Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 3866006, 19 pages
https://doi.org/10.1155/2021/3866006

Review Article

Blockchain-Envisioned Secure Authentication Approach in AIoT: Applications, Challenges, and Future Research

Mohammad Wazid,[1] **Ashok Kumar Das**,[2] **and Youngho Park**[3]

[1]*Department of Computer Science and Engineering, Graphic Era Deemed to Be University, Dehradun 248 002, India*
[2]*Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500 032, India*
[3]*School of Electronics Engineering, Kyungpook National University, Daegu 41566, Republic of Korea*

Correspondence should be addressed to Youngho Park; parkyh@knu.ac.kr

Received 18 June 2021; Revised 25 July 2021; Accepted 8 September 2021; Published 7 October 2021

Academic Editor: Jose Santa

The Artificial Intelligence of Things (AIoT) is the amalgamation of Artificial Intelligence (AI) methods and the Internet of Things (IoT) infrastructure, which are deployed there to improve the overall performance of the system. AIoT can be deployed to achieve more efficient IoT operations; thereby can improve human-machine interactions and provide better data analysis. AI methods can be used to transform IoT data into useful information for the better decision-making processes, and it further increases the overall usability of the system. AIoT frameworks are very useful and applicable in a variety of applications, like security and surveillance system, smart home, intelligent transportation system, smart farming, secure and safe healthcare monitoring, industrial automation and control, eCommerce, logistics operations and control, and many more. However, AIoT frameworks may have issues related to data security and privacy as they are vulnerable to various types of information security-related attacks. These issues further cause the serious consequences, like the unauthorized data leakage and data update. Blockchain is a specific type of database. It is a digital ledger of transactions, which is duplicated and distributed across the entire network of computer systems. It stores data in the form of some blocks, which are then chained together. Blockchain is tamper proof and provides more security as compared to the traditional security mechanisms. Hence, blockchain can be integrated in various AIoT applications to provide more security. A generalized blockchain-envisioned secure authentication framework for AIoT has been proposed. The adversary model of blockchain-envisioned secure authentication framework for AIoT is also highlighted that covers most of the potential threats of a kind of communication environment. Various applications of the proposed framework are also discussed. Furthermore, different issues and challenges of the proposed framework are highlighted. In the end, we also provide some future research directions relevant to the proposed framework.

1. Introduction

AIoT is the combination of Artificial Intelligence (AI) methods and Internet of Things (IoT) infrastructure. As we know, IoT is about different "Things" (i.e., smart IoT devices), which are connected to various users through the Internet [1–3]. AI provides methods to train the devices so that they can understand the novel data based on the training procedure that they have completed. AIoT works for a common goal, which is the generation of useful data about the world through IoT devices and drawing of useful insights from the collected data through some AI methods [4–9]. Artificial Intelligence (AI) refers to any human-like intelligence manifested by a machine, i.e., a computer and a robot. It is the ability of a machine, which mimics like the learning capabilities of the human, i.e., learning from the experience, object recognition, decision-making, and problem solving. It is an interdisciplinary science with multiple methods and tools, especially the advancements, which happen due to machine learning

and deep learning creating a paradigm shift in various sectors of the tech industry [10–14].

1.1. Common AI Technologies. The following are the common AI technologies [1–3, 15–19]:

(i) Speech recognition: speech recognition mechanism is used to convert and transform human speech in some useful format so that a computer application can process it. The "transcription and transformation of human language" into some useful format is in demand these days.

(ii) Natural language processing (NLP): it focuses on the interactions between computers and human languages. Text analysis methods are used to analyse the structure of sentences and their interpretation through the ML algorithms. NLP is also helpful for the fraud detection systems. Automated assistants and applications derive unstructured data through NLP.

(iii) Image recognition: it is the process of identification and detection of features in a video or an image file. It further facilitates the process of image searches for example, detecting license plates and diagnosis of diseases.

(iv) Machine learning platforms: it is a subdiscipline of computer science and the important part of AI. The motive is to develop new mechanisms to enable the learning of computer systems to make them more intelligent. With the deployment of various algorithms, application programming interface (APIs), training tools, big data analytics, and machine learning platforms become popular these days, which are used for the purpose of categorization and predictions. The organizations like Amazon, Fractal Analytics, Google, and Microsoft provide various ML platforms as per the requirements of the customers.

(v) Decision management: due to the AI logic and capabilities, machines can be used for training and maintenance. For adding value to the business and to make it more profitable, decision management system is being used. With the deployment of ML-based mechanisms, these systems execute automated decision.

(vi) Deep learning platforms: the deep learning (DL) techniques use artificial neural networks. DL is another form of ML, which duplicates the neural network of human brain to process the data and draw patterns from this. These patterns are further used in the decision-making process. Some of the applications of DL are speech recognition system, image recognition system, and prediction system, which can predict about any phenomena of the digital sphere. Some of the DL platforms providers are Deep Instinct, Ersatz Labs, Fluid AI, and MathWorks.

(vii) Robotic process automation: robotic process automation depicts the functioning of corporate processes, which automate the process through the mimicking of human activities and tasks. However, it is essential to mention that AI is not there to replace the humans, but to support and complement their skills and associated tasks. The organizations like automation anywhere, blue prism, and WorkFusion are working in this domain

(viii) Cyber security: it is a computer defense mechanism, which detects and defends the various information security-related attacks happening in the cyber space. Neural networks, which have the ability to process sequences, can be deployed with ML techniques to create learning technologies for the mitigation of cyber attacks.

(ix) Marketing automation: these days, AI is also going famous for marketing automation, especially to predict about the market trends, offers, and customers' mood. That happens because of the advantages it put into the domain.

(x) Virtual agents: a virtual agent can be a computer agent or a program, which has the ability of interaction with humans. It is used in customer service's system via chat bots. The organizations like Apple, Google, Amazon, and Microsoft provide support through virtual agents.

1.2. Categories of Machine Learning Algorithms. The different categories of machine learning algorithms are given below.

1.2.1. Supervised Learning Algorithms. This class of algorithm uses labeled data to learn (training). There is a mapping function that turns input variables α into the output variable β. In other words, it solves function f as per the following equation:

$$\beta = f(\alpha). \tag{1}$$

Supervised learning algorithms are further divided into three categories, i.e., classification, regression, and ensembling.

(1) Classification: in this method, variables are in the form of certain categories, and then, there is a prediction about the outcome of the given sample. A classification model might look at the input data and try to predict labels for example, in case of cyber attack detection, threat, or normal flow.

(2) Regression: there are another categories of algorithms, which come under regression, which is used to predict the outcome of the given sample, in case when output variables are in the form of real values. A regression method may be used to process input data for the prediction of amount of rainfall and temperature in a specific week of a month.

(3) Ensembling: for this particular category, a combination of different algorithms is used to produce better results, i.e., "Bagging with Random Forests" and "Boosting with AdaBoost."

"Linear Regression, Logistic Regression, CART, Naive-Bayes, and K-Nearest Neighbors (KNN)" are examples of supervised learning algorithms.

1.2.2. Unsupervised Learning Algorithms. These algorithms are used when only one input variable (X) is there and no corresponding output variables. The unlabeled training data is used to model the underlying structure of the data. Unsupervised learning algorithms are further divide into three categories, i.e., association, clustering, and dimensionality reduction. Their details are as follows:

(1) Association: this method is used to find out the "probability of the cooccurrence of items in a collection." Most of the time this technique is used in market-basket analysis. For example, it can be used to find out if a customer purchases shirt, he/she is 80% likely to also purchase trouser.

(2) Clustering: this method is used to group samples such that objects in a cluster are more similar to each other than to the objects in the other clusters, i.e., K-means and clustering algorithm.

(3) Dimensionality reduction: in unsupervised learning, there is another approach called as dimensionality reduction, which is used to reduce the number of variables of a dataset without omitting the important information. This can be done through "feature extraction methods" and "feature selection methods." Feature selection mechanism selects a subset of the original variables whereas feature extraction does data transformation from a "high-dimensional space" to a "low-dimensional space." Algorithm Principal Component Analysis (PCA) comes under feature extraction approach.

Algorithms like Apriori, K-means, and Principal Component Analysis (PCA) are examples of unsupervised learning.

1.2.3. Reinforcement Learning. It is the another category of ML algorithms, which allows an agent to decide the next best action to be performed on the basis of its current state via learning behaviors, which will maximize a reward. These methods learn optimal actions in a trial and error way, for example, a video game in which the player has to move to certain places at certain times to earn more points. The player may correct his/her move on the basis of previous loses attempts. Examples of reinforcement learning algorithms are Q-Learning and State-Action-Reward-State-Action (SARSA).

1.2.4. Deep Learning. Deep learning is another category of ML algorithms, which are inspired by the structure and function of the human brain. They are based on artificial neural networks and representation learning. They are concerned with building much larger and more complex neural networks. Deep learning algorithms are concerned with very large datasets of labelled analog data, i.e., image, text, audio, and video. Some of the popular deep learning algorithms are Generative Adversarial Network (GAN), Convolutional Neural Network (CNN), Recurrent Neural Networks (RNNs), and Long Short-Term Memory Networks (LSTMs). Here, learning can be performed in a supervised or unsupervised way. The different categories of machine learning along with algorithms are also depicted in Figure 1.

Internet of Things (IoT) expresses the network of physical objects also called as "Things," which are embedded with sensors, software, and other related technologies. They are deployed for the aim of connecting and exchanging data with other devices and systems over the Internet. These billions of IoT devices collect and share the data through the Internet all around the world. The connection of all these smart objects, which have inbuilt sensors, provides the level of digital intelligence to them. This enables them to exchange the real-time data without any human involvement. The number of connected IoT devices was 15.41 billion in 2015, which will be increased to 75.44 billion in 2025. The trends of number of connected IoT devices are provided in Figure 2 [20].

