Future Generation Computer Systems 110 (2020) 721–743

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

BlockIoTIntelligence: A Blockchain-enabled Intelligent IoT Architecture with Artificial Intelligence

Sushil Kumar Singh, Shailendra Rathore, Jong Hyuk Park *

Department of Computer Science and Engineering, Seoul National University of Science and Technology, (SeoulTech) Seoul 01811, Korea

ARTICLE INFO

Article history:
Received 23 June 2019
Received in revised form 13 August 2019
Accepted 6 September 2019
Available online 12 September 2019

Keywords:
Artificial intelligence
Blockchain
Internet of things
Big data analysis
Security and privacy

ABSTRACT

In the recent year, Internet of Things (IoT) is industrializing in several real-world applications such as smart transportation, smart city to make human life reliable. With the increasing industrialization in IoT, an excessive amount of sensing data is producing from various sensors devices in the Industrial IoT. To analyzes of big data, Artificial Intelligence (AI) plays a significant role as a strong analytic tool and delivers a scalable and accurate analysis of data in real-time. However, the design and development of a useful big data analysis tool using AI have some challenges, such as centralized architecture, security, and privacy, resource constraints, lack of enough training data. Conversely, as an emerging technology, Blockchain supports a decentralized architecture. It provides a secure sharing of data and resources to the various nodes of the IoT network is encouraged to remove centralized control and can overcome the existing challenges in AI. The main goal of our research is to design and develop an IoT architecture with blockchain and AI to support an effective big data analysis. In this paper, we propose a Blockchain-enabled Intelligent IoT Architecture with Artificial Intelligence that provides an efficient way of converging blockchain and AI for IoT with current state-of-the-art techniques and applications. We evaluate the proposed architecture and categorized into two parts: qualitative analysis and quantitative analysis. In qualitative evaluation, we describe how to use AI and Blockchain in IoT applications with "AI-driven Blockchain" and "Blockchain-driven AI." In quantitative analysis, we present a performance evaluation of the BlockIoTIntelligence architecture to compare existing researches on device, fog, edge and cloud intelligence according to some parameters such as accuracy, latency, security and privacy, computational complexity and energy cost in IoT applications. The evaluation results show that the proposed architecture performance over the existing IoT architectures and mitigate the current challenges.

1. Introduction

Information of things is a method for providing the connection between peripherals and human to the internet known as the Internet of Everything (IoE). Peripherals are capable of performing communication with each other; it includes smart homes, smart vehicle, and intelligent automotive. Internet of Things (IoT) provides solutions in many fields for optimizing productions efficiently. However, IoT has many issues, such as big data analytics, security, connectivity, centralization, hardware capabilities, and GIS visualization, and so on. According to Proofpoint, Inc., (NASDAQ: PFPT) report, more than 750,000 consumer devices were compromised to distribute phishing and spam emails in the year of 2014 [1]. Chung et al. [2] described that the internet is a source of generating enormous amounts of data from IoT applications accumulated speedily. Hence big data analysis is a significant issue in IoT Applications. To mitigate this issue, many researchers propose Artificial Intelligence (AI) technology such as Deep Learning (DL), Reinforcement Learning (RL) for IoT applications [3]. For the analysis of a large amount of data and provide useful information to the decision analysis, prediction, classification, and detection of future actions in IoT, the DL analytical tool is often employed. DL enables feature extraction and scaling of IoT big data generated and collected from various IoT applications [4]. Atlam et al. [5] studied the integration of AI and IoT, its benefits, opportunities, and challenges in various IoT applications. Lee et al. [6] proposed a user-oriented IoT system; it utilized two types of mechanism: bidirectional processing mechanism and an uncertainty-driven arbitration mechanism. A bidirectional processing machine is used for intimate knowledge (human knowledge), observation of external experience (communication networks) and uncertainty-driven arbitration mechanism used for big data analytics.

* Corresponding author.
E-mail addresses: sushil.sngh001007@seoultech.ac.kr (S.K. Singh), rathoreshailendra@seoultech.ac.kr (S. Rathore), jhpark1@seoultech.ac.kr (J.H. Park).

https://doi.org/10.1016/j.future.2019.09.002
0167-739X/© 2019 Published by Elsevier B.V.

