IoT Security: AI Blockchaining Solutions and Practices

Hephzibah Rajan
Department of Computing and Engineering
Quinnipiac University
Hamden, Connecticut
hephzibah.rajan@quinnipiac.edu

John Burns
Department of Computing and Engineering
Quinnipiac University
Hamden, Connecticut
john.burns@quinnipiac.edu

Chetan Jaiswal
Department of Computing and Engineering
Quinnipiac University
Hamden, Connecticut
chetan.jaiswal@quinnipiac.edu

2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC) | 979-8-3503-3286-5/23/$31.00 ©2023 IEEE | DOI: 10.1109/CCWC57344.2023.10099111

***Abstract*—The IoT market is continuously expanding, and security measures parallel to the growing industrialization has drawn the research community's attention. While several works have focused on the different technologies used to protect IoT devices, this paper aims to narrow the focus to Blockchain and Artificial Intelligence (AI) solutions for security and privacy issues faced by these devices. These technologies address two major vulnerabilities with edge devices on IoT networks: centralization and weak edge nodes. Blockchain provides a distributed system that can help avoid a single-point failure and can be used to optimize battery life on low-level devices by load balancing. On the other hand, AI's power to learn and adapt is critical to automate systems and make them intelligent enough to analyze collected data. The combination of these two technologies is capable of mitigating multiple challenges IoT architectures face currently. The paper discusses the latest major architectures that integrate Blockchain and AI to enhance security within the. This paper also presents the comprehensive take on the device security and drawbacks to these mechanisms. This work also addresses the future of security in IoT and suggests different areas that need further work to better comprehend how the combination of these technologies can assist in enhancing security.**

Keywords—IoT, security, Blockchain, Artificial Intelligence, Machine Learning, privacy, decentralization, edge devices

I. INTRODUCTION

The Internet of Things (IoT) market, a network of devices that communicate and exchange data with each other, has expanded over the last decade. IoT devices provide different applications such as health care, smart homes, wearables, and smart cities. The advent of a wide range of devices requires security that matches its capabilities to ensure the safety of the system and network. The number and type of attacks carried out against IoT devices have increased exponentially. As the need for faster and more efficient devices increases, there is a lag in equal breakthroughs in IoT security. According to Business Insider's 2020 IoT research, IoT devices are predicted to increase to 41 billion by 2027 [1].

In order to meet this challenge, we must focus on the security strategies that match IoT devices' hardware and computational power to minimize internal or outsider attacks.

Traditional IoT networks have always faced three big challenges: centralization, big data analytics and security. Blockchain has been used in IoT devices to explore novel security needs and provide a decentralized and distributed system. Blockchain is a powerful tool as evident by its use in Bitcoin and other cryptocurrencies for security and privacy. Blockchain is a distributed database, often called ledgers, that connects different systems together using a peer-to-peer (P2P) network. Every computer on the blockchain contains the entire content of the blockchain, making it computationally infeasible to make malicious widescale changes to it. Each node of the blockchain contains two parts: the header and the body. The header contains metadata such as a timestamp, hashes of the block's data, and the previous block's header information. The body is the core data of the node that is being protected, this can range from medical records to monetary transactions [2]. There are two types of blockchains: public and private. In public blockchains, there can be an unlimited number of anonymous users adding to the blockchain and they can read from and write to it, however, public blockchains are energy intensive and wasteful. Private blockchains are more selective in which users they let in; they must be authenticated. Thus, read and write permissions to the ledger are restricted to authorized users while the owner of the blockchain has total control of the system [3]. An example of Blockchain and IoT technologies is Telstra, which is a smart home company that includes biometric data, blockchain, and IoT to prevent unwanted intrusions [4]. Integrating blockchain technology in IoT security tackles the centralized architecture that most IoT devices have, which causes them to be vulnerable to a single point of failure.