The IoT construction consists of four parts: device hardware, device software, communication, and platform. Device hardware deals with the hardware devices like sensors, and networking devices, which connect the IoT systems and devices to the external world via Internet. Device software deals with the different tools and software, which are needed to connect the IoT devices to the other devices (i.e., cloud server, fog server, and gateway nodes) and users. It also provides the graphical user interface to the various users so that they can access the services of the IoT-based systems (i.e., smart home). These softwares provide actual intelligence to the Things; i.e., task like big data analytics can be performed and prediction can be made. Communication layer facilitates the data exchange between the IoT system and the outer world. Communication layer includes physical connection solutions such as mobile, satellite, local area networks, and specific communication protocols such as Message Queuing Telemetry Transport (MQTT) used in different IoT environment. The last important part is the platform layer. It consists of various required platforms, which can collect, manage, process, analyse, and display all data in a user-friendly manner. There are many IoT platforms (i.e., Google Cloud IoT, Cisco IoT Cloud Connect, Amazon, and AWS IoT Core) are in the market, which provide services to the different users as per their demands. The details of these four important components of IoT construction are also provided in Figure 3.

1.3. Layered Architecture of IoT. The layered architecture can be divided into four layers: i.e., device, pipe, cloud, and application. It is also depicted in Figure 4. The functionalities of these layers are given below [21, 22]:

(i) The device layer consists of the details of all smart devices, various sensors, operating system, and

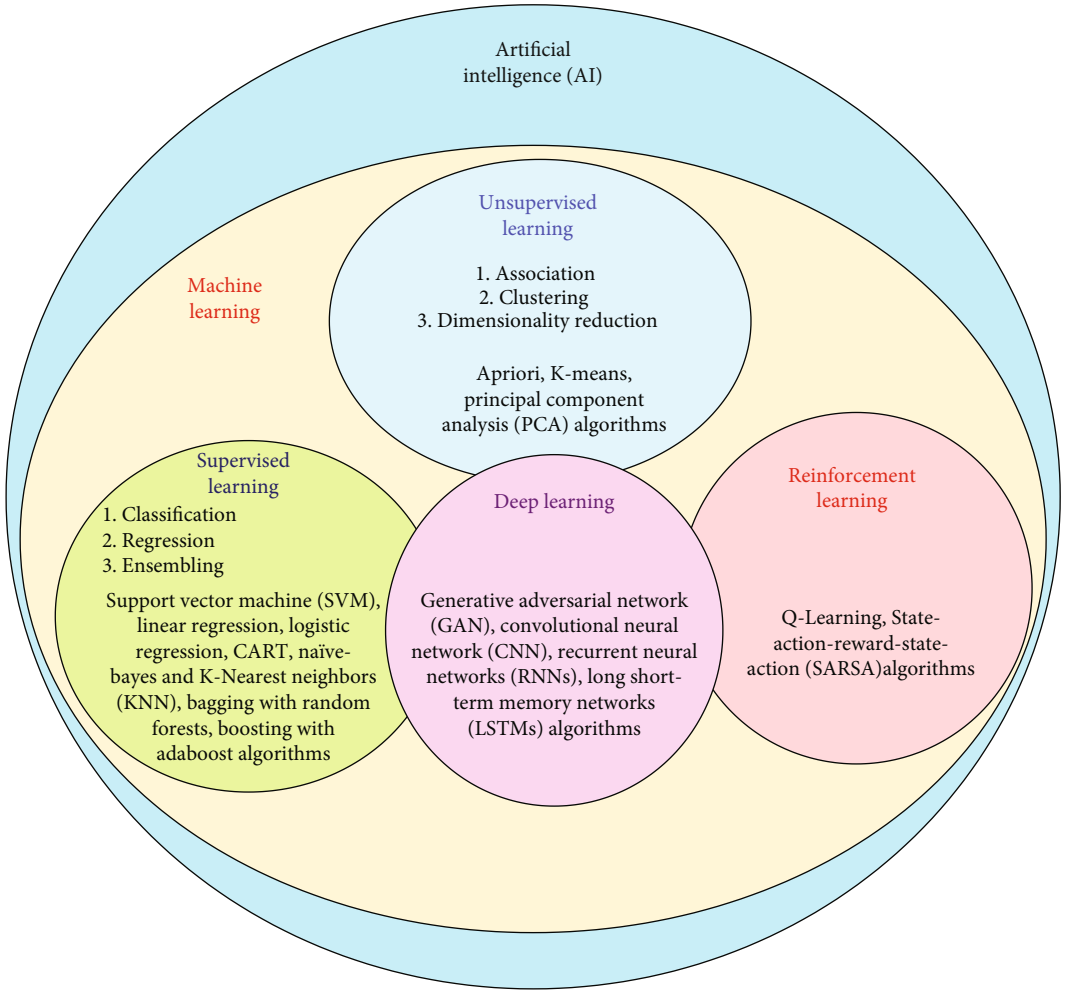

Figure 1: Different categories of machine learning along with algorithms.

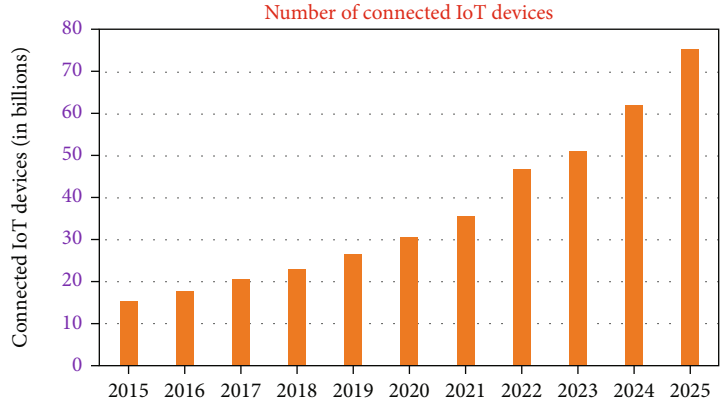

Figure 2: Trends of number of connected IoT devices.

communication module. This layer is responsible for information collection and signal processing

(ii) The pipe layer deals with the communication related technologies. It is responsible for the access and data transmission among the different devices and users. It works through wired and wireless networks including, 2G, 3G, 4G, 5G, 6G, NarrowBand-Internet of Things (NB-IoT), Long-Term Evolution (LTE), and Zigbee

(iii) The cloud layer provides different cloud-based platforms for the data processing, storage, and analysis. It is responsible for device access, device

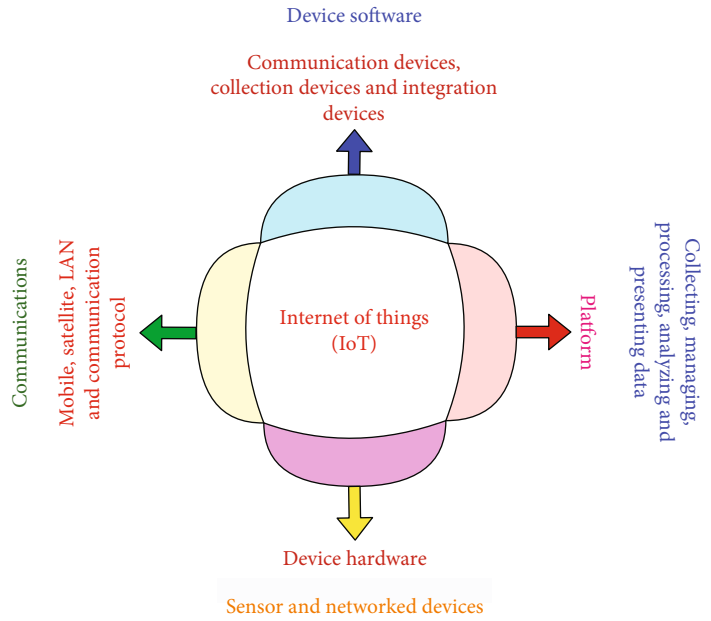

Figure 3: IoT construction.

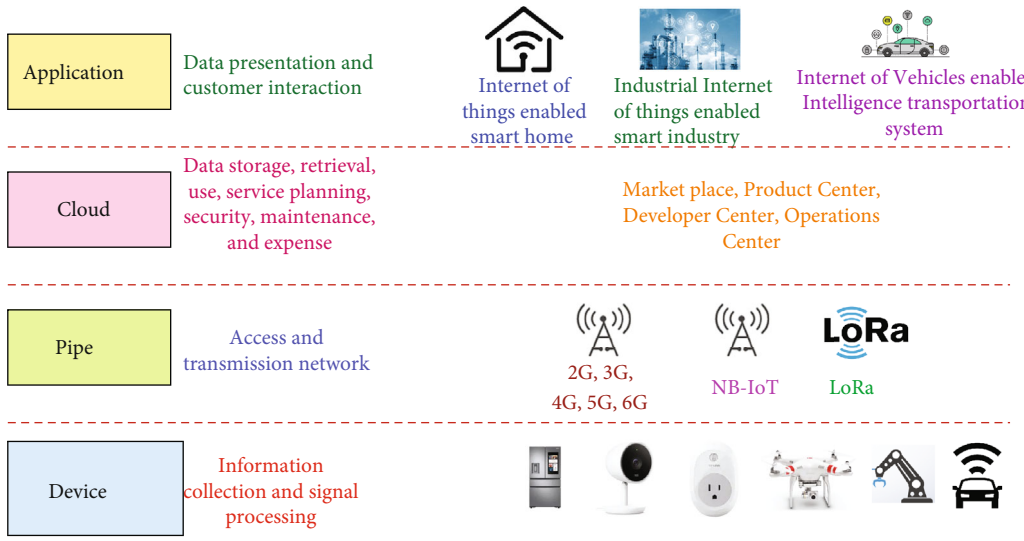

Figure 4: Layered architecture of IoT.

management, data integration, and storage. It also provides application programming interface (API) for upper layer operations

(iv) The application layer is the upper most layer, which is responsible for presentation, customer interaction, and service logic processing. It is the interface for direct contract with end users. Various types of applications are supported from different domains such as IoT-enabled smart home, IoT-enabled smart city, Industrial Internet of Things- (IIoT-) enabled smart industry, and Internet of Vehicles- (IoV-) enabled intelligent transportation system

Blockchain is a specific type of database. It is a digital ledger of transactions, which is duplicated and distributed across the entire network of computer systems (i.e., cloud servers) on the blockchain. It differs from a conventional database in the way it stores the information. Blockchain stores data in the form of some blocks, which are then chained together. As new data comes in, it is entered into a newly generated block [23, 24].