Various framework and architecture are used in existing researches to support efficient big data analysis and handle computation load in IoT applications. The existing studies can be divided into four categories: (1) Cloud analysis, (2) Fog analysis, (3) Edge analysis, and (4) Device analysis. In cloud analysis, a single system is used for big data analysis at a cloud server. However, due to a centralized server, it has many issues such as low accuracy, low speed, low latency, less computational storage and single point of failure because of IoT applications generates a massive amount of data. Fog analysis is used where the data collection and load balancing of the system are utilized in a distributed manner of IoT data to resolves these issues. However, the cloud server is a central controller, and it has significant control over the fog intelligence. So, the fog analysis has also some issues such as resource management, scalability, and so on. Edge analysis is adopted for the architecture where distribute the load in two manners to mitigate these issues. The edge node completes the training task, and cloud server completes the processing task. Feature extraction and scaling of data are completed at edge layer and processing, analyzing of data at the cloud analysis. However, edge analysis has also some issues, such as excellent communication, energy consumption, privacy, and security. To address these issues, device intelligence is utilized where every device connected to others with peer to peer manner.

We find out major challenges from existing studies that require solving to design an effective big data analysis approach for IoT applications: (a) Lack of accuracy, (b) Low latency, (c) Security and privacy, and (d) Centralization. To mitigate these issues, Blockchain technology is adopted because it has many advantages. Blockchain is a secure, decentralized, and distributed database technology. All nodes in blockchain networks are connected in a distributed manner where all transactions and timestamp are recorded quickly and shared transaction without the use of the third party. Blockchain technology has appropriate solutions for various fields such as finance, data security, agriculture, and healthcare in IoT. The data stored in blocks are attached in a chain through a hash function (cryptographic structure includes timestamp and link to the previous block). Since every block connects to the last block, it is not possible to hack the transaction by any malicious system in the network of the blockchain technology. The convergence of Blockchain and AI for IoT have various concepts for mitigating the issues such as decentralization, digitally signed, distributed, validated, public digital ledger, smart contract, immutable, secure share data, and explainable AI. In recent years, IoT devices are collecting a massive amount of data in a centralized form; then security and space problems are generated [7]. To mitigate this problem, using a decentralized database implemented in the convergence of Blockchain and AI on IoT [8]. If any person wants to share the transaction with another person in IoT application, therefore, the transaction should be immutable, secure, explainable, digitally signed, and validated. These concepts provide a considerable amount of data securely, which is used in many applications such as healthcare, agriculture, smart home, military, government, and smart transportation [9]. A smart contract is a program used in the blockchain network for providing security and is stored in the digital ledger [10].

Integration of Blockchain and AI supports to address the accuracy, latency, centralization, and security and privacy. Database in blockchain technology holds the transactions with a digitally signed hash value. Therefore, accuracy, latency, security and privacy, and centralization issues to mitigate. AI algorithms are also used to solve these issues. With the property of decentralization to automatic and fast validation of data in blockchain networks, resolves a single point of failures in a cloud server for big data analysis and blockchain help to the IoT with AI. Rathore et al. [4] provide the security architecture for IoT networks to deliver secure and scalable IoT data from an IoT application with decentralized way at fog layer. It resolves the centralization issue of IoT network. In human's everyday life, AI is used in various areas of advanced technologies such as blockchain thinking [11], decentralized AI [12] the intelligence of things, intelligent machines and so on in human's every life. The convergence of AI and IoT provide the way for collecting maximum information, analyze it. It finds appropriate learning which is used for many applications such as healthcare, smart home, smart farming, and intelligent vehicle, and so on. Rathore et al. [3] proposed blockchain-based secure DL methods to provide reliable data in IoT application with the convergence of blockchain and AI at the device layer. It achieves high accuracy, high latency for IoT data. Gil et al. [13] studied intelligent machines in which eliminates a human's effort in many fields such as medical science, automatic sensing devices, automated vehicle driving, and cooking. Intelligence is the ability to contribute accumulated knowledge to solve complex problems, while AI is the learning method to the growth of creative techniques and share the original collected thought. According to McKinsey's report [14], AI market will grow up to 13 trillion US dollars by the year of 2030 in market research expresses an outcome in advance recently. Decentralized AI method is a combination of AI and Blockchain; it is used to share the information in cryptographically signed, secured, and trusted manner without the use of the third party. It also has decision-making capabilities for machines to taken decision automatically in IoT applications. In the last years, with continuous change in technologies, devices, and IoT devices, Blockchain, AI, and IoT have become most contributing technologies that are catalyzing the pace of innovation ideas in every area. The fundamental concept of Blockchain and AI for IoT is shown in Fig. 1.

