IEC
Institute of Electronics and Computer

Journal of Artificial Intelligence and Systems, 2024, 6, 112-123
https://iecscience.org/journals/AIS
ISSN Online: 2642-2859

Blockchain Integration with AIoT Data Security and Privacy for Sustainability

Priyanka Arora[1,*], Ritu Makani[2]

[1]Research Scholar, GJUST, Hisar, Haryana, India
Email: priyankaarora2844@gmail.com
[2]Associate Professor, GJUST, Hisar, 125001, Haryana, India
Email: ritunagpal1973@gmail.com
*Corresponding Author

How to cite this paper: Priyanka Arora, Ritu Makani (2024). Blockchain Integration with AIoT Data Security and Privacy for Sustainability. Journal of Artificial Intelligence and Systems, 6, 112–123. https://doi.org/10.33969/AIS.2024060108.

Received: February 19, 2023
Accepted: April 10, 2024
Published: April 24, 2024

Abstract

AIoT (Artificial Intelligence of Things) is the fusion of AI (artificial intelligence) methods with IoT (Internet of Things) infrastructure, which is deployed there to enhance the overall system performance of AIoT. Artificial Intelligence of Things can be used to make Internet of Things operations more efficient, which will enhance data analysis and human-machine interactions. The system's general usefulness is further increased by applying artificial intelligence techniques to convert Internet of Things data into relevant information for improved decision-making processes. The Artificial Intelligence of Things frameworks have a wide range of applications, including eCommerce, logistics operations and control, smart homes, smart farms, intelligent transportation systems, industrial automation and control, eCommerce, secure as well as safe healthcare monitoring, and many more. AIoT frameworks, however, are susceptible to a variety of information security-related assaults, which could result in problems with data security and privacy. Serious repercussions, such as unapproved data updates and leaks, are also brought on by these problems. One particular kind of database is the blockchain. It's a digital record of all the transactions that's distributed throughout the whole network of systems. Data is stored in the blocks that are linked in a chained manner. Compared to conventional security methods, blockchain technology offers greater security and is impervious to tampering. Therefore, to increase security, blockchain can be used in a variety of AIoT applications. A safe authentication architecture for AIoT has been suggested, modelled after a generalised blockchain. The adversarial model, which handles most potential security threats in this kind of communication environment, is also highlighted. This framework is part of the blockchain-envisioned safe authentication framework for the Internet of Things. The suggested framework's numerous applications are also covered. Additionally, certain problems and difficulties with the suggested framework are emphasised. Finally, we also offer some suggestions for future research that are related to the framework that has been suggested.

Keywords

Blockchain, Artificial Intelligence, Internet of things, Security, Privacy, Integration

1. Introduction

AIoT: The acronym AIoT represents Artificial Intelligence of Things. It describes how Artificial Intelligence (AI) technologies are incorporated into the Internet of Things (IoT) framework. Data collection and sharing are made possible via the Internet of Things (IoT), which is a network of physically connected objects such as cars, appliances, and other products that have been embedded with sensors, software, and network connectivity. AI, on the other hand, entails building devices or systems that can mimic human intelligence, including the ability to think, reason, and make decisions. Through the integration of AIoT, IoT devices can use AI algorithms and techniques to process data, make smart decisions, and carry out tasks without the need for human participation. Devices can become more intelligent, effective, and able to adjust to shifting conditions by combining AI with IoT.

Applications of AIoT are found across many different areas, including manufacturing, transportation, smart cities, healthcare, and agriculture. Improved data analysis, autonomous operations, predictive maintenance, and increased productivity across a range of industries are all made possible by this connection [6]. The term "Internet of Things," or "Things," refers to a network of physical items that are embedded with sensors, software, and other relevant technology. With them, additional systems and gadgets have to be connected to the Internet in order to exchange data. Global data collection and sharing via the Internet is facilitated by these billions of IoT devices. This level of digital intelligence is made possible by the interconnection of all these smart items, which are equipped with built-in sensors. This eliminates the need for human intervention and allows them to communicate the data in real time. In 2015, there were 15:41 billion linked IoT devices; by 2025, that number is predicted to increase to 75:44 billion. The trends in the number of connected IoT devices are seen in Figure 1 [7].