Figure 5 defines the different properties of a blockchain. Their details are given below [23]:

(i) Programmable: a blockchain can be implemented through some programming language, i.e., smart contract via solidity programming

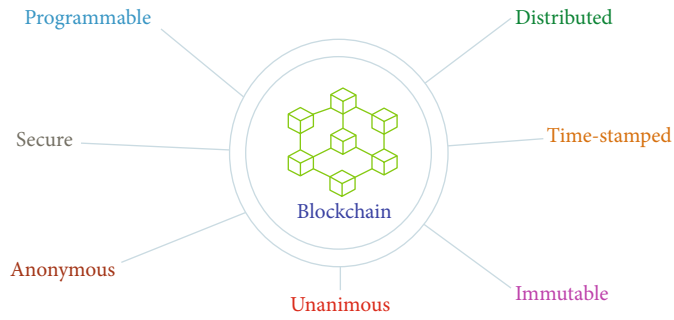

Figure 5: Properties of a blockchain.

(ii) Secure: blockchain uses hashing and encryption mechanisms to provide the security to the stored data. The Merkle tree is built from the all hashes of the transactions, which is further used for the integrity checking. Therefore, it is very difficult to change or update the data, which is stored inside the blockchain. Furthermore, data is stored in the form of encrypted transactions; thus, unauthorized leakage of data is not possible

(iii) Anonymous: due to this property, the identities of the entities are preserved. This further signifies that adversary ($\mathscr{A}$) is not able to discover who is communicating with whom

(iv) Distributed: a blockchain is built through the peer-to-peer distributed network in the form of a distributed ledger. This ledger is shared among all authorized entities (i.e., miner nodes)

(v) Time-stamped: in a blockchain, when a block is constructed, then, it is also stored with a freshly generated timestamp value. This mechanism is further helpful to resolve the data freshness issues. This further signifies that entities are able to identify "when a particular record is stored in the block"

(vi) Immutable: a blockchain is built through certain number of blocks; whatever we store there will go inside the blocks. These blocks are connected through a hash chain. It is not possible for $\mathscr{A}$ to change the data of the block. If an $\mathscr{A}$ attempts for updating the blocks, then in that situation, he/she has to update a certain fraction of blocks, which is practically impossible

(vii) Unanimous: there is a requirement of execution of a consensus algorithm for the addition of a newly created block in the blockchain. The steps of the consensus algorithm are executed by the miner nodes (i.e., cloud servers). During this process, majority of the miner nodes agree on the addition of the "newly created blocks," if a given fraction of miner nodes, like 80% nodes, commit (agree). In such situation, block is added into the blockchain. Therefore, during this implementation and execution, nodes decide unanimously for some particular tasks

On the basis of their characteristics and features, blockchain can be divided into different categories. Details are given below [23].

(i) Public blockchain: in the public blockchain architecture, data and access to the system's resources can be given to anyone who wishes to participate. For example, bitcoin, ethereum, and litecoin cryptocurrencies are the example of public blockchains. In contrast to that, a public blockchain is open-ended and thus can be called as decentralized. In a public blockchain, all records are visible to the participants, who take participation in the agreement (consensus) process. However, it is less efficient since it takes a considerable amount of time to accept each new record into the blockchain. Moreover, it is not efficient as the time required for each transaction is less ecofriendly. It needs a huge amount of computation power as compared to the private blockchain.

(ii) Private blockchain: it is different than the public blockchain architecture; in this architecture, the system is controlled only by users from a specific organization or authorized users, who get invitations to participate: for example, "blockchain of healthcare system." It is considered to be more centralized as it is controlled by a particular organization.

(iii) Consortium blockchain: in consortium blockchain, some organizations decide for the implementation of a blockchain, which is also maintained by these organizations. In this blockchain, procedures are set up and controlled by the preliminary assigned users: for example, blockchain of an "intelligent transportation system."

The structure of a block, which is used in the blockchain, is given in Figure 6. It contains important information like version of the block, which is unique for every block. It contains the hash value of the previous block, hash value of current block, and signature of the current block, which is computed through some algorithms like Elliptic Curve Digital Signature Algorithm (ECDSA). It also contains the value of Merkle tree root, which is the hash value of all transactions and used for the integrity checking of transactions. It further contains values like owner's information, public key

Block header	
Block version	*BVer*
Previous block hash	*PBhash*
Merkle trss root	*MR*
Timestamp	*TR*
Owner of block	*OB*
Public key of owner	Pub_{cs_j}
Block payload (Encrypted transactions)	
Encrypted transactions #1	$E_{pub_{cs_j}}(Tx_1)$
Encrypted transactions #2	$E_{pub_{cs_j}}(Tx_2)$
⋮	⋮
Encrypted transactions $\#n_t$	$E_{pub_{cs_j}}(Tx_{n_t})$
Current block hash	*CBhash*
Signature on block using ECDSA	*Bsing*

Figure 6: Structure of a block.

of the owner, and timestamp value, which is freshly generated for each block. Another important information that a block has is encrypted transactions. The entire data is converted in the form of certain transactions, and then, this will be encrypted with the public key of the owner. The entity who has the corresponding private key can only decrypt the transactions; otherwise, it is not possible. This particular arrangement is especially useful for the private blockchain networks, where privacy is essentially required [23].

1.4. Novelty and Research Contributions. The novelty and research contributions of the paper are given as follows:

(i) A blockchain-envisioned secure authentication framework for AIoT is presented in the paper, in which we provide the full details of the design of that framework

(ii) The adversary model of "blockchain-envisioned secure authentication framework for AIoT" is then highlighted. It covers most of the potential threats in such kind of communication environment

(iii) The security analysis of the proposed framework is provided to prove its security against the various possible attacks

(iv) Various applications of blockchain-envisioned secure authentication framework for AIoT are also highlighted

(v) Next, the different issues and challenges of blockchain-envisioned secure authentication framework for AIoT are discussed

(vi) Finally, we highlight some future research directions of "blockchain-envisioned secure authentication framework for AIoT," which should be addressed in the future

1.5. Paper Outline. The remaining part of the paper is organized as follows. The various applications of blockchain-envisioned secure authentication framework for AIoT are discussed in Section 2. Various issues and challenges of the blockchain-envisioned secure authentication framework for AIoT are provided in Section 3. We provide the details of architecture of the proposed generalized framework in Section 4. After that, the security analysis of the proposed framework is provided in Section 5, and a detailed comparative study with the state of art solutions is also provided in Section 6. Some future research directions of the presented framework are given Section 7. Finally, the paper is concluded in Section 8.

2. Applications of Blockchain-Envisioned Secure Authentication Framework for AIoT

In this section, we discuss some of the potential applications of blockchain-envisioned secure authentication framework for AIoT. Their details are provided below [1–9, 25–27].

2.1. Security and Surveillance System. The security and surveillance system can be deployed in different locations like in a city to monitor activities of thieves or in the border areas to monitor the activities of enemies. The security and surveillance system is equipped with smart sensors, drones, infrared camera, and CCTVs. These devices are connected to some central server, i.e., cloud server for their data processing, storage, and analysis. However, such kind of arrangement of data storage and analysis is not fully secure. Therefore, it is better to maintain it in the form of blockchain over the peer-to-peer to cloud server network. Whole data can be stored in the form of encrypted transactions. The authorized users of the system can also access data of the system after completing the steps of essential user authentication process. In such system, the AI component is helpful to predict about some threats, like chances of infiltration activities.

2.2. Smart Home. It is the convenient setup for a home in which smart appliances (i.e., smart air conditioner, refrigerator, television, and coffee maker) are deployed. These smart appliances can be automatically controlled remotely at anytime from anywhere through the Internet using the smartphone applications. The deployed devices of smart home are interconnected via Internet that allows its user to control functions, like the security access to the home, increasing/decreasing of temperature, and lighting on/off. These devices are connected to some central server, i.e., cloud server for their data processing, storage, and analysis. Again, it is better to maintain the data of smart home in the form of blockchain over the peer-to-peer to cloud server network. In such an arrangement, AI can improve the overall performance of the system and serve the users in a better way, for example, making coffee as per the taste of the users on the basis of feedback received in the past [5, 28, 29].

2.3. Intelligent Transportation System. Intelligent Transport Systems (ITS) is enabled with smart IoT devices and smart vehicles. ITS are the control and information systems, which use communications and data processing technologies to achieve the following objectives. It improves the mobility of people and goods. It also increases the safety and reduces

traffic congestion along with the management of different incidents as per the situation, like road side condition and occurrence of accidents. From this discussion, it is clear that for safety and security of data of the ITS, we need important mechanism, like the blockchain, which can be deployed there to achieve the desired needs of information security. Moreover, the AI component is helpful to predict about some threats, like chances of road accidents, traffic congestion in a street, and available best routes. For the ITS system, it is better to deploy a consortium kind of blockchain as it fulfils most of the requirements of the system [30, 31].

2.4. Smart Farming. Smart farming refers to the management of crop farms through some tools and technologies, for example, smart IoT devices, robotics, drones, and AI. This further helps to increase the quantity and quality of crops along with the minimum use of human labour required. For the security of data of the smart farming system, it is better to use blockchain technology. Furthermore, AI component is helpful to predict about different phenomena, like use of fertilizer as per the soil condition, weather condition, and expectancy of crops quantity for a particular session [32, 33].

2.5. Secure and Safe Healthcare Monitoring. Smart healthcare is enabled with Internet of Medical Things (IoMT), which is an amalgamation of smart healthcare devices and applications. These devices are connected to the healthcare information technology systems through some networking technologies. The advantage of this system is that it can reduce unnecessary hospital visits and the burden on healthcare systems by facilitating the communication among the patients and their physicians. However, in such a system the sensitive healthcare data transferred through the open channel, where this can be attached by various types of adversaries. Hence, it is better to deploy blockchain mechanism there for the secure processing and storage of sensitive healthcare data. Here, AI can also play an important role in the prediction of different health-related phenomena, like chances of getting heart attack, diabetic shocks, and effective role of a medicine for a specific disease [23, 34, 35].

2.6. Industrial Automation and Control. It uses smart sensors and actuators to enhance manufacturing, industrial, and control jobs. It is facilitated by the Industrial Internet of Things (IIoT). It uses the functions of smart devices and real-time analytics to take advantage of the data, which is produced by the industrial machinery. The smart machines are not only better than humans in the capturing and analysis of data in the real time but also good in communication of essential information, which is required to execute the faster business decisions in the accurate way. This communication environment also deals with the sensitive data, which should be protected against any kind of information security-related attacks. Therefore, if we envision blockchain mechanism there, then, data can be processed in a safe and secure manner. Moreover, the decentralized nature of blockchain can also be helpful to protect against the system failure-related problems. In industrial automation and control, AI can also play an important role in the prediction of different related phenomena, like the health condition of deployed tools and machinery [36].