This paper discusses the issue of privacy, accuracy, latency, and centralization by converging Blockchain and AI in IoT applications. The convergence of Blockchain and AI is utilized to propose a Blockchain-enabled Intelligent IoT Architecture with AI where Blockchain-enabled decentralized cloud used at the cloud layer, Blockchain-based distributed fog networks applied at the fog layer, Blockchain-based distributed edge networks utilized at the edge layer and peer to peer blockchain networks converged at the device layer and mitigate the recent challenges. The primary goal of our study is the integration of Blockchain and AI to support secure, decentralized big data analysis for IoT applications.

Research contribution: The main contributions of our research are as follows:

- We study the Blockchain and AI for IoT and summarize their existing researches with the specified table.
- Based on the advantages of Blockchain and AI, we design and develop a BlockIoTIntelligence: A Blockchain-enabled Intelligent IoT Architecture with Artificial Intelligence that includes four-intelligence: cloud intelligence, fog intelligence, edge intelligence, and device intelligence with the adoption of blockchain and AI at each intelligence to achieve the goal of secure, decentralized big data analysis for IoT applications.
- We provide the methodological flow of the proposed BlockIoTIntelligence architecture with the convergence of Blockchain and AI in IoT layered framework.
- We evaluate the proposed architecture in two types of analysis: qualitative and quantitative. In qualitative analysis, how AI mitigates the issues in Blockchain is known as "AI-driven Blockchain" and how Blockchain mitigates the issues in AI is known as "Blockchain-driven AI". In quantitative analysis, we present a performance evaluation of the BlockIoTIntelligence architecture to compare existing researches

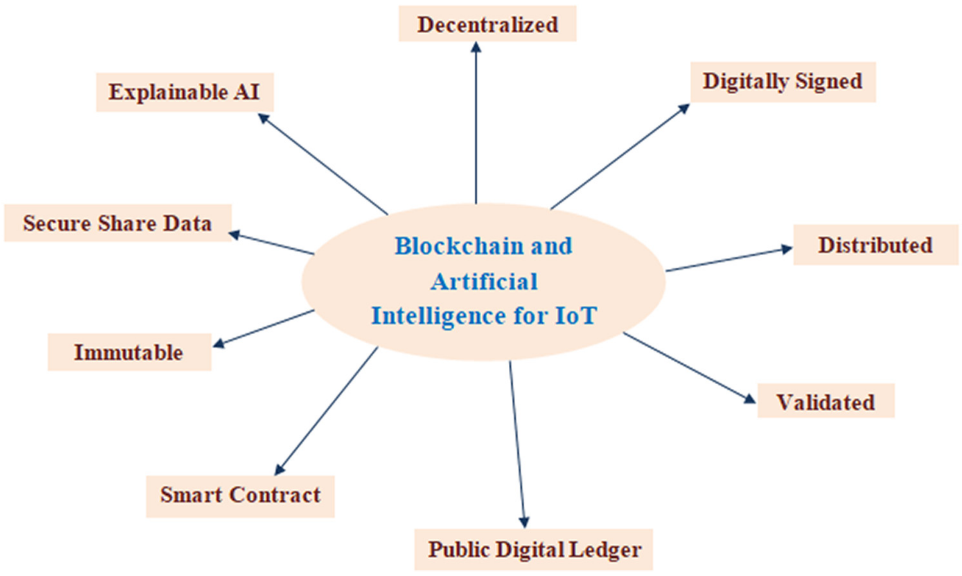


Fig. 1. The Fundamental Concept of Blockchain and AI for IoT.

Table 1
Contribution of our study related with existing research.