Some AI Technologies are: [1-5]

1. **Cyber Security:** This computer defence system guards against online threats connected to information security by identifying and thwarting them. With the help of machine learning techniques, neural networks—which can interpret sequences—may be used to develop learning technologies that can help mitigate cyberattacks.
2. **Speech Recognition:** To translate and transform human speech into a format that can be processed by a computer programme, speech recognition mechanisms are used. There is a need for the "translation and transformation of human language" into

a format that is beneficial these days.

3. **Image recognition:** It involves finding and identifying certain elements in an image or video file. It further streamlines image searches, making it easier to diagnose illnesses and find licence plates, for example.

4. **Virtual Agent:** A computer agent or programme that can communicate with people is called a virtual agent. Chatbots are utilised in the customer service system to utilise it. Virtual agents are used by companies like Apple, Google, Amazon, and Microsoft to deliver support.

5. **Natural Language processing:** It is centred on the communication between human languages and computers. Sentence structure and interpretation via machine learning algorithms are analysed using text analysis techniques. Systems for detecting fraud can benefit from NLP as well. NLP is used by applications and automated assistants to extract unstructured data.

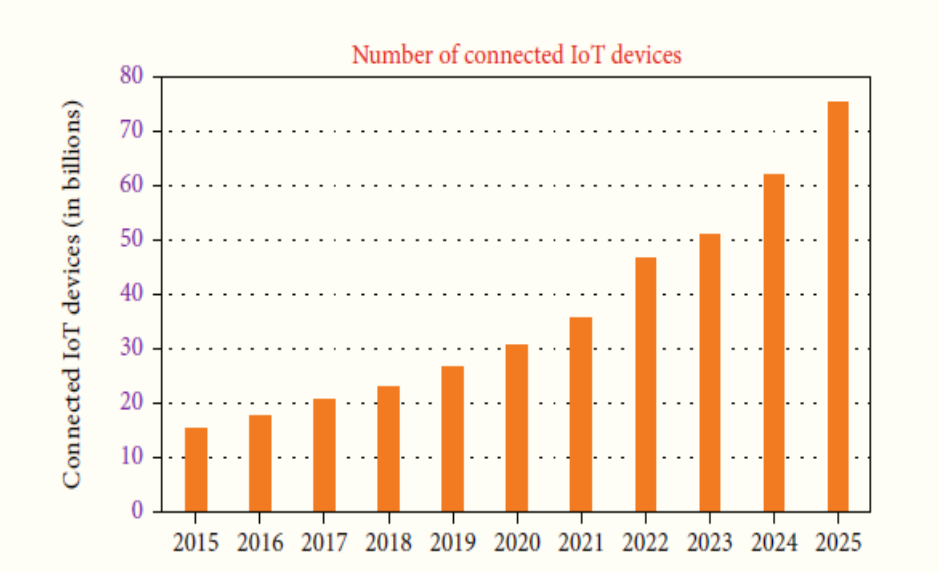

Figure 1. Numbers of IoT devices linked over time

Blockchain: Distributed ledger technology, or blockchain, makes it possible to create a transparent, unchangeable record of transactions via a network of computers. Instead of being controlled by a single entity, it functions as a decentralised database that is maintained by numerous participants (nodes). The blockchain is a digital log of transactions that is replicated and dispersed over the whole network of computer systems, or cloud servers. The manner the data is stored distinguishes it from a traditional database. Blockchain is a distributed ledger system that maintains data as a series of linked blocks. Fresh data is added to a block that is created whenever it is received.

Some Properties of Blockchain:

1. **Programmable:** A blockchain can be constructed using Solidity programming or another programming language to create smart contracts.
2. **Secure:** Blockchain protects the stored data by encrypting it and using hashing techniques. Utilizing all of the transaction hashes, the Merkle tree is constructed and subsequently utilised for integrity verification. As such, it is exceedingly challenging to update or modify the data that is kept inside the blockchain. Moreover, information is kept in encrypted transactions, making it impossible for data to leak without authorization.
3. **Distributed**: In the form of a distributed ledger, a peer-to-peer distributed network creates a blockchain. All authorised entities have access to this ledger (i.e., miner nodes).
4. **Anonymous:** This feature allows the entities' identities to be maintained. This shows that opponent (A) is unable to determine who is speaking with whom.