2.7. Smart Cities. A smart city is a municipality, which uses Information and Communications Technology (ICT) to increase operational efficiency, share information with the public, and provide a better quality of government service and citizen welfare. It optimizes the various executing functions in a city and also promotes economic growth. It improves the quality of life of its citizens through the use of various deployed smart IoT sensors, related tools and technologies, and the data analysis process. Inside the smart city, the data can be collected from various sources like citizens, devices, buildings, and assets. This data is further processed and analysed to monitor and manage traffic problem, power plants, utilities, water supply, wastage management, crime detection and prevention, healthcare, and other community services. Blockchain and AI both can play an important role in the reliable and secure functioning of a smart city activity. If we deploy blockchain mechanism there, then, data can be processed in the secure way. Again, the decentralized nature of blockchain can also be helpful to protect against the system failure-related problems, which are very common when we talk about the broader domain, i.e., a smart city. Moreover, AI can also play an important role in data analysis process, which is one of the essential requirements of a smart city.

2.8. eCommerce. Blockchain-envisioned AIoT in eCommerce sector helps the businesses for the advanced product positioning, optimization of relationship with vendors, automation of billing and invoice, and generation of real-time insights on shipment deliveries. However, the data storage and analysis of this communication environment are not secure. Therefore, it is better to maintain it in the form of blockchain over the peer-to-peer to cloud server network, where the entire data can be stored in the form of encrypted transactions inside the various blocks and then all these blocks are chained together through a hash chain. This type of arrangement can protect the data and associated process against the various types of information security-related attacks.

2.9. Logistics Operations and Control. AIoT can optimize the supply chains and also do the management of inventories. The smart IoT sensors and related devices can detect when an item would go out of stock and autonomously reload the products per the need. It also facilitates the commercial fleets and delivery modules for their safety and smooth executions. In the logistics operations and control, there is requirement of communication among the various users and devices, and these entities communicate over the public channel. However, this public channel is vulnerable to various types of information security-related attacks. Thus, the data storage and analysis of this communication environment are insecure. Henceforth, it is better to maintain it in the form of blockchain, which can protect the data and associated process against the various types of attacks.

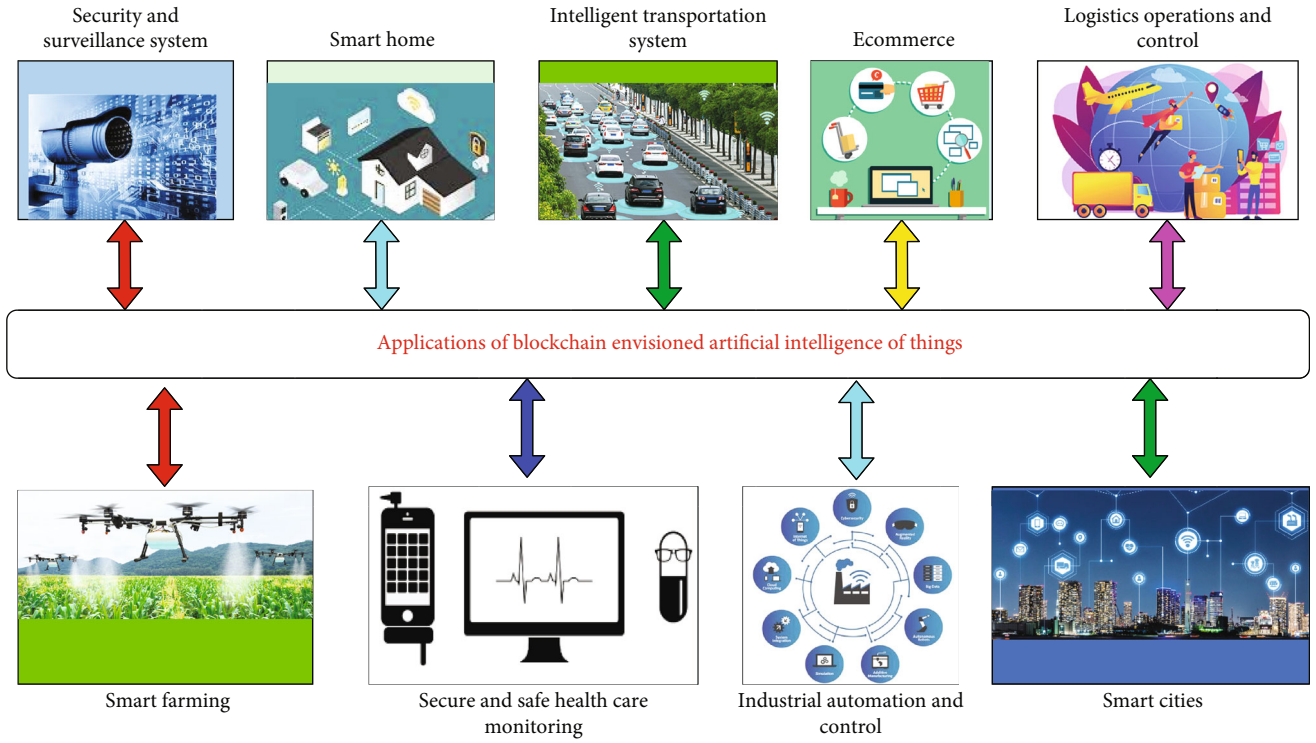

Figure 7: Applications of blockchain-envisioned AIoT.

The various applications of blockchain-envisioned artificial intelligence of things are also depicted in Figure 7.

3. Issues and Challenges of Blockchain-Envisioned Secure Authentication Framework for AIoT

The blockchain-envisioned secure authentication framework for AIoT can be deployed for various applications as discussed earlier. However, at the same time, it also suffers from various types of issues and challenges. Some of the potential issues and challenges are discussed below [23].

3.1. Scalability. The management of increasing number of users and IoT devices is always challenging. The blockchain-envisioned secure authentication framework for AIoT uses various types of complex algorithms, which are related to blockchain's consensus, AI-based analysis, and IoT communication. In case of the increasing number of people and devices, the average transactions have also increased correspondingly. It severely hit the processing speed of the transactions as a higher number of users and devices need more computing and storage devices. It causes the creation of an overall cumbersome system. Therefore, scalability is a challenging problem in this particular environment.

3.2. Information Security Issues. In most of the cases, IoT devices operate with low-quality software, which are susceptible to different kinds of vulnerabilities. The smart IoT devices are vulnerable due to malware injection, software exploits, weak cryptographic usage and failure of authentication, and access control schemes. A blockchain-envisioned secure authentication framework for AIoT is also vulnerable to various types of information security-related attacks, i.e., "replay," "man-in-the-middle (MiTM)," "impersonation," "credential leakage," "illegal session key computation," "data modification," "data disclosure." Another issue is with the mechanism of blockchain, as blockchain lacks in the set of regulatory oversight, which makes it a volatile environment and an easy target for market manipulation. No matter how robust the mechanism you deploy, there is always a chance that it will be hacked or it may be blocked by the government agencies due to some umbrageous practices [37, 38].

3.3. Overall Complexity of the System. In the blockchain-envisioned secure authentication framework for AIoT, the smart IoT devices need rich and well-equipped hardware, software, and data storage capabilities. Therefore, its adoption usually requires sufficient investments of money for which every organization is not ready. Other than that, IoT devices have limited computational power and are incompatible with robust protection technique by their design. To mitigate these flaws and safeguard the network from malware injections and other hacking attempts, IoT adopters require to deploy multilayered security controls. The included blockchain mechanism again introduces the complexities in the system due to its inherit properties. Before going for the deployment of blockchain, it is recommended to go through the principles of encryption and distributed ledger. Furthermore, various AI algorithms especially the deep learning also overloaded the system in terms of communication cost, computation cost, and storage cost. Thus, complexity is another important issue in a blockchain-

envisioned secure authentication framework for AIoT, which needs to be handled carefully.

3.4. Privacy. Blockchain is an essential component of the blockchain-envisioned secure authentication framework for AIoT. It is an open ledger and visible to all parties. It is the essential requirement in some of the cases. However, in some of the cases, it becomes a liability if it is deployed for a sensitive environment, i.e., healthcare. Therefore, the ledger requires to be remodeled in such a way that it provides access only to the authorized people, not to everyone. However, such kind of issues can be sorted out by making use of different categories of blockchain; for example, private blockchain can be preferred in case we need more privacy. Furthermore, to achieve the desired goals of privacy, IoT devices must exchange data through the Internet in a secure way, so that Internet attackers do not get any chance to exploit it. Therefore, IoT devices should have to exchange their data through the best encryption algorithms, i.e., AES, RSA, and ECC, to avoid the data leakage [39–41].

3.5. Cost Factor. In the blockchain-envisioned secure authentication framework for AIoT, there is a requirement to deploy blockchain. In most of the cases, blockchain is implemented for the elimination expenses related to the third parties and intermediaries, which facilitate the process of transferring the assets (i.e., health-related data in a healthcare system). Blockchain is in the riser stages, which makes it difficult to integrate into the legacy systems. Due to such reasons, it becomes expensive and further prevents its adoption in the government and other private organizations. Furthermore, it is difficult for the financial institutions (i.e., banks) to adopt the blockchain for the secure payment gateways as it incurs extra costs to the system [23].

3.6. Requirement of Highly Skilled Man Power. The blockchain-envisioned secure authentication framework for AIoT requires highly skilled man power for the implementation, maintenance, and support purpose. This man power should have knowledge of AI, IoT, and blockchain technologies at the same time. Therefore, rigorous training is required to work in this particular domain. Moreover, such type of courses should also be taught to the students, who are doing their degrees in various universities.

3.7. Problem of Biasing. Since the blockchain-envisioned secure authentication framework for AIoT is enabled with AI, then, there may be some chances of biasing. It is a general problem with the AI systems; they are only as good or as bad as they have trained. For example, there are some techniques, which are used for the determination of who has been called for an interview and whose loan has been sanctioned. If we have bias in the algorithms, then, we make vital decisions, which are also unrecognized. This may further lead to unethical and unfair consequences; i.e., the system has predicted that this particular fellow has a chance of getting massive heart attack; however, that person is completely fit and fine. Therefore, in such systems, everything depends on their training procedure and the available dataset. Hence, we should rectify these issues as much as possible. The developer should always try for the improvement of accuracy and correctness of the system.