Research work	Year	Technological aspects	Blockchain driven AI	AI-driven blockchain	Research challenges	Proposed architecture
Rathore et al. [3]	2019	Blockchain + AI	Limited	Yes	Limited	Yes
Rathore et al. [4]	2019	Blockchain + AI	Limited	Yes	Limited	Yes
Atlam et al. [5]	2018	IoT + AI	Limited	Yes	Limited	Yes
Zheng et al. [8]	2017	Blockchain	Limited	Limited	Yes	No
Wright et al. [10]	2018	Blockchain + IoT + Edge Computing	Limited	Limited	No	Yes
Swan et al. [11]	2015	Blockchain + AI	Limited	Yes	Limited	No
Salah et al. [15]	2019	Blockchain + AI	Yes	No	Limited	No
Qian et al. [16]	2018	Blockchain + IoT	Yes	Limited	Limited	Yes
Kshetri et al. [17]	2017	Blockchain + IoT	Yes	No	Limited	No
Reyna et al. [18]	2018	Blockchain + IoT	Limited	No	Yes	No
Banerjee et al. [19]	2017	Blockchain + IoT	Yes	No	No	No
Li et al. [20]	2017	Blockchain	No	No	Yes	Yes
Xu et al. [21]	2017	Blockchain + AI	Yes	Limited	No	Yes
Lin et al. [22]	2018	Blockchain + IoT	Limited	Limited	No	Yes
Lu et al. [23]	2018	Blockchain	No	No	Yes	No
Rathore et al. [24]	2019	Blockchain + AI + SDN	Yes	Limited	Yes	Yes
Vukobratovic et al. [25]	2016	AI + IoT	No	No	Yes	Yes

on device, fog, edge and cloud intelligence considering standard parameters such as accuracy, latency, security and privacy, computational complexity and energy cost in IoT applications.
- Finally, we summarize and discuss the research challenges and their solutions in the proposed BlockIoTIntelligence architecture.

The rest of the paper is organized as follows; in Section 2, we describe related works on IoT, AI, and Blockchain. In Section 3, we discuss proposed BlockIoTIntelligence with architecture overview and methodological flow of the proposed architecture. In Section 4, we evaluate the architecture with qualitative analysis and quantitative analysis. In qualitative analysis, we present how to use AI and Blockchain in IoT application as AI-driven Blockchain and Blockchain-driven AI with high-level taxonomy structure. In quantitative analysis, we present a performance evaluation of the BlockIoTIntelligencearchitecture to compare existing studies in terms of standard parameters in IoT applications. We present research challenges and provide solutions to the proposed architecture in Section 5. Finally, we conclude our research in Section 6.

2. Related work

In this section, we discuss the basic concepts of Blockchain and AI for IoT and how blockchain and AI transform IoT. Blockchain and AI are the core technologies for IoT applications. Blockchain is used for providing a decentralized and distributed platform for IoT applications. On the other hand, AI is utilized for analyzing and processing the data in IoT applications, offers intelligent and decision making capabilities for the machine to human. We summarize the contribution of the existing researches with Table 1.

2.1. Blockchain

Blockchain is a collection of blocks, and each block has four parts: details of the transaction (bitcoin, ethereum), the hash value of the present block and the previous block, and timestamp. Blockchain technology is a decentralized, distributed, and public digital ledger that is utilized for saving the transaction in various nodes. Therefore, any third person involved record cannot alter because every block has a cryptographic value of the previous block and own itself. In blockchain technology, every transaction is cryptographically signed with hash value and verified by all