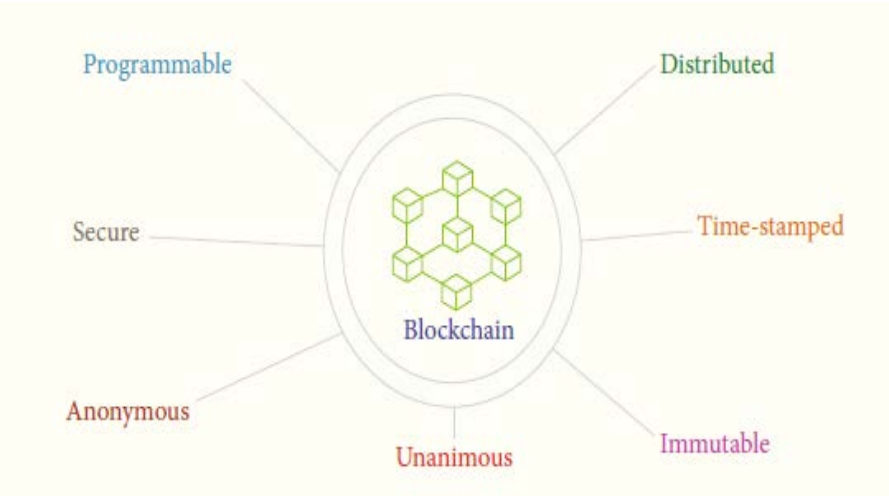

Figure 2. Properties of Blockchain

5. **Time-Stamp:** A newly created timestamp value is also saved with a block when it is constructed in a blockchain. Further assistance in resolving the data freshness concerns is provided by this approach. This also indicates that entities have the ability to determine "when a specific record is stored in the block."
6. **Immutable:** Anything we keep there will be contained within the blocks that make up a blockchain. A hash chain links these blocks together. A cannot alter the block's data in any way. If A tries to update the blocks, then in that case, he or she needs to change a specific.
7. **Unanimous:** A consensus method must be carried out in order for a newly produced block to be added to the blockchain. The miner nodes carry out the

consensus algorithm's steps (i.e., cloud servers). The bulk of the miner nodes concur during this procedure regarding the addition of the "newly produced blocks," if a specific percentage of nodes, such as 80 percent of nodes, commit (agree). A block is added to the blockchain in such a case. Thus, nodes vote on specific jobs in unanimity during implementation and execution.

2. Applications of AIoT-Related Secure Authentication Framework Inspired by Blockchain

We go over a few possible uses for the blockchain-envisioned safe authentication system for the Internet of Things in this part. Their information is given below: [1-5, 8-9]

2.1 Surveillance System and Security

The deployment of security and surveillance systems can take place in various areas, such as cities to keep an eye on criminal activity or border regions to keep an eye on hostile activity. Drones, CCTVs, infrared cameras, and smart sensors are all part of the security and surveillance system. For the purpose of processing, storing, and analysing data, these devices are linked to a central server, or cloud server. Nevertheless, this type of data analysis and storage setup is not entirely secure. Maintaining it in the form of a blockchain via a peer-to-peer cloud server network is therefore preferable. Transactions that are encrypted can be used to store whole data sets. Once the necessary user authentication steps have been completed, authorised users of the system can also access system data. In this kind of system, the artificial intelligence component helps forecast potential dangers, such as the likelihood of infiltration attempts.

2.2 Smart Home

This is a practical configuration for a house that has smart appliances installed, such as a refrigerator, air conditioner, TV, and coffee machine. These smart appliances can be remotely managed automatically by smartphone applications at any time, from any location, over the Internet. A user can control features such as temperature control, on/off lights, and security access to the home by connecting the Internet to the deployed smart home's components. For the purpose of processing, storing, and analysing data, these devices are linked to a cloud server or other central server. Maintaining blockchain-based smart home data via a peer-to-peer cloud server network is preferable. Under such a setup, artificial intelligence (AI) can enhance the system's overall functionality and better serve the consumers.