The internet is a vast source of information and is constantly generating enormous amounts of data. IoT devices need to process this data and more often than not, has proved to be incapable of big data analysis. Artificial Intelligence (AI) is capable of mitigating this challenge. The field of Machine Learning (ML) and AI has grown over the past decades from understanding patterns in large datasets to self-driving cars. AI

is an umbrella term that covers multiple concepts such as Deep Learning (DL) and ML and uses them to build machines that can learn from the large amount of data provided to predict the behavior of future data. AI is used in multiple applications such as Google Assistant, Amazon Alexa and in different industries for fraud prevention, personalized advertisements, and spam filtering. An example of ML and IoT coming together is monitoring vehicle health. Intangles is a company that specializes in this area, predicting when problems will arise to be proactive in fixing them [5]. AI methods can help with substantial amounts of data since it provides hybrid algorithms based on decision trees and statistical approach. The combination of these technologies is powerful and can address the accuracy, latency, security and privacy of large-scale IoT devices.

In this paper, we provide different research works and solutions that use a combination of blockchain and AI/ML to address security and privacy issues. This paper provides a relative benchmark for a fundamental understanding of security in IoT and how the use of blockchain in conjunction with AI can improve it. We will further dive into the benefits and limitations of the innovative schemes that have been proposed. Finally, the article will discuss the future of IoT security and the grounds for improvement in designs that use AI and Blockchain.

This paper is organized as follows: in section II, we discuss the role of AI and blockchain in IoT. In section III, we delve into how the combination of the above technologies are used to improve security in IoT networks. In section IV, we present past work that has used AI-driven Blockchain and Blockchain-driven AI in IoT applications. Additionally, we discuss the challenges and solutions the algorithms or schemes provide. In section V, we provide topics that need to be investigated in the future for further research. In section VI, we conclude our research and finally, in section VII, a list of the abbreviations used in this work is provided.

II. DEFINING THE ROLE OF AI AND BLOCKCHAIN IN IOT

A. Blockchain in IoT Devices

Blockchain is a collection of data in blocks connected to each other. Each block holds details of the transaction, its own hash and the previous block's hash and the timestamp of the transaction. Due to the data in a block, a third person will be unable to alter the record without disturbing the entire chain. Blockchain technology goes beyond cryptocurrency and distributed data storage: for instance, it offers on-demand scalability. With the millions of messages sent across the network every second, delays are inevitable and can cost people time and money. By having a peer-to-peer system, these delays are minimized as the requests are spread out over a larger area. In addition, blockchain is compatible with several different IoT devices. This allows deprecated devices to continue to run on the system while new updated devices can share and join the same network.

Blockchain technology is the state-of-the-art solution for privacy. Many different approaches are used to preserve privacy, one being pseudonyms to reduce the likelihood that one's real identity is leaked. A more prominent approach is that all the users have a copy of the entire ledger. Hence, a malicious user can only make changes to the ledger if they are able to change 51% of the nodes holding the ledger: this has been proven to be computationally infeasible [6].

B. AI/ML in IoT Devices

IoT devices, in most cases, act as data-collection end points. Very rarely are they capable of comprehending the data or analyzing it. The components of any IoT network are capable of moving data, but they are not designed to process massive amounts of data efficiently. That essentially depends on the device's ability to automate and adapt [7]. The primary goal of an efficient IoT device is to sense/read data and transfer it to an IoT gateway or edge device where data is sent to the cloud to be analyzed or analyzed locally. AI/ML can dramatically improve this process by automating IoT devices to behave independently without human assistance. In addition, it can also make such devices adaptable to the changing environment to accept new parameters and react better to new test cases: hence smarter.

AI uses hybrid algorithms using decision trees and statistical approaches to process this data efficiently. This can reduce the amount of data on the IoT network since the devices are selective and adaptable to the changing environment. Figure 1 shows how data is moved from the local devices to a larger database [8]. The raw data is processed and stored in an organized manner in a data lake [1]. AI/ML uses algorithms to learn and provide feedback to ensure data refinement. This can help avoid fraud and fake data collection from the devices which consequently helps improve system security. Therefore, AI can optimize feedback learning for attack predictions and deploying smart key management systems [8].