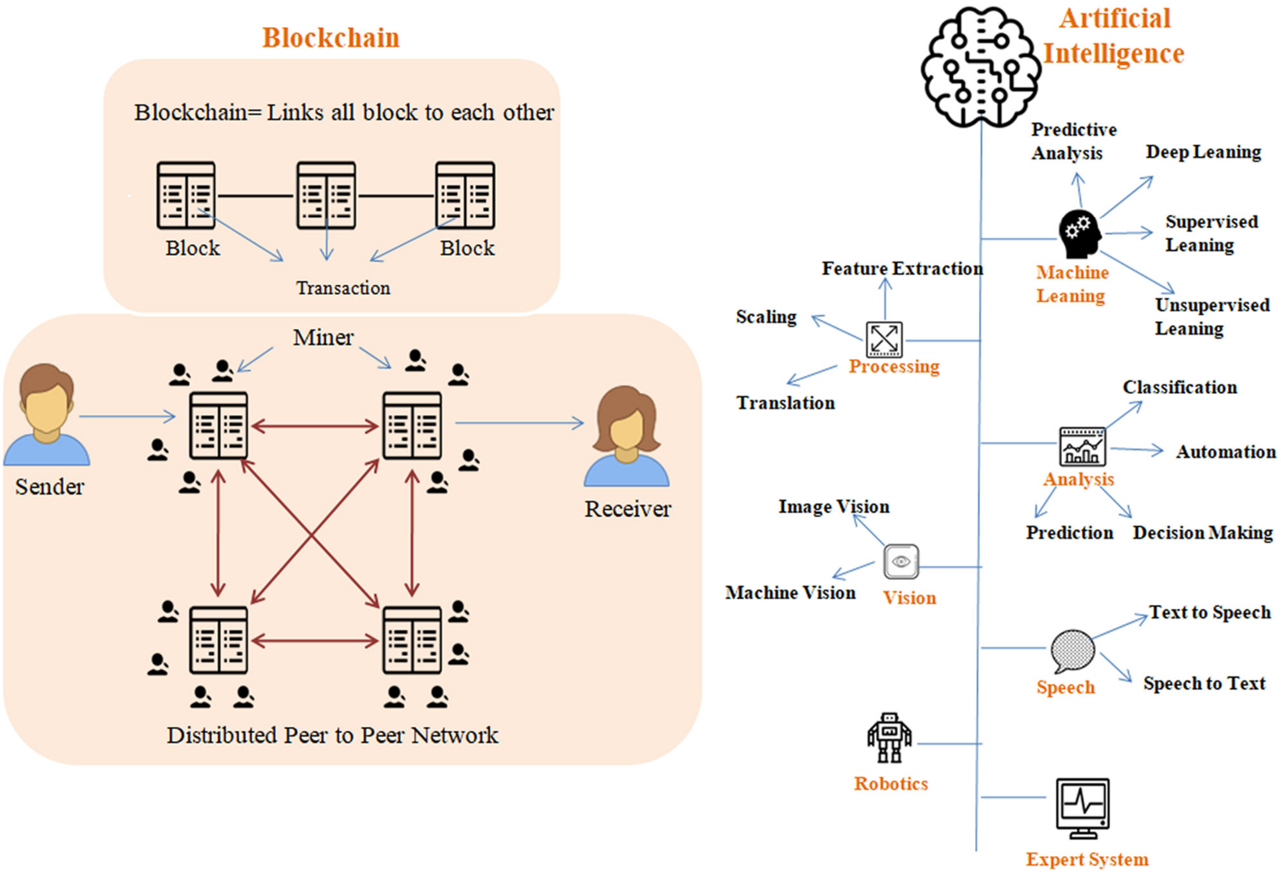


Fig. 2. Basic concept of Blockchain and Artificial Intelligence.

miners. It holds a duplicate value of the entire ledger and contains blocks of all transactions; as described in Fig. 2. Blockchain provides the ability to share the ledger of data in decentralized, distributed, secure, and trusted form [15]. Decentralized storage is the way of blockchain and used for storing a large amount of data which is linked the current block to the previous block by smart contract code. Swarm, LitecoinDB, MoneroDB, SiacoinDB, IPFS, BigchainDB, and so on are used for the decentralized database in today's current scenario [15]. The Interplanetary File System (IPFS) is a Point to Point, decentralized, and distributed database that is connected and transfers common files [26,27]. IPFS is a substantial storage medium, which is used by blockchain technology for IoT applications for high throughput [28].

Atzori et al. [29] described three categories of IoT: internet-oriented, sensor oriented, and knowledge oriented. Internet-oriented IoT refers to a combination of devices connected by the internet, which generate the massive size of data. Sensor oriented IoT is the use of sensor-related accessories such as RFID. Knowledge-oriented IoT means to a collection of knowledgable data, and it used for IoT application. IoT is an emerging technology that has a combination of various devices with a unique address and communicates with each other by the internet simultaneously. The massive amount of data has a security vulnerability, privacy, and fault tolerance challenges in IoT applications. To mitigate these challenges, many researchers propose blockchain technology for IoT. Blockchain-related techniques provide a decentralized and distributed architecture for security, vulnerability, and privacy and fault tolerance; they involve significant energy consumption, computational overhead, and less delay, Security and privacy in IoT are provided by blockchain technology in various applications such as smart home, smart city, healthcare, and agriculture. Blockchain concept offers a peer to peer network for authentication, robustness against attacks. Integration of blockchain and IoT has a holistic approach, and it used for extensive data management and development complexity.