3.8. Computing Power. The blockchain-envisioned secure authentication framework for AIoT is enabled with three important components, i.e., AI, IoT, and blockchain. This system uses various types of complicated and resource hungry algorithms, i.e., consensus algorithms and deep learning algorithms, which may trouble the organization working on such projects. For the smooth functioning of such systems, we need a lot of computation power and storage capacity as it generates data in the massive amount. Therefore, we need to deploy resource-rich devices, which may be very costly for some organizations having budget constraints.

3.9. Legal Issues. The blockchain-envisioned secure authentication framework for AIoT may face some legal issues. Countries have different laws for security and privacy of data. Even in some countries, blockchain in the initial phase of setup and different government agencies are working on the law formation for the blockchain, for example, which is allowed and which is prohibited. Therefore, some strong and uniform laws should be there. Moreover, such system deals with the sensitive data which may be in the violation of state/federal laws. Therefore, an organization should have to be careful of any perceived impact, which may put negative impact on the reputation of the organization.

3.10. Issues with Accepting the Technologies. The blockchain-envisioned secure authentication framework for AIoT is enabled with three important components, i.e., AI, IoT, and blockchain. Therefore, some of the early adopters may have their first experiences be negative or there are chances that investors do not want to fund such projects. However, such kind of issues can be resolved with the passing of time. Slowly, people will understand the usefulness of these technologies and start accepting them.

3.11. Interoperability. The blockchain-envisioned secure authentication framework for AIoT is the amalgamation of tools and technologies, which are related to AI, IoT, and blockchain. This operates through various types of complicated algorithms, i.e., consensus algorithms, deep learning algorithms, and IoT communication algorithms. In such kind of communication environment, there may be the issues related to interoperability of tools, technologies, and devices. Sometimes, it may cause the malfunctioning of deployed smart IoT devices, which can further create serious consequences. Hence, this issue should be handled carefully.

4. The Proposed Generalized Framework

In this section, we provide the detailed architecture of the proposed generalized framework. We also discuss about the potential adversaries of this communication environment under the "adversary model." Moreover, we provide the details of security analysis, which is mandatory to prove the security of proposed framework against the various potential attacks. A comparison of "security" and "functionality" features of

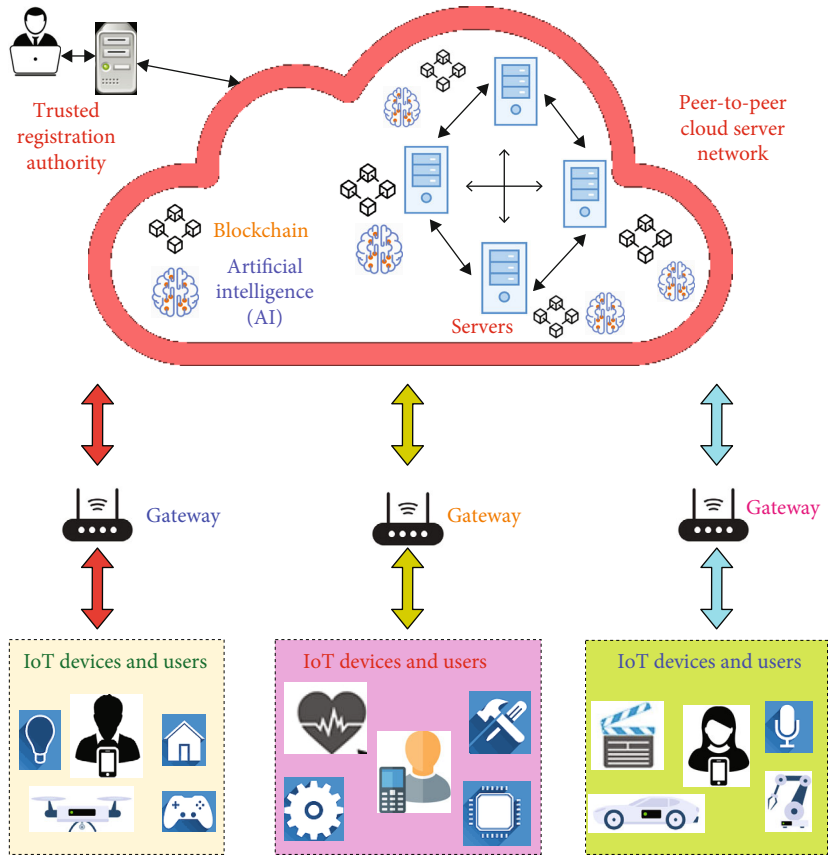

Figure 8: Architecture of blockchain-envisioned secure authentication framework for AIoT.

proposed framework with the other closely related security mechanisms is also provided [23, 42–44].

4.1. Architecture for Proposed Framework. The architecture of the proposed framework is given in Figure 8. This architecture contains different types of smart IoT devices, like smart home appliances, smart healthcare devices, smart vehicles, drones, industrial monitoring, and control equipment. It also contains various types of users (i.e., doctors, smart home's residence, traffic control's authority, and industrial plant's authority), who are interested in accessing the data of this system. All these users and smart IoT devices are located at the end layer. In the middle, we have gateway node devices, which receive the data from the smart IoT devices and convert it into partial blocks and then forward them to the connected cloud server. Cloud server is the part of peer-to-peer cloud server (P2PCS) network. Once a cloud server receives a partial block, it converts it into a full block. After that, this block is forwarded to the P2PCS network for its mining and addition into the blockchain. When a fraction (like 70%) of miner nodes (i.e., cloud servers) agrees on the addition of the block, it will be added into the blockchain, which is maintained through the distributed ledger technology. The distributed ledger is common and accessible to legitimate miner nodes [21, 22]. Therefore, the added block will be reflected to miner nodes' ledger. Here, it is important to mention that the entire communication (i.e., communication between smart devices, smart device and gateway node, gateway node and cloud server, cloud server and other cloud servers, and cloud server and user) happens in the secure way through the different established session keys [43]. The different notations, which are used in the paper, are provided in Table 1. The flow of activities of "blockchain-envisioned secure authentication framework for AIoT" is given below.

4.1.1. Registration of Devices and Users. In this phase, various cryptographic parameters and algorithms (i.e., Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard (AES)) are selected to use. Then, the registration of various devices (i.e., smart IoT devices, gateway nodes, cloud servers, and different users) is performed by the trusted registration authority. After the registration of these entities, the registration values are stored in the memory of these devices and also in the smartphone/smart card of the users. These stored values will further help in the login, authentication, and key establishment processes [44]. The registration process is then summarised in Algorithm 1.

4.1.2. User Login. In this phase, the legitimate users try to login into the system through the help for their smartphones/smart cards, as they have some pre-stored registration values. These registration values again facilitate the login process and abort the login process in case of any fake or unauthorized user login. Note that a user can use 2-factor or 3-factor user authentication protocol for the login

Table 1: Notations used in the paper.

Notation	Meaning
$\mathscr{A}$	An adversary
TA	Trusted authority
SD_i	i^{th} smart IoT device
GW_k	k^{th} gateway node
CS_l	l^{th} cloud server
$Pr\,i_x$	Private key of an entity x
Pub_x	Public key of an entity x
	Note $Pub_x = Pr\,i_x \cdot G$
TS_y	Timestamp values
$h(\cdot)$	Cryptographic one-way hash function
$SK_{x,y}$	Session key between entity x and entity y
$\|$	Concatenation operation
$\oplus$	Bitwise XOR operation
PB_a	Partial block of an entity a
FB_a	Full block of an entity a

Result: Deployed registered E_i
for Entity (i.e., device) $E_i \forall i = 1,2 \cdots num_E$ **do**
    TA generates credentials
    TA stores generated credentials in E_i's memory
    E_i is then deployed
end

Algorithm 1: Registration phase.

purpose [45]. The user login process is summarised in Algorithm 2.

4.1.3. Authentication and Session Key Establishment. In this phase, there are executions of the authentication and key establishment procedures among the various entities, like IoT device to other IoT device, IoT device to gateway node, gateway node to cloud server, cloud server to other cloud server, and cloud server to user. After performing the steps of mutual authentications, these entities establish different session keys for their secure communication. During the computation of session keys, it is recommended to use short-term secret values (i.e., different nonce values, freshly generated timestamp values, and long term secret values, i.e., different identities and secret key values). Such type of recommendation is helpful to generate the different session keys for different entities in the different sessions. Moreover, the illegal session key computation attack also becomes difficult for the attackers to launch. Without guessing the correct session keys, the attacker cannot decrypt the exchanged messages. Therefore, the ongoing communication is safe and secure against the various potential attacks [44, 45]. This phase is summarised in Algorithm 3.

Result: Logged in U_i
for U_i where $i = 1,2 \cdots num_U$ **do**
    U_i inputs his/her identity & password
    U_i inserts his/her smart card
    U_i provides his/her biometric data
    System checks the genuine of U_i
    IF U_i passes authenticity criteria
    Allows U_i to logged in
    ELSE
    Abort the login process
end

Algorithm 2: Login phase.

4.1.4. Blockchain Implementation. In this, blockchain is implemented at the P2PCS network. When a gateway node receives data from the connected IoT devices, it converts this into a partial block, where a partial block contains fields, like the owner of the block (i.e., gateway node), public key of the owner, and encrypted transactions, which are encrypted through the public key of the owner. Here, it is important to mention that the gateway node creates the encrypted transactions from the data that it receives from the connected IoT devices in the secure manner. After that, gateway node sends this partial block to the connected cloud server (over the P2PCS network) in the secure way. The cloud server creates the full block from the partial block by adding other fields (i.e., version of the block, timestamp value, hash of previous block, hash of current block, Merkle tree root value (from all transactions), and signature of current block (i.e., through Elliptic Curve Digital Signature Algorithm (ECDSA)) [46]), into it. After that, the block is forwarded to the P2PCS network for the consensus process. The consensus process can be executed through algorithms, like ripple protocol consensus algorithm (RPCA) and practical byzantine fault tolerance consensus (PBFT). In the consensus process, an elected leader (cloud server) executes the steps of consensus (mining), in which it decides for a puzzle and then sends encrypted puzzle and the block to the other legitimate cloud servers. Each cloud server tries solving the puzzle and then submits their responses to the leader. In case, when a fraction of cloud servers (say, 70%) commit on the addition of the block, the block will be then added into the blockchain. Blockchain is maintained through the distributed ledger, which is shared and accessible to all legitimate cloud servers. Therefore, the newly added block is reflected to all the legitimate cloud servers [23, 42]. This phase is summarised in Algorithm 4.

