 28, no. 2, pp. 149–160, 2020.
- [15] A. Juneja, S. Juneja, V. Bali, V. Jain, and H. Upadhyay, "Artificial intelligence and cybersecurity: current trends and future prospects," *The Smart Cyber Ecosystem for Sustainable Development*, vol. 27, pp. 431–441, 2021.
- [16] H. Grindvoll, O. Vermesan, T. Crosbie, R. Bahr, and N. Dawood, "A wireless sensor network for intelligent building energy management based on multi communication standards—a case study," *Journal of Information Technology in Construction*, vol. 17, pp. 43–61, 2012.
- [17] P. Tadejko, "Application of internet of things in logistics—current challenges," *Ekonomia Zarządzanie*, vol. 7, pp. 54–64, 2015.
- [18] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for internet of things," *Journal of Network and Computer Applications*, vol. 42, pp. 120–134, 2014.
- [19] S. H. Mahmud, L. Assan, and R. Islam, "Potentials of internet of things in Malaysian construction industry," *Annals of Emerging Technologies in Computing*, vol. 2, no. 4, pp. 44–52, 2018.
- [20] O. Vermesan, P. Friess, and P. Guillemin, "Internet of things strategic research roadmap," *Global Technological and Societal Trends*, vol. 1, pp. 9–52, 2011.
- [21] K. K. Patel and S. M. Patel, "Internet of things definition, characteristics & future challenges," *International Journal of Engineering Science and Computing*, vol. 6, no. 5, pp. 6122–6131, 2016.
- [22] S. Mostafavi and W. Shafik, "Fog computing architectures, privacy and security solutions," *Journal of Communications Technology, Electronics and Computer Science*, vol. 1, no. 24, pp. 1–4, 2019.
- [23] O. Said and M. Masud, "Towards internet of things: survey and future vision," *International Journal of Computer Networks*, vol. 5, no. 1, pp. 1–17, 2013.
- [24] A. T. Caposelle, V. Cervo, C. Petrioli, and D. Spenza, "Counteracting denial-of-sleep attacks in wake-up-radio-based sensing systems," in *2016 13th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, pp. 1–9, London, UK, June 2016.
- [25] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things: a vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.
- [26] L. Atzori, A. Iera, and G. Morabito, "IIoT: giving a social structure to the internet of things," *IEEE Communications Letters*, vol. 15, no. 11, pp. 1193–1195, 2011.
- [27] S. Bandyopadhyay, M. Sengupta, S. Maiti, and S. Dutta, "Role of middleware for internet of things: a study," *International Journal of Computer Science & Engineering Survey*, vol. 2, no. 3, pp. 94–105, 2011.
- [28] O. Salman, I. Elhajj, A. Kayssi, and A. Chehab, "Edge computing enabling the internet of things," in *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)*, pp. 603–608, Milan, Italy, 2015.
- [29] D. Zeng, S. Guo, and Z. Cheng, "The web of things: a survey," *Journal of Communications*, vol. 6, no. 6, pp. 424–438, 2011.
- [30] H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: architecture, applications, and approaches," *Wireless Communications and Mobile Computing*, vol. 13, no. 18, 1611 pages, 2013.
- [31] S. V. Zanjali and G. R. Talmale, "Medicine reminder and monitoring system for secure health using internet of things," *Procedia Computer Science*, vol. 78, no. 3, pp. 471–476, 2016.
- [32] S. Veena, K. Mahesh, M. Rajesh, and S. Salmon, "The survey on smart agriculture using internet of things," *International Journal of Innovative Research in Engineering & Management*, vol. 5, no. 2, pp. 63–66, 2018.
- [33] G. Omeroglu, A. Ertug, and A. Ozkavukcu, "Systematic literature review for work sampling with IOT technology in retail store operations," in *International Conference on Intelligent and Fuzzy Systems*, vol. 21, pp. 1666–1674, Springer, Cham, 2020.
- [34] H. Liu, C. Zhong, A. Alnusair, and S. R. Islam, "FAIXID: a framework for enhancing ai explainability of intrusion detection results using data cleaning techniques," *Journal of Network and Systems Management*, vol. 29, no. 4, pp. 1–30, 2021.
- [35] N. S. Zulkifli, M. R. Satrial, M. Z. Osman, N. S. Ismail, and M. R. Razif, "IoT-based smart environment monitoring system for air pollutant detection in Kuantan, Pahang, Malaysia," *Materials Science and Engineering*, vol. 769, no. 1, article 012014, 2020.
- [36] M. Abdelsalam, M. Gupta, and S. Mittal, "Artificial intelligence assisted malware analysis," in *Proceedings of the 2021 ACM*

Workshop on Secure and Trustworthy Cyber-Physical Systems, pp. 75–77, New York, United States, 2021.

- [37] S. A. Alabady, F. Al-Turjman, and S. Din, “A novel security model for cooperative virtual networks in the IoT era,” *International Journal of Parallel Programming*, vol. 48, no. 2, pp. 280–295, 2020.
- [38] X. He, Z. Peng, J. Wang, and G. Yang, “Generic and efficient connectivity determination for IoT applications,” *IEEE Internet of Things Journal*, vol. 13, pp. 33–42, 2020.
- [39] K. H. Phung, H. Tran, and V. Tran-Quang, “Service platform for integration of various M2M/IoT system,” *Journal of Science & Technology*, vol. 144, pp. 17–21, 2020.
- [40] K. Kiela, V. Barzdenas, M. Jurgo et al., “Review of V2X–IoT standards and frameworks for ITS applications,” *Applied Sciences*, vol. 10, no. 12, p. 4314, 2020.
- [41] A. Gupta, R. Gupta, and G. Kukreja, “Cyber security using machine learning: techniques and business applications,” in *Applications of Artificial Intelligence in Business, Education and Healthcare*, pp. 385–406, Springer, Cham, 2021.
- [42] X. Zheng and Z. Cai, “Privacy-preserved data sharing towards multiple parties in industrial IoTs,” *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 5, pp. 968–979, 2020.
- [43] S. Soderi, “Acoustic-based security: a key enabling technology for wireless sensor networks,” *International Journal of Wireless Information Networks*, vol. 27, no. 1, pp. 45–59, 2020.
- [44] J. Al Ali, Q. Nasir, and F. T. Dweiri, “Business continuity framework for internet of things (IoT) services,” *International Journal of System Assurance Engineering and Management*, vol. 11, no. 6, pp. 1380–1389, 2020.