2.2. Artificial intelligence

Any automatic machine can perform various functions such as perceiving, learning, reasoning, and solve the problem automatically is known as artificial intelligence. Machine learning, deep learning, and neural network are using for solving the complex problem automatically, and the benchmark for AI is the human level concerning reasoning, speech, and vision. Peer to peer blockchain node in device intelligence is used for data collection and recorded. Blockchain-based distributed fog node in edge fog intelligence is utilized for processing of data. Analysis of big data is completed in cloud intelligence. AI technology provides exceptional decision-making skills to machines for human tasks. The devices are capable of completing the tasks automatically; otherwise, it needs a human brain. In AI, to create devices that possess capabilities similar to human intelligence, are based on three levels, superintelligence, general AI, and narrow AI. Intelligence machines are used to remove the tasks of human in many fields such as medical science, automatic sensing devices, automated vehicle driving, and mechanized farming [29]. AI is the mechanism in which find the knowledge of the intelligent agent. It takes raw data as input and performs decision making, and finally gives the maximum outputs for a specific purpose [30].

Recently many researchers found various challenges in IoT such as big data analytics, security, and privacy, traffic congestion, and energy efficiency. To address these challenges, AI techniques for IoT has developed, such as machine learning, deep learning. With the use of deep learning, energy efficiency issue is solved in IoT based of the smart building in which the main parameters such as data association, data prediction are analyzed and included in building energy management to help designers select the most useful settings to control energy consumption [31]. Machine learning is used to identify patterns, anomalies, and make a prediction based on a massive amount of data which is generated by IoT application such as healthcare, transportation, weather forecasting, and industrial IoT. With the use of automated decision-making capability and control activities like streamline decision making, devices optimize the operations; manage warehouses, decrease downtime, and repairs in transportation management. With ML-based IoT authentication, it provides IoT security solution based on machine learning techniques which include supervised, unsupervised and reinforcement learning, access control, secure offloading, and malware detection schemes to protect data privacy [32,33]. By applying the analytics capabilities in AI for data collection by IoT applications and companies, we identify patterns and provide more informed decisions for a new ecosystem. Basic techniques are used in AI and basic concepts, as described in Fig. 2.

2.3. Existing research

Many researchers have studied and discussed the open research issues of Blockchain for AI, and AI for Blockchain on IoT. Atlam et al. [5] described an overview of the integration of IoT and AI, integration benefits and opportunities of AI in different IoT Applications and presented the challenges and discussion for successful convergence of IoT with AI. Zheng et al. [8] presented blockchain technology in four categories: (a) blockchain taxonomy and key characteristics, (b) consensus algorithm, (c) blockchain Applications, and (d) technical challenges in the existing research. Wright et al. [10] introduced an Ethereum based smart edge for smart contract computing and demonstrated that it is a low price and high accuracy tools for resource management. It allows nodes to offload calculation in a verifiable manner to edge devices in exchange for payment. Swan et al. [11] discussed the benefits of Blockchain thinking for AI and human enhancement, architectural proposal for blockchain thinking, processing of Blockchain thinking in AI. Salah et al. [15] presented an overview of Blockchain applications for AI and identified open research challenges of utilizing Blockchain for AI. They reviewed the literature, summarized Blockchain applications, and platform protocols targeting AI areas. Qian et al. [16] presented three layers of IoT, perception layer, network layer and application layer, the security problems of each three layers, high-level security management methods based on blockchain technology for different IoT devices, and open research problems. Their research included abnormal network traffic monitoring based on machine learning and identity verification. Kshetri et al.'s research [17] categorized IoT challenges into four categories: (a) Costs and Capacity Constraints (b) Deficient Architecture (c) Cloud server downtime and unavailability of services (d) Susceptibility to manipulation. Their research included Potential Blockchain solution on each challenge of IoT and Blockchain role in improving overall security in supply chain networks.

Reyna et al. [18] analyzed how Blockchain could potentially improve the IoT, discussed the relationship of Blockchain and IoT, presented investigation challenges in Blockchain IoT Applications, and surveyed the most relevant work to analyze how blockchain improves the IoT. Banerjee et al. [19] studied IoT security solutions, including the lack of IoT datasets, which are used by both research and expert communities. Given the potentially conscious nature of IoT datasets, there is a need to develop a standard for sharing IoT data values among the research and expert communities and other relevant colleagues and provide Blockchain technology in future for the security in IoT applications. Li et al. [20] presented a systematic study on the security threats to blockchain and discussed similar real attacks by expanding popular Blockchain systems. They reviewed the security enhancement solutions for blockchain technology. Lin et al. [22] proposed an open and ecological food traceability system, which is based on Blockchain and IoT. It is a trusted, self-organized, open, and is ecological for smart agriculture ecosystem. Lu et al. [23] studied the basic features and categories of Blockchain and delineated the practical applications. They investigated the development prospects of blockchains through analysis of existing applications and technologies. Vukobratovic et al. [25] proposed novel architecture about reconfigurable knowledge acquisition system for data analysis at the cloud layer by e-route processing. It is achieved via network function virtualization (NFV), software-defined network (SDN), and machine learning.