III. DEFINING THE ROLE OF AI AND BLOCKCHAIN IN IOT SECURITY

A. Blockchain in IoT Security

All the benefits of Blockchain can be applied to IoT security in resulting in major paradigm shift. Blockchain has the potential to fill in the gaps that are apparent in the current IoT network set up and strengthen the parts of the network that work. Blockchain really shines when it comes to data integrity, however with the limited processing power on smaller IoT devices it is infeasible to run a complete Blockchain on that device.

One solution to this is to have a hierarchy of devices with sensors as the leaf nodes. The devices a level above wouldn't be the sensors but machines with relatively higher capabilities that could handle the power consumption requirements of a blockchain. This approach leaves the data in the leaf devices more open to attack, so it would not be ideal for devices carrying data such as medical information, but for less private data such as temperature sensors, this solution would work [8].

Another solution would be to have p higher capability devices among n ($\in p < n$) on a network. These high-power devices would implement the blockchain, leaving the rest of the IoT devices as data collection nodes. This approach provides a greater sense of security as all the devices would be on the same network level. This also allows for increased security when the data is forwarded up a level, making it a better solution for sensitive information like medical data [9].

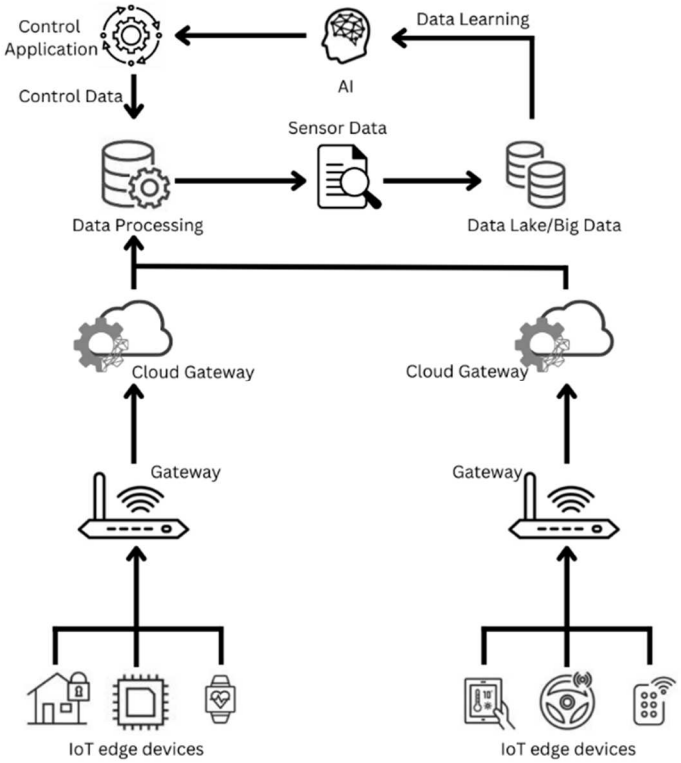

Figure 1: Flow of data from edge devices to databases

B. AI/ML in IoT Security

In IoT security, AI can be used to build smarter devices by automating the data processing and comprehension at the device's level rather than conventional IoT networks where the devices are mere raw data-collection endpoints. However, from the perspective of security, this raises a wide variety of security issues that outsiders can exploit. Wu's [10] work shows that there are four main security threats in IoT devices that need to be addressed urgently: device authentication, DoS/DDoS attack, intrusion detection and malware detection. Standard solutions to these challenges cannot match the size of the data sets nor are they efficient. AI rises to this challenge and uses ML methods to help detect and categorize future attacks by making predictions of unknown events.

According to [10] the current AI solutions for privacy and security issues have six standard steps, as: 1) data collection, 2) data pre-exploration and pre-processing, 3) model selection, 4) data conversion, 5) training and testing, and 6) model evaluation and deployment. On a higher level, the process is as follows:

- Data is collected from different IoT devices in specific environments and separated into training and testing data sets.
- The collected data is mined for outliers or incomplete data entries. It is cleaned to delete errors and prepare the data for further processing.
- An ML model is selected based on the model and the characteristics of the data. Different models are used based on the size and pre-exploration results of the data.
- Once a model is selected, the collected data is converted to meet the model's standards.
- Now that the data is prepped and we have a model, the model is trained. When the model achieves optimization, it is tested using test datasets from the real world. Depending on the test results, models have to be adjusted further.
- Effect indicators are used on all the trained models to decide the final model that will be deployed.