4.1.5. AI-Based Data Analysis. In this phase, data analysis is performed on the received data from the IoT smart devices. As we know, IoT devices generate enormous amount of data, which is in various forms. The data can be considered the Big data, and the similar big data analytics algorithms are applicable here for the data analysis purpose. This phase is a very important to draw some useful conclusion from the received, processed, and stored IoT data. For example, various types of prediction can be made (i.e.,

Result: Session key between E_i and E_j
for Entity E_i and entity E_j **do**
E_i generates fresh timestamp TS_{E_i} & random secret RS_{E_i}
E_i computes authentication request message MSG_{ARQ} through TS_{E_i} & RS_{E_i}
E_i sends MSG_{ARQ} to E_j
E_j verifies timeliness of received TS_{E_i}
IF verification of TS_{E_i} happens successfully
E_j computes RS_{E_i} from received MSG_{ARQ}
E_j Checks genuineness of MSG_{ARQ}
IF MSG_{ARQ} is valid
E_j generates fresh timestamp TS_{E_j} and random secret RS_{E_j}
E_j generates session key SK_{E_j,E_i} through TS_{E_i}, TS_{E_j}, RS_{E_i}, RS_{E_j} and other secrets
E_j computes authentication response message MSG_{ARS} through SK_{E_j,E_i}, TS_{E_j} & RS_{E_j}
E_j sends MSG_{ARS} to E_i
ELSE E_j aborts the process
ELSE E_j aborts the process
E_i verifies timeliness of received TS_{E_j}
IF verification of TS_{E_j} happens successfully
E_i computes RS_{E_j} from received MSG_{ARS}
E_i computes session key SK_{E_i,E_j}
E_i computes $MSG_{ARS}{}'$ through SK_{E_i,E_j}
E_i verifies $MSG_{ARS}{}' = MSG_{ARS}$?
IF MSG_{ARS} is valid
Computed SK_{E_i,E_j} is correct
Both E_i & E_j establish session key $SK_{E_i,E_j} = SK_{E_j,E_i}$
E_i & E_j start their secure communication through $SK_{E_i,E_j} = SK_{E_j,E_i}$
ELSE E_i aborts the process
ELSE E_i aborts the process
end

Algorithm 3: Authentication and session key establishment phase.

chances of road side accident in a particular street of a city, prediction of harsh weather conditions, prediction of crop diseases, and prediction of critical health issues (i.e.., massive heart attack, diabetic shock, and cancer)). AI-based data analytics is conducted at the P2PCS network as cloud servers are resource-rich devices and can be further helpful for the smooth execution of various AI techniques (i.e., deep learning algorithms) [47]. This phase is summarised in Algorithm 5.

4.1.6. Secure Data Delivery to Authorized Users. This phase is responsible to provide the data to the authorized users of "blockchain-envisioned secure authentication framework for AIoT." The entire transfer of data happens in the secure way through the established session keys. However, each legitimate user has to first execute the required steps of remote user authentication mechanisms (may be 2-factor or 3-factor user authentication) to get entry into the system. There are two possibilities: (1) the user can get the live data directly from the smart IoT device, and (2) the user can get the data stored over the P2PCS network. However, in the second case, the corresponding gateway node decrypts the encrypted transactions' data and then provides it to the genuine authorized users [48]. This phase is summarised in Algorithm 6.

4.2. Adversary Model. It is very important to highlight the potential adversaries (attackers/threats) of a communication environment. In the designing of "blockchain-envisioned secure authentication framework for AIoT", we have followed two important threat models. First one is the Dolev-Yao (DY) model; in this model, it is assumed that the communication channel is open and insecure and the existing adversaries can modify, delete, drop, and delay the exchanged messages [49]. Moreover, an adversary $\mathcal{A}$ can physically capture some of deployed IoT devices and then can extract the sensitive information (i.e., identity information and secret keys) from their memory with the application of sophisticated power analysis attack [50]. $\mathcal{A}$ can also deploy his/her fake devices in the network, which can further launch other attacks (i.e., routing attacks) to interrupt the ongoing communication. Again, $\mathcal{A}$ can also introduce various malware attacks on the ongoing communication. Further, the smartcards/smartphones of the legitimate users can also be stolen by $\mathcal{A}$ physically; then, $\mathcal{A}$ can extract the sensitive information (i.e., identity information and secret

Result: Implemented blockchain BC over P2PCS network
for GW_k and CS_l **do**
GW_k computes $PB_{GW_k} = \{OB_{GW_k}, Pub_{GW_k}, E_{Pub_{GW_k}(T_{xn_t})}\}$
GW_k generates fresh timestamp TS_{GW_k}
GW_k sends $\{PB_{GW_k}, TS_{GW_k}\}$ to CS_l through SK_{GW_k,CS_l} securely
CS_l verifies the timeliness of received TS_{GW_k}
IF verification of TS_{GW_k} happens successfully
CS_l creates full block as $FB_{CS_l} = \{BVer, PBHash, MR, TS_{CS_l}, OB_{GW_k}, Pub_{GW_k}, E_{Pub_{GW_k}(T_{xn_t})}, CBHash, BSign\}$
CS_l forwards FB_{CS_l} to P2PCS network
ELSE CS_l discards PB_{GW_k}
A leader LD is elected at P2PCS network
LD calls the steps of consensus algorithm
LD decides a puzzle PZZ
LD encrypts PZZ with the public key of miner node (cloud server CS_m) where it has to be sent as $E_{Pub_{CS_m}}(PZZ)$
LD sends $\{E_{Pub_{CS_m}}(PZZ), FB_{CS_l}\}$ to CS_m
CS_m solves $E_{Pub_{CS_m}}(PZZ)$ & submit response to LD
IF a fraction of miner nodes commit (i.e., 70%) addition of FB_{CS_l}
FB_{CS_l} is added in BC
ELSE LD calls the another consensus process
end

Algorithm 4: Blockchain implementation phase.

Result: Predictions on Blockchain data
for CS_l **do**
CS_l gathers data from BC
CS_l calls the steps of a standard big data analytics
CS_l predicts the results
end

Algorithm 5: AI-based data analysis.

keys) from their memory with the application of sophisticated power analysis attack. This malicious activity further helps $\mathscr{A}$ in the guessing of secret credential (i.e., passwords) of the users. Another important model "Canetti and Krawczyk's adversary model (CK-adversary model)" is also considered in the designing of the proposed framework [51]. As per the guidelines of the CK-adversary model, $\mathscr{A}$ has all features like the DY model along with that he/she can compromise the secret credentials and with the "session keys or the session states" corresponding to the established sessions. Therefore, $\mathscr{A}$ also has the ability to compromise the session keys, which are established among the different entities of the network. It is also assumed that gateway nodes are kept in physical security under some locking system to prevent their physical stealing. Thereafter, the secret parameters are not available to $\mathscr{A}$ to launch further attacks, like impersonation, MITM, and illegal session key computation.

5. Security Analysis of the Proposed Framework

In this section, we provide the details of the conducted security analysis of the proposed framework. The proposed framework is able to protect against the following types of potential attacks.

5.1. Prevention of Replay Attack. In the proposed framework, we consider the use of freshly generated timestamp values in all exchanged messages, which are also verified at the recipient's end when messages reach there. If verification happens successfully, then messages are treated as fresh. Otherwise, it is considered as the replayed messages. In this way, the proposed framework prevents the replay attack.

5.2. Prevention of Man-In-The-Middle (MiTM) and Impersonation Attacks. In the proposed framework, we consider the use of freshly generated timestamp values, random secret values, and secret keys in the different computed and transmitted messages. Due to such kind of arrangement, only the legitimate entity can produce the original message as he/she has the information of secret values. Hence, $\mathscr{A}$ does not have the ability to calculate the messages on behalf of the legitimate entities of the network. $\mathscr{A}$ is not able to update the content of the exchanged message without knowing the secret values. In this way, the proposed framework is able to prevent both MiTM and impersonation attacks.

5.3. Prevention of Ephemeral Secret Leakage (ESL) Attacks. The proposed framework assumes that session keys should be calculated using short-term secrets (such as timestamps and random nonce) and long-term secrets (such as secret keys and multiple identities). For each session, a new session key is computed and established by the communicating entities. An $\mathscr{A}$ does not have ability to calculate the correct value of session key without knowing long-term secrets and short-term secrets. Hence, the proposed framework is able to

Result: Secure data delivery to authorized users
for U_i and CS_l **do**
U_i logged into the system using the steps of Algorithm 2
U_i and CS_l establish SK_{U_i,CS_l} using the steps of Algorithm 3
CS_l provides data to U_i through SK_{U_i,CS_l} securely
end

Algorithm 6: AI-based data analysis.

prevent unauthorized session key computation attack under the CK-adversary model.

5.4. Prevention of Privileged Insider Attack. In the proposed framework, the secret listed information is not accessible to the internal user of the registration authority because there is a mechanism to erase the secret registered information from the database (memory) of the registration authority. Accordingly, an inside user who has malicious forethought cannot launch other related attacks such as impersonation attack, secret credential guessing attack, and unauthorized session key computation attack. Thereafter, the proposed framework is protected against the privileged insider attack.

5.5. Protection against Physical IoT Device Capture Attack. In the proposed framework, we do not store any secret information in plain text in the memory of the IoT device. Furthermore, an $\mathcal{A}$ physically gets hold of an IoT device and tries to retrieve secret information (i.e., session key) from its memory using an advanced power analysis attack [50]. At that point, that type of malicious venture would not be useful to $\mathcal{A}$ as it could expose the session key of that specific IoT device and not the session key of other IoT devices. This happens in light of the fact that each IoT device has different identities and secret key values. As a result, obtaining this specific session key will not be useful to obtain the session keys of other IoT devices. Thus, the ongoing communication between other IoT devices is still safe and secure. Thereafter, the proposed framework is resilient against physical IoT device capture attack.