Table 1 provides a comparison of several existing studies in terms of technological aspects, "blockchain-driven AI", "AI-driven blockchain", and research challenges with solutions. Our study differs significantly from other existing studies in terms of providing integrated discussion, extensiveness, and comprehensiveness to convergence blockchain and AI for IoT. Based on the study, we present a BlockIoTIntelligence architecture for IoT by deploying the Blockchain and AI.

As described in the preceding section, the existing research faces significant challenges, such as lack of privacy, low accuracy, centralization, low latency, and a massive amount of data. Our research focuses on the convergence of blockchain and AI technology at the cloud, fog, edge, and device layer to mitigate these challenges. Rathore et al. [4] provide the security architecture for IoT networks to deliver secure and scalable IoT data from an IoT application with decentralized way at fog layer. It resolves the centralization issue of IoT network. Atlam et al. [5] provided an overview of the integration of AI and IoT robust technology to increase operating efficiency and avoid unplanned downtime in IoT applications. Qian et al. [16] proposed a high-profile security management scheme based on blockchain for IoT devices. However, this research has abnormal traffic monitoring and identity verification issues. Rathore et al. [3] proposed blockchain-based secure DL methods to provide reliable data in IoT application with the convergence of blockchain and AI at the device layer. It achieves high accuracy, high latency for IoT data. Xu et al. [21] proposed blockchain-based decentralized resource management framework for resolving resource management problem using dynamic voltage frequency algorithm. As benefited from the integration of blockchain and AI for IoT, BlockIoTIntelligence architecture is introduced in the subsequent section.

3. Proposed BlockIoTIntelligence architecture

In this section, we propose a BlockIoTIntelligence architecture that converges the blockchain and AI for IoT with above-discussed challenges and applications. The proposed architecture is divided into four intelligence namely cloud intelligence, fog intelligence, edge intelligence and device intelligence which is used to demonstrate how to converge Blockchain and AI to achieve the goal of big data analysis, security, and centralization issues of IoT applications such as smart healthcare, smart city, and smart transportation.