2.3 Intelligent Transportation System

Smart IoT devices and smart cars enable Intelligent Transport Systems (ITS). The following goals are accomplished by the control and information systems, or ITS, through the employment of data processing and communications technology. It facilitates better commodities and people transportation. Along with managing various situations according to the circumstances, such as roadside conditions and accident occurrence, it also improves safety and lessens traffic congestion. From this conversation, it is evident that significant mechanisms, such as the blockchain, are required for the safety and security of the ITS data. These mechanisms can be implemented there to meet the necessary requirements for information security. Additionally, the artificial intelligence component helps forecast certain risks, such as the likelihood of traffic accidents, gridlock on a street, and the best routes that are available [11,12].

2.4 Smart Farming

Using robotics, drones, artificial intelligence, smart IoT devices, and other technology to manage crop farms is known as "smart farming." This also contributes to a reduction in the amount of human labour needed while increasing crop quantity and quality. It is preferable to employ blockchain technology for the smart farming system's data security. AI is also useful in forecasting other occurrences, such as the application of fertiliser based on soil conditions, weather patterns, and anticipated crop yield for a given session.

2.5 Safe and secure Healthcare Monitoring

Internet of Medical Things (IoMT) is a collection of smart healthcare applications and equipment that enables smart healthcare. Using various networking protocols, these devices are linked to the healthcare IT systems. By enabling contact between patients and their doctors, this approach has the advantage of potentially lowering the number of needless hospital visits and the strain on healthcare systems. Unfortunately, in such a system, private medical information is transmitted over an open channel, making it vulnerable to attack from several kinds of adversaries. For the safe processing and storage of private medical data, it is therefore preferable to implement blockchain technology. Artificial Intelligence (AI) has the potential to significantly impact several health-related outcomes, such as the likelihood of a heart attack, the effectiveness of a medication for a certain ailment, and diabetic shocks.

2.6 Industrial Automation and Control

It improves manufacturing, industrial, and control tasks with intelligent sensors and actuators. The Industrial Internet of Things helps to make it possible (IIoT). Utilizing

real-time analytics and the capabilities of smart devices, it makes use of the data generated by industrial machines. Not only can intelligent computers capture and analyse data more quickly than people, but they are also adept at communicating vital information that is needed to make appropriate business decisions more quickly. Sensitive data is also handled in this communication environment, and it needs to be safe from any attacks linked to information security. Consequently, data processing may be done safely and securely if we imagine the blockchain system there. Furthermore, the decentralised structure of blockchain can also serve as a safeguard against issues connected to system failure. AI has a significant function in industrial automation and control in the prediction of various connected phenomena, such as the state of equipment and tools that are being used [10].

2.7 Smart Cities

A municipality that employs information and communications technology (ICT) to improve citizen welfare and government service quality, as well as to share information with the public, is referred to as a smart city. In addition to fostering economic growth, it maximises a city's numerous functional functions. It uses a variety of deployed smart IoT sensors, associated tools and technologies, and data analysis techniques to enhance the quality of life for its residents. Data can be gathered inside a smart city from a variety of sources, including people, things, structures, and assets. Further processing and analysis of this data is done in order to monitor and manage issues related to traffic, power plants, utilities, water supply, waste management, crime prevention and detection, healthcare, and other community services.AI and blockchain technology can both be crucial to the safe and dependable operation of a smart city. Data can then be processed securely if the blockchain protocol is implemented there. Once more, when discussing the larger domain—that is, a smart city—the decentralised character of blockchain can also be useful in preventing issues linked to system failure. AI may also be very helpful in the data analysis process, which is one of the key components of a smart city.

2.8 E-Commerce

Blockchain-envisioned Businesses in the eCommerce industry benefit from AIoT through improved product positioning, improved vendor relationships, automated invoicing and billing, and the creation of real-time information about shipment deliveries. This communication environment's data analysis and storage, however, are not secure. It is therefore preferable to retain it in the form of a blockchain over a peer-to-peer cloud server network, where all of the data can be saved as encrypted transactions inside of different blocks, which are then connected by a hash chain. This kind of architecture can defend against several kinds of information security-related

attacks on the data and related processes.