The above mentioned steps are used to help AI-powered devices to differentiate between authenticated and unauthenticated users, classify between normal and abnormal networks, detect malware, identify DoS/DDoS attacks and multiple other security measures.

IV. EXISTING BLOCKCHAIN AND ML BASED SOLUTIONS FOR IOT SECURITY

There are numerous authentication protocols and security schemes, some of which are discussed here. The following four works propose the integration of Blockchain and AI technologies to secure devices on IoT networks. This section describes the architecture, analyzes it and discusses the strengths and potential enhancements. Table 1 summarizes the features, advantages, and shortcomings of the following four works.

A. Custom Blockchain with Software-Defined Network Authentication Mechanism

Latif et al. [11] proposed a solution that is a customized blockchain where the Software-Defined Network (SDN) controller provides a distributed authentication mechanism in each SDN domain. IoT devices register themselves to a ledger and the SDN controller manages that ledger. This enhances security by keeping out non-authenticated nodes and reduces energy requirements on the IoT devices. The controller controls the communication it its respective domain, which reduces network delay and reduces wasted computational power (for redundant overhead). In this work, public and private blockchains are used; public for inner and outer domain security, and private for IoT devices in their respective domain. They ran an experiment comparing this solution to different routing protocols, mainly: AODV, DSDV, SMSN, EESCFD, and AOMDV, and their solution had improved throughput, less delay and less energy consumption. This solution has not been created only simulated, so there could be discrepancies between the theoretical and practical applications of this system.

B. *Blockchain-Based Framework for Medical Data on IoD equipped with AI for Data Analysis*

Wazid et al. [12] analyzed and built a framework that deals with the Internet of Drones (IoD), which is a subcategory of IoT. This framework is a blockchain based solution that uses AI to analyze data. This work proposed a security system for drones in the medical field. The premise of their framework is that there is a ground station server (GSS) and a control room (CR) that act as the controllers. The drones can communicate to the GSS and to other neighboring drones in their zone. This medical data is then made available to the cloud servers in a P2P connection. These cloud servers will run a private blockchain and allow AI/ML algorithms to run on them as well, allowing predictions to be extrapolated from the data. This solution never considered the energy requirements that will be needed to run their Blockchain. Based on this paper, the solution is a proof of concept but does not show that it is feasible to implement in reality.

C. *Bio-inspired algorithm based on AI and Blockchain for secure communications over IoT networks*

This framework proposed by [13] uses AI and Blockchain for separate purposes: 1) secure communication provided by blockchain technology and 2) AI to monitor the blockchain-enabled IoT communication network. The communication network is divided into a decentralized multi-layer security network, consisting of an infrastructure design layer, cluster creation and cluster head selection layer, blockchain-based security design layer.

The infrastructure design layer is further divided into layers, specifically three layers: kernel level, high level and foot level. The kernel level holds the controlling agents while the high and foot level have the base stations and sensor nodes respectively. The infrastructure layer, consisting the IoT network, is split into clusters using unsupervised clustering techniques. In the cluster creation and cluster head section layer, clusters are grouped together to create cluster headsets. A cluster head (kernel level) is selected from within a cluster based on Particle Swarm Optimization (PSO) and Genetic Algorithm (GA). This is advantageous as cluster-based algorithms help reduce the number of large-area transmission nodes between base station, thus saving electricity and distance-based expenses. Clustering helps reduce latency and overhead in the network. The algorithms employed in this work also help distribute energy and increase the network's life.

At the blockchain-based security design layer, lightweight sessions keys are assigned by cluster heads to the local authentication nodes. The cluster head uses a Local Authority Program and symmetric keys to authorize and authenticate other locally registered computers. Additionally, they send and receive data to upper layer using the localized blockchain in place. In addition to registering a new entity and managing nodes, cluster heads and base stations are also responsible for managing and protecting communication, connecting within the cluster, and distributing blocks, thus ensuring security and privacy within the network. Base Stations are the highest standard level and contain a distributed way. A global blockchain solution will be introduced along with more complex authentication systems in this layer.