5.6. Protection against Stolen Verifier Attack. In the proposed framework, we store all the parameters in a secure area of the database of the cloud servers. It is also assumed that gateway nodes are kept in physical security under some locking system to prevent their physical stealing. Thereafter, the secret parameters are not available to $\mathcal{A}$ to launch further attacks, like impersonation, MITM, session key computation, and so forth. Hence, the proposed framework is able to prevent the stolen verifier attack [52].

5.7. Prevention of 51% Attack and Selfish Mining. There are possibilities of some attacks on the blockchain-based system, for example, 51% attack and selfish mining. These attacks may happen when $\mathcal{A}$ has high "hashing power" [53]. In particular, the 51% attack demands $\mathcal{A}$ needs to possess more than half of the hashing power. Typically, the 51% attack is mounted in opposition to "cryptocurrencies," where $\mathcal{A}$ performs malicious activities like the double spending. On the other hand, selfish mining in the blockchain context is another well-known vulnerability used by miners to steal block rewards. Recently, it is identified that the consensus algorithm "Proof-of-Work (PoW)" is vulnerable to 51% attack, which is not used in the proposed framework. Hence, the proposed framework is secured against the 51% attack and selfish mining attack.

6. Comparative Study

A comparative study of the proposed framework and other closely related frameworks is conducted. Various frameworks, for example, Liu et al.'s framework [54], Garg et al.'s framework [23], Saha et al.'s framework [55], Xiang et al.'s framework [56], Xu et al.'s framework [57], Aujla and Jindal's framework [58], and Islam and Shin's framework [59] are analysed and compared. The details of comparisons are given in Table 2. During the comparative study, the following important security and functionality features are considered:

(i) SFF_1: "provides mutual authentication/access control"

(ii) SFF_2: "supports anonymity property"

(iii) SFF_3: "supports untraceability property"

(iv) SFF_4: "provides session-key agreement"

(v) SFF_5: "provides session key security under CK adversary model"

(vi) SFF_6: "provides data confidentiality"

(vii) SFF_7: "provides data integrity"

(viii) SFF_8: "protection against strong replay attack"

(ix) SFF_9: "protection against man-in-the-middle attack"

(x) SFF_{10}: "availability of efficient login phase"

(xi) SFF_{11}: "availability of password update phase"

(xii) SFF_{12}: "availability of biometric update phase"

(xiii) SFF_{13}: "availability of dynamic controller node (personal server) addition phase"

(xiv) SFF_{14}: "availability of dynamic IoT device addition"

(xv) SFF_{15}: "protection against stolen mobile device/programmer attack"

Table 2: Comparison of security and functionality features.

Feature	Liu et al. [54]	Garg et al. [23]	Saha et al. [55]	Xiang et al. [56]	Xu et al. [57]	Aujla and Jindal [58]	Islam and Shin [59]	Proposed framework
SFF_1	√	√	√	√	√	√	√	√
SFF_2	√	√	√	√	√	√	√	√
SFF_3	√	√	√	√	√	√	√	√
SFF_4	×	√	√	√	×	√	×	√
SFF_5	×	√	√	×	×	×	×	√
SFF_6	√	√	√	√	√	√	√	√
SFF_7	√	√	√	√	√	√	√	√
SFF_8	√	√	√	√	√	√	√	√
SFF_9	√	√	√	√	√	√	√	√
SFF_10	NA	√	NA	√	NA	×	NA	√
SFF_11	NA	√	NA	√	NA	×	NA	√
SFF_12	NA	√	NA	×	NA	×	NA	√
SFF_13	×	√	×	×	×	×	×	√
SFF_14	×	√	×	×	×	×	×	√
SFF_15	NA	√	NA	√	NA	NA	NA	√
SFF_16	√	√	√	√	√	√	√	√
SFF_17	×	√	×	√	×	×	×	√
SFF_18	×	×	×	×	×	×	×	√
SFF_19	×	√	√	√	√	√	√	√
SFF_20	×	×	×	×	×	×	×	√

×: "a framework is insecure against that particular attack or does not support a specific feature"; √: "a framework is secured against that particular attack or supports a specific feature"; NA: "not applicable in a scheme".

(xvi) SFF_{16}: "protection against impersonation attack"

(xvii) SFF_{17}: "provides formal security verification using AVISPA/SCYTHER tool"

(xviii) SFF_{18}: "provides formal security analysis under Real-or-Random (RoR) model"

(xix) SFF_{19}: "blockchain enabled security"

(xx) SFF_{20}: "provides AI-based data analysis"

From Table 2, it is clear that schemes of Liu et al. [54], Saha et al. [55], Xiang et al. [56], Xu et al. [57], Aujla and Jindal [58], and Islam and Shin [59] do not provide required security and functionality features like "provides session-key agreement," "provides session key security under CK adversary model," "availability of password update phase," "availability of biometric update phase," "availability of dynamic controller node (personal server) addition phase," "availability of dynamic smart healthcare device addition," "provides formal security verification using AVISPA/SCYTHER tool," and "provides formal security analysis under Real-or-Random (RoR) model." Moreover, Garg et al.' scheme [23] does not support feature like AI-based data analysis. However, the proposed framework supports most of the desired security and functionality features.

7. Future Research Directions

The blockchain-envisioned secure authentication framework for AIoT has various types of applications as discussed earlier. However, some limitations and challenges are also there. To resolve these issues, some research work needs to be conducted. In the following part of the section, we discuss some future research directions of this particular domain [21, 22, 41–43].

7.1. Security Enhancement. The blockchain-envisioned secure authentication framework for AIoT uses various kinds of authentication processes, which are required for the mutual authentication and key establishment among the communicating entities. To execute this task, user authentication schemes like 2-factor user authentication, 3-factor user authentication, and device to device authentication schemes like certificate-based authentication and certificateless authentication are used. However, these schemes come up with full proof security. Still, some of them are not fully secured, and there are some chances of vulnerability exploitation. Therefore, security schemes should be designed in such a way that they are secured against various types of possible attacks. The security of these schemes should be proved with various types of security analysis, like AVISPA simulation,

BAN logic, and formal security analysis via Real-or-Random (RoR) model. Hence, some research work is required in this direction [42, 43].

7.2. Efficiency of the Framework. The blockchain-envisioned secure authentication framework for AIoT has important components, like blockchain and AI. These technologies usually run some resource hungry algorithms, i.e., consensus algorithm and deep learning algorithm. These algorithms require lots of computation power, communication cost, and storage capacity. Therefore, it is very difficult to operate such kind of system when we have less number of resources. Hence, these frameworks should be designed in such a way that they require resources in the lesser amount. For example, the selection of algorithms can be done wisely; for example, it is better to use pBFT in place of PoW as it requires less number of resources. It is better to use lightweight cryptographic algorithms in place of other algorithms as they provide the same level of security with less communication, computation, and storage costs. For example, ECC and RSA provide the same level of security; however, ECC requires less costs. Thus, some research work should be done on the designing of efficiency of the frameworks [42, 44].

7.3. Interoperability of Tools and Technologies. The blockchain-envisioned secure authentication framework for AIoT is the amalgamation of tools and technologies, which are related to AI, IoT, and blockchain. This operates through various types of complicated algorithms, i.e., consensus algorithms, deep learning algorithms, and IoT communication algorithms. In such kind of communication environment, there may be the issues related to interoperability of tools, technologies, and devices. Sometimes, it may cause the malfunctioning of deployed smart IoT devices, which can further create serious consequences. Therefore, it should be handled carefully. Hence, some research work is also required in this direction [60].

7.4. Handling of Privacy Issues. As we know, blockchain is an essential component; it is implemented through an open ledger (distributed ledger), which is visible to all parties. It is essentially needed in some of the cases (i.e., public blockchain). In some of the cases, it becomes a liability if it is deployed for a sensitive environment, i.e., a system dealing with the healthcare data. This ledger requires to be remodeled in such a way that it provides access only to the authorized users. However, such kind of issues can be sorted out by making the use of different categories of blockchain (for example, private blockchain can be preferred in case when we need more privacy). Again for the achieving of desired goals of privacy, IoT devices must exchange the data through the Internet in a secure way, so that Internet attackers do not get any chance to exploit it. Therefore, IoT devices should have to exchange their data through the best encryption algorithms to avoid the data leakage. Meanwhile, authentication schemes are also needed to achieve the mutual authentication between the communicating entities (i.e., IoT devices, cloud servers, and users). We can deploy some access control mechanism to restrict the access of unauthorized entities. Hence, everything should be clearly defined to the programmer of the system (i.e., which technique should be used for which purpose). As a result, some research works should be carried out to improve the privacy of the framework [41].

7.5. Improvement of Accuracy of the System. As we know, AI is an integral part of such kind of frameworks; then, there may be some chances of biasing (i.e., wrong value of accuracy). It is very common with the AI-based systems; they are only as good or as bad as they have trained. If we have flaws in the algorithms, then, we make wrong predictions (results). This further may lead to unfair consequences; i.e., the system has predicted that this particular fellow has chance of getting massive heart attack; however, that person is completely fit and fine. Therefore, in such systems, everything depends on their training procedure and the available dataset. Hence, such issues should be rectified. The developer should always try for the improvement of accuracy and correctness of the system. Hence, some research work should be carried out to improve the accuracy of the frameworks [61, 62].

8. Conclusion

AIoT frameworks are very useful and applicable in a variety of applications as discussed earlier. However, AIoT frameworks may have issues related to data security and privacy due to the existence of information security-related attacks. A blockchain-envisioned secure authentication framework for AIoT is presented in the paper. The given adversary model covers most of the potential threats of such kind of communication environment. Various applications of the proposed framework are also discussed. Moreover, different issues and challenges of the proposed framework are highlighted. Furthermore, we provide some future research directions of the proposed framework, which should be addressed in the future.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education under Grant 2020R1I1A3058605. This work was also supported by the Ripple Centre of Excellence Scheme, CoE in Blockchain (Sanction No. IIIT/R&D Office/Internal Projects/001/2019), IIIT Hyderabad, India.

References

[1] Z. Xiong, Z. Cai, D. Takabi, and W. Li, "Privacy threat and defense 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] Y.-H. Lai, T.-C. Wu, C.-F. Lai, L. T. Yang, and X. Zhou, "Cognitive optimal-setting control of AIoT industrial applications with deep reinforcement learning," *IEEE Transactions on Industrial Informatics*, vol. 170, no. 3, pp. 2116–2123, 2021.