2.9 Logistics Operations and Control

Supply chain optimization and inventory management are two tasks that AIoT can handle. Smart Internet of Things sensors and associated devices are able to predict when an item will run out of stock and automatically replenish the inventory based on demand. It also makes delivery modules and commercial fleets safer and more efficiently operated. The many users and equipment involved in logistical operations and control must communicate with one another, and these entities do so via the public channel. Nevertheless, a variety of assaults connected to information security could target this open channel. This communication environment's data analysis and storage are therefore unsafe. It is therefore preferable to keep it in the form of blockchain, which can defend the linked processes and data from different kinds of attacks.

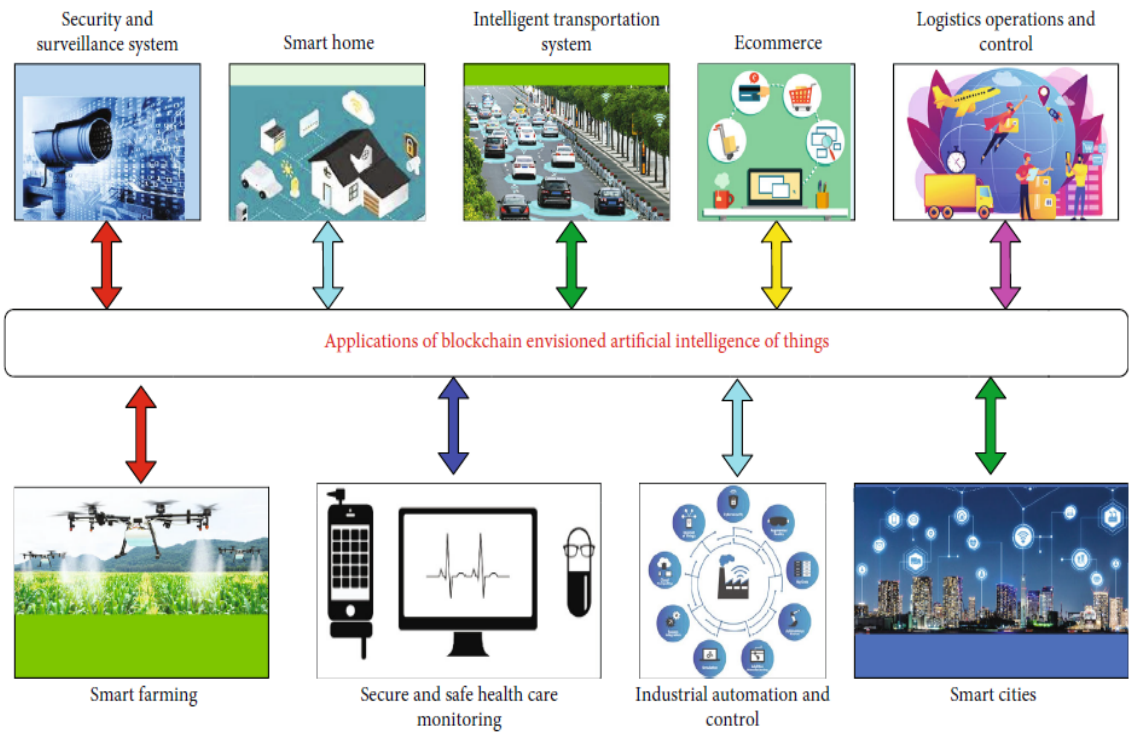

Figure 3. Applications of AIoT Inspired by Blockchain

3. Problems and Difficulties with the Secure Authentication Framework for AIoT Envisioned by Blockchain

As mentioned previously, there are several uses for the blockchain-envisioned safe

authentication architecture for AIoT. But it also faces a number of problems and difficulties concurrently. Below is a discussion of a few probable problems and obstacles.

3.1 Scalability

It's never easy to manage an expanding number of IoT devices and users. A variety of intricate algorithms connected to blockchain consensus, AI-based analysis, and IoT connectivity are used in the safe authentication framework for AIoT that the blockchain has envisioned. The average number of transactions has increased in tandem with the growth in both the number of people and devices. Because more users and devices require more computers and storage, it significantly impacted the transaction processing speed. It results in the overall design of a laborious system. As such, scalability presents a difficult issue in this specific setting.