The proposed communication network framework was monitored using AI for analysis. AI tracks the communication within the IoT network. The authors propose a recurrent neural network (RNN) to learn the difficulties of the network.

The work is a theoretical proposal and may not behave the same in a practical setting. Although AI concepts are proposed in the work, it has not been implemented in the architecture. Therefore, it raises the question as to whether AI is even feasible in this system.

D. *Protecting Edge Layer Devices using AI/ML and Blockchain HDPoA Protocol*

The authors in [14] proposed a system architecture consisting of four layers: sensing layer, network layer, processing layer and sharing platform. Sensing layer consists of all the small IoT devices. Network layer is the communication link i.e., Wi-Fi or LoRaWAN. Sensing layer holds the AI engine, and the sharing platform is the freely accessible and public blockchain platform. These layers are necessary for the system to carry out the platform's main operations as listed below:

- Monitoring and collection – IoT system monitors the environment and uses devices at the lowest layer to collect data. The sensing layer helps the most with this step.
- Analysis and prediction – Collected data is moved to intelligent nodes for analysis. This happens in the processing layer.
- Sharing – Analyzed data is shared with all nodes on the system. This occurs after the data results are passed from the processing layer to the sharing platform.

The blockchain protocol used in this work was previously published by the authors [15] and is known as honesty-based distributed proof of authority (HDPoA). HDPoA combines proof of authority (PoA) and proof of work (PoW) and enhances PoA's security by adding PoW-based security layer that relies on honest and scalable work. Based on this protocol and trust levels, devices could either be authority nodes (AN) or worker nodes (WN). WN collect data whereas authority nodes manage the mining process. This protocol has its merits and demerits as discussed in rest of this section.

This architecture holds merits that make it stand apart from other ideas, some being the use of blockchain to authenticate the flow of data between layers. Additionally, it uses trust levels to ensure that the nodes in the IoT system are genuine. This helps when a node is found behaving in a harmful manner. That node will immediately lose all access to the blockchain because of the HDPoA consensus algorithm.

Malicious WN cannot be added to the network since all WN data is authenticated by AN. As for AN, all other AN on the network must validate the data outcome for it to be accepted

and added to the platform. AN cannot produce incorrect AI data either since multiple nodes will be used to perform AI prediction to validate the outcome. Any node found to be acting maliciously will be removed immediately as an AN and have to build its trust levels from zero.

This work brings up two challenges: 1) the authors assume that the network layer is safe and does not suggest a safe communication link for the nodes to exchange data. Therefore, this protocol is only as strong as the network provider. 2) if all the WN on the network are attacked, like in a DDoS flooding attack, the network becomes ineffective and will require a long time to be restored. Since the architecture depends on trust levels, the WN would be removed from the network at the first sign of malicious data. The nodes then would have to re-establish their trust each time they try to connect to the IoT network. This process is repetitive, time consuming and resource intensive. It also leaves the network vulnerable during this process and useless for data collection.

TABLE 1: EXISTING BLOCKCHAIN AND AI SOLUTIONS

Proposed Architecture	**Features**	**Advantages**	**Shortcomings**
Custom Blockchain with Software-Defined Network Authentication Mechanism	Custom blockchains used for data integrity, controllers authenticate IoT devices in their respective domains	Reduced network delay between devices and less computational power used	Has only been simulated not implemented in a real time setting
Blockchain-Based Framework for Medical Data on IoD equipped with AI for Data Analysis	Server and control rooms act as controllers for the drones, drones communicate on a P2P basis, controllers communicate with the cloud which allows AI to analyze the data	Medical data is secured from tampering, predictions can be made on the data which could allow for medical advances	Energy requirements are never stated in the paper, showing only a proof of concept
Bio-inspired algorithm based on AI and Blockchain for secure communications over IoT networks	Decentralized multilayer network: kernel, high and foot level using Local Authority Program with 2 different levels of blockchain	Uneven clustering strategy to distribute energy and increase the network's life	AI might not be a feasible solution for the architecture
Protecting Edge Layer Devices using AI/ML and Blockchain HDPoA Protocol	Custom Blockchain protocol (HDPoA) using trust levels to assign different nodes as authority and worker nodes	Authentication required by authority nodes for entrance to IoT network and the trust levels will block any malicious activity	Building trust between nodes takes time