[5] B. Dong, Q. Shi, Y. Yang, F. Wen, Z. Zhang, and C. Lee, "Technology evolution from self-powered sensors to AIoT enabled smart homes," *Nano Energy*, vol. 79, article 105414, 2021.

[6] P. Zhang, R.-P. Chen, T. Dai, Z.-T. Wang, and K. Wu, "An AIoT-based system for real-time monitoring of tunnel construction," *Tunnelling and Underground Space Technology*, vol. 109, article 103766, 2021.

[7] S.-C. J. Hsu, H.-M. Hsu, and S.-Y. Hwang, "Co-creating future of Artificial Intelligence of Things (AIoT) through ecosystem partnership: a case study of Advantech Co., Ltd.," Springer, Singapore, 2021.

[8] W. C.-C. Chu, C. Shih, W.-Y. Chou, S. I. Ahamed, and P.-A. Hsiung, "Artificial Intelligence of Things in sports science: weight training as an example," *Computer*, vol. 520, no. 11, pp. 52–61, 2019.

[9] Y.-J. Lin, C.-W. Chuang, C.-Y. Yen, S.-H. Huang, J.-Y. Chen, and S.-Y. Lee, "Live demonstration: an AIoT wearable ECG patch with decision tree for arrhythmia analysis," in *2019 IEEE Biomedical Circuits and Systems Conference (BioCAS)*, Nara, Japan, 2019.

[10] C. K. Wu, Y. He, K. F. Tsang, and S. Mozar, "The IDex case study on the safety measures of AIoT-based railway infrastructures," in *2020 IEEE International Symposium on Product Compliance Engineering-Asia (ISPCE-CN)*, pp. 1–4, Chongqing, China, 2020.

[11] W.-P. Ma, C. Y. Nian, and H. Xu, "Application of AIoT in wireless image transmission to rotating machinery," in *2020 3rd IEEE International Conference on Knowledge Innovation and Invention (ICKII)*, pp. 45–47, Kaohsiung, Taiwan, 2020.

[12] H.-T. Pham, M.-A. Nguyen, and C.-C. Sun, "AIoT solution survey and comparison in machine learning on low-cost microcontroller," in *International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS)*, pp. 1-2, Taipei, Taiwan, 2019.

[13] I.-J. Huang, S.-R. Kuang, Y.-N. Chang, C.-C. Hung, C.-R. Tsai, and K.-L. Feng, "AIoTs for smart shrimp farming," in *International SoC Design Conference (ISOCC)*, pp. 17-18, Jeju, Korea (South), 2019.

[14] J. M. Corchado, "Aiot for smart territories," in *7th International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, p. 1, Paris, France, 2020.

[15] Edureka, "Top 15 hot artificial intelligence technologies," May 2021, https://www.edureka.co/blog/top-15-hot-artificial-intelligence-technologies/.

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

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

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

[19] C. C. Aggarwal, *Neural Networks and Deep Learning*, Springer, Berlin, Germany, 2018.

[20] T. Poongodi, A. Rathee, R. Indrakumari, 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.

[21] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the internet of things: a survey of existing protocols and open research issues," *IEEE Communications Surveys Tutorials*, vol. 170, no. 3, pp. 1294–1312, 2015.

[22] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: a survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys Tutorials*, vol. 170, no. 4, pp. 2347–2376, 2015.

[23] N. Garg, M. Wazid, A. K. Das, D. P. Singh, J. J. P. C. Rodrigues, and Y. Park, "BAKMP-IoMT: design of blockchain enabled authenticated key management protocol for internet of medical things deployment," *IEEE Access*, vol. 8, pp. 95956–95977, 2020.

[24] R. M. Amir Latif, K. Hussain, N. Z. Jhanjhi, A. Nayyar, and O. Rizwan, "A remix IDE: smart contract-based framework for the healthcare sector by using blockchain technology," *Multimedia Tools and Applications*, 2020.

[25] 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.

[26] K.-K. R. Choo, S. Gritzalis, and J. H. Park, "Cryptographic solutions for industrial internet-of-things: research challenges and opportunities," *IEEE Transactions on Industrial Informatics*, vol. 140, no. 8, pp. 3567–3569, 2018.

[27] S. S. Seshadri, D. Rodriguez, M. Subedi et al., "IoTCop: 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.

[28] P. Kumar, A. Gurtov, J. Iinatti, M. Ylianttila, and M. Sain, "Lightweight and secure session-key establishment scheme in smart home environments," *IEEE Sensors Journal*, vol. 16, no. 1, pp. 254–264, 2016.

[29] A. Braeken, P. Porambage, M. Stojmenovic, and L. Lambrinos, "eDAAAS: efficient distributed anonymous authentication and access in smart homes," *International Journal of Distributed Sensor Networks*, vol. 120, no. 12, 11 pages, 2016.

[30] 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.

[31] 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.

[32] O. Friha, M. A. Ferrag, L. Shu, L. Maglaras, and X. Wang, "Internet of Things for the future of smart agriculture: a comprehensive survey of emerging technologies," *IEEE/CAA Journal of Automatica Sinica*, vol. 80, no. 4, pp. 718–752, 2021.

[33] N. Ahmed, D. De, and I. Hussain, "Internet of Things (IoT) for smart precision agriculture and farming in rural areas," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4890–4899, 2018.

[34] A. P. Singh, N. R. Pradhan, A. K. Luhach et al., "A novel patient-centric architectural framework for blockchain-enabled healthcare applications," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 8, pp. 5779–5789, 2021.

[35] A. Ullah, M. Azeem, H. Ashraf, A. A. Alaboudi, M. Humayun, and N. Z. Jhanjhi, "Secure healthcare data aggregation and transmission in IoT-a survey," *IEEE Access*, vol. 9, pp. 16849–16865, 2021.

[36] 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.

[37] 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.

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

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

[40] 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.

[41] C. Li and B. Palanisamy, "Privacy in Internet of Things: from principles to technologies," *IEEE Internet of Things Journal*, vol. 60, no. 1, pp. 488–505, 2019.

[42] M. Zhaofeng, M. Jialin, W. Jihui, and S. Zhiguang, "Blockchain-based decentralized authentication modeling scheme in edge and IoT environment," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2116–2123, 2021.

[43] Y. Aydin, G. K. Kurt, E. Ozdemir, and H. Yanikomeroglu, "A flexible and lightweight group authentication scheme," *IEEE internet of things Journal*, vol. 7, no. 10, pp. 10277–10287, 2020.

[44] B. Hammi, A. Fayad, R. Khatoun, S. Zeadally, and Y. Begriche, "A lightweight ECC-based authentication scheme for Internet of Things (IoT)," *IEEE Systems Journal*, vol. 14, no. 3, pp. 3440–3450, 2020.

[45] Z. Liu, C. Guo, and B. Wang, "A physically secure, lightweight three-factor and anonymous user authentication protocol for IoT," *IEEE Access*, vol. 8, pp. 195914–195928, 2020.

[46] D. Johnson, A. Menezes, and S. Vanstone, "The Elliptic Curve Digital Signature Algorithm (ECDSA)," *International Journal of Information Security*, vol. 1, no. 1, pp. 36–63, 2001.

[47] L. Zhu, F. R. Yu, Y. Wang, B. Ning, and T. Tang, "Big data analytics in intelligent transportation systems: a survey," *IEEE Transactions on Intelligent Transportation Systems*, vol. 200, no. 1, pp. 383–398, 2019.

[48] D. Fang, Y. Qian, and R. Q. Hu, "A flexible and efficient authentication and secure data transmission scheme for IoT applications," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3474–3484, 2020.

[49] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[50] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Transactions on Computers*, vol. 51, no. 5, pp. 541–552, 2002.

[51] R. Canetti and H. Krawczyk, "Universally composable notions of key exchange and secure channels," in *Advances in Cryptology — EUROCRYPT*, L. R. Knudsen, Ed., pp. 337–351, Springer, Berlin, Heidelberg, 2002.

[52] Z. Ali, S. A. Chaudhry, M. S. Ramzan, and F. Al-Turjman, "Securing smart city surveillance: a lightweight authentication mechanism for unmanned vehicles," *IEEE Access*, vol. 8, pp. 43711–43724, 2020.

[53] S. Sayeed and H. Marco-Gisbert, "Assessing blockchain consensus and security mechanisms against the 51% attack," *Applied sciences*, vol. 9, no. 9, p. 1788, 2019.

[54] X. Liu, Q. Liu, T. Peng, and J. Wu, "Dynamic access policy in cloud-based personal health record (PHR) systems," *Information Sciences*, vol. 379, pp. 62–81, 2017.

[55] S. Saha, A. K. Sutrala, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues, "On the design of blockchain-based access control protocol for IoT-enabled healthcare applications," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, pp. 1–6, Dublin, Ireland, Ireland, 2020.

[56] X. Xiang, M. Wang, and W. Fan, "A permissioned blockchain-based identity management and user authentication scheme for E-health systems," *IEEE Access*, vol. 8, pp. 171771–171783, 2020.

[57] J. Xu, K. Xue, S. Li et al., "A blockchain-based privacy preserving scheme for large-scale health data," *IEEE Internet of Things Journal*, vol. 60, no. 5, pp. 8770–8781, 2019.

[58] G. S. Aujla and A. Jindal, "A decoupled blockchain approach for edge-envisioned IoT-based healthcare monitoring," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 2, pp. 491–499, 2021.

[59] A. Islam and S. Young Shin, "A blockchain-based secure healthcare scheme with the assistance of unmanned aerial vehicle in Internet of Things," *Computers & Electrical Engineering*, vol. 84, article 106627, 2020.

[60] A. Broring, S. Schmid, C.-K. Schindhelm et al., "Enabling IoT ecosystems through platform interoperability," *IEEE Software*, vol. 34, no. 1, pp. 54–61, 2017.

[61] P. Hao and X. Wang, "Integrating PHY security into NDN-IoT networks by exploiting MEC: authentication efficiency, robustness, and accuracy enhancement," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 50, no. 4, pp. 792–806, 2019.

[62] A. Y. Khan, R. Latif, S. Latif, S. Tahir, G. Batool, and T. Saba, "Malicious insider attack detection in IoTs using data analytics," *IEEE Access*, vol. 8, pp. 11743–11753, 2020.