3.2 Information Security Issues

IoT devices work with subpar software most of the time, which leaves them vulnerable to many types of vulnerabilities. The failure of authentication and access control systems, software attacks, malware infiltration, and inadequate cryptography usage make smart IoT devices susceptible. Certain information security-related attacks, such as "replay," "man-in-the-middle (MiTM)," "impersonation," "credential leakage," "illegal session key computation," "data alteration," and "data exposure," might also affect a blockchain-envisioned safe authentication framework for AIoT. Another problem with the blockchain's process is that it lacks governmental oversight, which creates a volatile atmosphere and makes it simple for market manipulation [13, 14].

3.3 Privacy

A key element of the blockchain-envisioned secure authentication architecture for the Internet of Things is blockchain. Everybody can see the ledger, which is open. In certain situations, it is a necessary necessity. When used in a delicate setting, like the healthcare industry, it can, nevertheless, occasionally become a liability. As such, the ledger needs to be modified such that access is restricted to those who are permitted and not to everyone else. But these kinds of problems can be resolved by utilising several blockchain categories; private blockchain, for instance, is the better option if we require further privacy. IoT devices also need to share data securely over the Internet in order to prevent hackers from taking advantage of it, in order to meet the intended privacy aims. And so, in order to prevent data leaks, IoT devices ought to be required to share data using the finest encryption methods, such as AES, RSA, and ECC [15, 16].

3.4 Issues with Accepting the Technologies

Three key components—Blockchain, IoT, and AI—allow the blockchain-envisioned safe authentication framework for AIoT. Consequently, there's a potential that investors won't want to support such initiatives, or some early adopters may have had unpleasant experiences. With time, these kinds of problems can be resolved, though. People will eventually come to appreciate these technologies' benefits and begin to adopt them.

3.5 Computing Power

Three key elements are required for the blockchain-envisioned safe authentication framework for AIoT to function: blockchain, IoT, and AI. The implementation of this system involves a number of intricate and resource-intensive techniques, such as deep learning and consensus algorithms, which could cause issues for the company handling these kinds of projects. These kinds of systems generate enormous amounts of data, so we need a lot of processing power and storage to keep them running well. Because of this, we must use resource-rich gadgets, which could be highly expensive for some enterprises with tight budgets.

3.6 Issues with Accepting the Technologies

Three key components—Blockchain, IoT, and AI—allow the blockchain-envisioned safe authentication architecture for AIoT to function. Consequently, there's a potential that investors won't want to support such initiatives, or some early adopters may have had unpleasant experiences. With time, these kinds of problems can be resolved, though. People will eventually come to appreciate these technologies' benefits and begin to adopt them.

3.7 Problem of Biasing

There may be some possibility of biassing because AI is used to support the blockchain-envisioned secure authentication framework for AIoT. AI systems generally have this issue: they are only as excellent or horrible as what they have been educated to be. To find out who has been approved for a loan and who has been contacted for an interview, for instance, certain methods are employed. We also make important but unacknowledged decisions if the algorithms are biassed. This could also have unethical and unfair outcomes; for example, the algorithm may have predicted that this specific man will suffer a catastrophic heart attack, even if he is perfectly healthy. As a result, the training process and the dataset that are available to these systems determine everything. Therefore, we should take every effort to resolve these problems. The system's accuracy and correctness should always be improved, according to the developer.

3.8 Legal Issues

Legal challenges may arise for the blockchain-envisioned safe authentication architecture for the Internet of Things. Distinct nations have different regulations pertaining to data security and privacy. Blockchain is still in its early stages of implementation in certain nations, and many government bodies are striving to create laws governing things like what is permitted and what is not. Thus, there ought to be a few strict and unified laws. Furthermore, this type of technology handles confidential information that can violate national or state regulations. An organisation must thus exercise caution on any perceived effects that might harm the organization's reputation.

4. Future Research Directions

As was previously said, the blockchain-envisioned secure authentication framework for AIoT offers a variety of applications. But there are also certain restrictions and difficulties. Future Research needs to be done in order to find solutions to these problems.