V. FUTURE PROSPECT FOR SECURITY IN IOT DEVICES

The combination of AI and Blockchain is powerful for IoT networks for several reasons like latency, privacy, security and decentralization. However, most of the proposed architectures are theoretical and have not been used in practical real time scenarios and settings. On the other hand, IoT is continuously growing at a rapid pace and the hardware for lower-level devices is becoming smaller as they become more efficient. Data processing using AI requires enormous amounts of computational power that small devices lack. The associated overhead and energy requirements are not cost effective for smaller networks. Such smaller IoT devices are vulnerable to attacks and data leakage. It is a challenge to keep up with the security and privacy needs with the growing innovations in the IoT market. At current pace, the pairing of AI/ML with blockchain is not feasible for the smaller components on an IoT network.

One of the topics that Ahangar et. al. [16] propose for further research in the IoT security field is deep learning methodologies for inferring IoT maliciousness. Based on our review of the works presented in this paper show AI's resiliency and the power it possesses to solve novel data through ML. Past AI projects have shown potential to detect fake data before it attacks the system and further research needs to be conducted to investigate methods and algorithms that can provide this feature for IoT devices, especially edge devices.

Another future prospect for security in IoT is trying to get Blockchain to be more efficient on smaller IoT devices. Some studies reviewed in this paper had to make changes to the Blockchain so as to have one higher-powered device run the Blockchain that other less-powerful devices connect to. This causes a break in security as that information can be intercepted and changed enroute to the device holding the blockchain ledger. Having all devices implement the blockchain would reduce this risk greatly.

VI. CONCLUSION

This paper defined the role that AI/ML and Blockchain have currently in IoT devices, explaining in detail how Blockchain technology works and how AI/ML is used to lessen the computational load on IoT devices. We then talked about Blockchain and AI/ML in IoT security and how having these technologies strengthens privacy, data integrity, and data processing. Four potential solutions were explored and analyzed to understand how they could help deficiencies in the current IoT network setup as well as challenges that were not addressed in the solutions. Finally, future lanes of research were brought up for researchers to study.

This paper presented the role that AI/ML and Blockchain have currently in IoT devices and how these two can work in

tandem to lessen the computational load on IoT devices. The paper then discussed the scope of Blockchain and AI/ML in IoT security towards strengthening privacy, data integrity, and data processing. Then it addresses the vulnerabilities and feasibility of AI/ML and Blockchain towards IoT security. With several potential solutions, four major works were studied. The paper then progresses to analyze these works on several parameters, summarizing them based on their: 1) Feasibility, 2) Security Strength, 3) Applicability and 4) Robustness.

Finally, the paper proposes possible future areas for prospective research and exploration in the field of security in IoT. In the future, researchers need to work on finding a viable solution for smaller edge devices that cannot be automated during hardware restrictions. Studies need to be conducted to learn more about the optimal conditions for minimal hardware and AI to coexist on edge devices to reduce overhead and increase efficiency.

VII. ACRONYM GUIDE

The following table (Table 2) enumerates the acronyms in this paper and their corresponding full forms.

TABLE 2: LIST OF ABBREVIATIONS

Abbreviation	Full Form
IoT	Internet of Things
AI	Artificial Intelligence
ML	Machine Learning
P2P	Peer-to-peer
DL	Data Learning
SDN	Software-Defined Network
AODV	Ad-hoc On-demand Distance Vector
DSDV	Distance Sequenced Distance Vector
SMSN	Secure Mobile Sensor Network
EESCFD	Energy Efficient Secured Cluster based Distributed Fault Diagnosis
AOMDV	Ad-hoc On-demand Multipath Distance Vector
IoD	Internet of Drones
GSS	Ground Station Server
CR	Control Room
PSO	Particle Swarm Optimization
GA	Genetic Algorithm
RNN	Recurrent Neural Network
LoRaWAN	Long Range Wide Area Network
HDPoA	Honesty-based Distributed Proof of Authority
PoA	Proof of Authority
PoW	Proof of Work
AN	Authority Nodes
WN	Worker Nodes
DDoS	Distributed Denial of Service

REFERENCES

[1] L. Q. A. K. S. a. Q. W. Zhihan Lv, "AI-empowered IoT Security for Smart Cities," *Association for Computing Machinery,* vol. 21, no. 4, 2021.

[2] M. T. Hammi, B. Hammi, P. Bellot and A. Serhrouchni, "Bubbles of Trust: A decentralized blockchain-based authentication system for IoT," *Computers & Security,* vol. 78, pp. 126-142, 2018.

[3] S. SETH, "Public, Private, Permissioned Blockchains Compared," Investopedia, 28 July 2022. [Online]. Available: https://www.investopedia.com/news/public-private-permissioned-blockchains-compared/#:~:text=In%20a%20public%20blockchain%2C%20anyone,delete%20entries%20on%20the%20blockchain.. [Accessed 13 October 2022].

[4] C. Reichert, "Telstra explores blockchain, biometrics to secure smart home IOT devices," ZDNET, 22 September 2016. [Online]. Available: https://www.zdnet.com/home-and-office/networking/telstra-explores-blockchain-biometrics-to-secure-smart-home-iot-devices/. [Accessed 20 February 2023].

[5] "Prognostic, Diagnostic & Digital Twin Solution for Fleets," [Online]. Available: https://www.intangles.ai. [Accessed 20 02 2023].

[6] A. I. A. A. M. A. T. A. E. E. H. A. S. A. G. F. K. K. Abdelzahir Abdelmaboud, "Blockchain for IoT Applications: Taxonomy, Platforms, Recent Advances, Challenges and Future Research Directions," *Electronics,* vol. 11, p. 630, 2022.

[7] D. C. A. L. Ashish Ghosh, "Artificial intelligence in Internet of things," *CAAI Transactions on Intelligence Technology,* vol. 3, no. 4, pp. 208-218, 2018.

[8] V. R. Ankit Attkan, "Cyber-physical security for IoT networks: a comprehensive review on traditional, blockchain and artificial intelligence based key-security," *Complex & Intelligent Systems,* vol. 8, pp. 3559-3591, 2022.

[9] B. O. Daniel Minoli, "Blockchain Mechanisms for IoT Security," *Internet of Things,* Vols. 1-2, pp. 1-13, 2018.

[10] H. H. X. W. a. S. S. H. Wu, "Research on Artificial Intelligence Enhancing Internet of Things Security: A Survey," *IEEE Access,* vol. 8, pp. 153826-153848, 2020.

[11] F. B. X. W. C. I. L.-l. F. W. S. M. M. Z. H. S. S. B. Sohaib A. Latif, "AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems," *Computer Communications,* vol. 181, pp. 274-283, 2022.

[12] M. Wazid, B. Bera, A. Mitra, A. K. Das and R. Ali, "Private Blockchain-Envisioned Security Framework for AI-Enabled IoT-Based Drone-Aided Healthcare Services," *Association for Computing Machinery,* pp. 37-42, 2020.

[13] R. Alroobaea, R. Arul, S. Rubaiee, F. S. Alharithi, U. Tariq and X. Fan, "AI-assisted bio-inspired algorithm for secure IoT communication networks," *Cluster Computing,* vol. 25, pp. 1805-1816, 2022.

[14] S. M. Alrubei, E. Ball and J. M. Rigelsford, "A Secure Blockchain Platform for Supporting AI-Enabled IoT Applications at the Edge Layer," *IEEE Access,* vol. 10, pp. 18583-18595, 2022.

[15] S. Alrubei, E. Ball and J. Rigelsford, "Securing IoT-Blockchain Applications Through Honesty-Based Distributed Proof of Authority Consensus Algorithm," *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA),* pp. 1-7, 2021.

[16] T. A. Ahanger, A. Aljumah and M. Atiquzzaman, "State-of-the-art survey of artificial intelligent techniques for IoT security," *Computer Networks,* vol. 206, no. 108771, 2022.