5. Research Gap and Analysis

We've already covered a number of applications where AIoT frameworks can be very helpful. However, because there are information security-related assaults, AIoT frameworks might have problems with data security and privacy. The article presents a blockchain-envisioned safe authentication architecture for the Internet of Things. Most possible risks associated with this type of communication environment are covered by the adversary model that is provided. There is additional discussion of the suggested framework's numerous applications. Furthermore, the proposed framework's various problems and difficulties are emphasised. In addition, we offer a few avenues for future research pertaining to the suggested framework that warrant further investigation.

Conflicts of Interest

The authors declare no conflict of interest.

References

[1] Z. Xiong, Z. Cai, D. Takabi, and W. Li, “Privacy threat and defence for federated learning with non-i.i.d. data in AIoT,” IEEE Transactions on Industrial Informatics, p. 1, 2021.

[2] C.-J. Chen, Y.-Y. Huang, Y.-S. Li, C.-Y. Chang, and Y.-M. Huang, “An AIoT based smart agricultural system for pests’ detection,” IEEE Access, vol. 8, pp. 180750–180761, 2020.

[3] X. Zhang, M. Hu, J. Xia, T. Wei, M. Chen, and S. Hu, “Efficient federated learning for cloud-based AIoT applications,” IEEE Transactions on Computer-

Aided Design of Integrated Circuits and Systems, 2020.

[4] S. Russell and P. Norvig, Artificial Intelligence: A Modern Approach, Pearson, London, UK, 2021.

[5] K. F. Lee, AI Superpowers China, Silicon Valley, and the New World Order, Houghton Mifflin Harcourt, Boston, New York, USA, 2018.

[6] A. Barto and R. S. Sutton, Reinforcement Learning: An Introduction, The MIT Pres, Cambridge, Massachusetts US, London, UK, 2014.

[7] T. Poongodi, A. Rathee, R. Indra Kumari, and P. Suresh, "IoT sensing capabilities: sensor deployment and node discovery, wearable sensors, wireless body area network (WBAN), data acquisition," in Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm. Intelligent Systems Reference Library, S. L. Peng, S. Pal, and L. Huang, Eds., vol. 174, pp. 127–151, Springer, Cham, 2020.

[8] K. L.-M. Ang and J. K. P. Seng, "Application Specific Internet of Things (ASIoTs): taxonomy, applications, use case and future directions," IEEE Access, vol. 7, pp. 56577–56590, 2019.

[9] S. S. Seshadri, D. Rodriguez, M. Subedi et al., "IoT Cop: a blockchain-based monitoring framework for detection and isolation of malicious devices in Internet-of-Things systems," IEEE Internet of Things Journal, vol. 80, no. 5, pp. 3346–3359, 2021.

[10] Y. Lu and L. D. Xu, "Internet of Things (IoT) cybersecurity research: a review of current research topics," IEEE Internet of Things Journal, vol. 60, no. 2, pp. 2103–2115, 2019.

[11] M. Zichichi, S. Ferretti, and G. D'Angelo, "A framework based on distributed ledger technologies for data management and services in intelligent transportation systems," IEEE Access, vol. 8, pp. 100384–100402, 2020.

[12] P. Dass, S. Misra, and C. Roy, "T-safe: trustworthy service provisioning for IoT-based intelligent transport systems," IEEE Transactions on Vehicular Technology, vol. 690, no. 9, pp. 9509–9517, 2020.

[13] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: present and future challenges," IEEE Internet of Things Journal, vol. 50, no. 4, pp. 2483–2495, 2018.

[14] D. Jeong, "Artificial intelligence security threat, crime, and forensics: taxonomy and open issues," IEEE Access, vol. 8, pp. 184560–184574, 2020.

[15] A. Alwarafy, K. A. Al-Thelaya, M. Abdallah, J. Schneider, and M. Hamdi, "A survey on security and privacy issues in edgecomputing- assisted Internet of Things," IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4004–4022, 2021.

[16] L. Ye, Z. Wang, Y. Liu et al., "The challenges and emerging technologies for low-power artificial intelligence IoT systems," IEEE Transactions on Circuits and Systems I: Regular Papers, pp. 1–14, 2021.