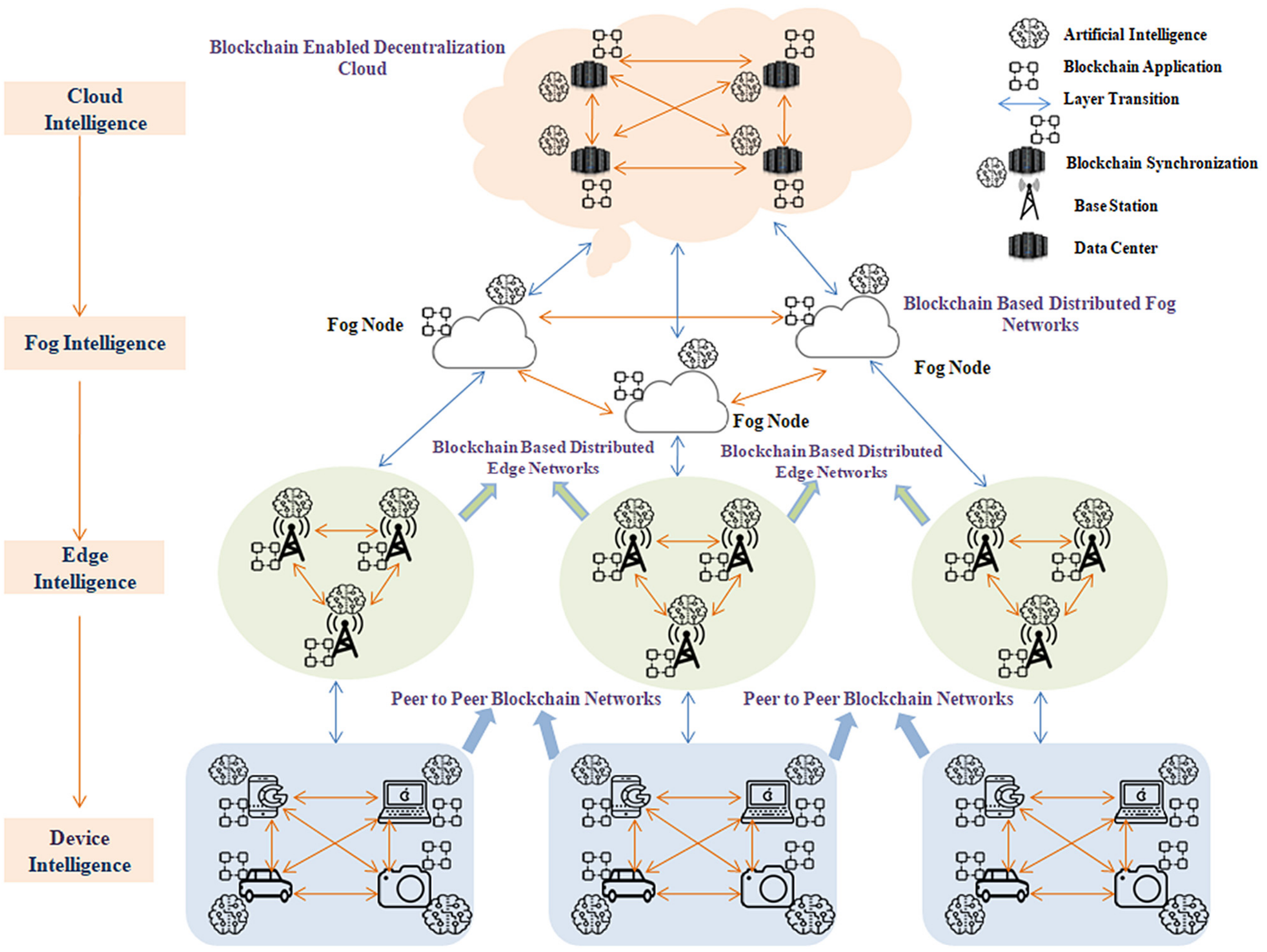

Cloud Intelligence
Fog Intelligence
Edge Intelligence
Device Intelligence
Blockchain Enabled Decentralization Cloud
Artificial Intelligence
Blockchain Application
Layer Transition
Blockchain Synchronization
Base Station
Data Center
Fog Node
Blockchain Based Distributed Fog Networks
Fog Node
Fog Node
Blockchain Based Distributed Edge Networks
Blockchain Based Distributed Edge Networks
Peer to Peer Blockchain Networks
Peer to Peer Blockchain Networks

Fig. 3. The design overview of the proposed BlockIoTIntelligence Architecture.

3.1. Architecture overview

We present an overview of the proposed architecture illustrated in Fig. 3, which is a hierarchically layered structure consisting of four intelligence: (1) Device intelligence, (2) Edge intelligence, (3) Fog intelligence and (4) Cloud intelligence. The device intelligence consists of various IoT devices with AI and blockchain applications; it produces a massive amount of data, which is transferred to the edge intelligence. Subsequently, the edge intelligence consists of AI-enabled base stations connected to the blockchain at the edge of the network. Each AI-enabled base station at the edge intelligence is connected to the number of sensing devices and its analyze and process the traffic data from sensing devices. The process data from edge intelligence are reported to the fog intelligence, which is a combination of several AI-enabled fog nodes with Blockchain. Each AI-enabled fog node with blockchain is associated with the composing of AI-enabled base stations at the edge intelligence and responsible for processing data to the cloud intelligence. Finally, cloud intelligence consists of AI-enabled data centers that are connected to the blockchain to provide decentralized and secure big data of IoT applications such as smart healthcare, smart transportations, and so on. Moreover, each data center declares the outputs of its data processing to the cloud intelligence for controlling a large amount of data analysis resolve low accuracy, latency, privacy issues for IoT. We discuss BlockIoTIntelligence Architecture of converging Blockchain and AI for IoT in thoroughly as following

Device Intelligence: It is the first layer of the proposed BlockIoTIntelligence architecture of converging Blockchain and AI for IoT applications. The device intelligence has several IoT devices and sensors, which produces a massive amount of data by IoT applications. Therefore, device intelligence in architecture is used for data collection, and these data are forwarded to the edge intelligence. AI technology is adopted in device intelligence for collection the data with the learning process automatically. On the other hand, the blockchain provides a distributed method for security and privacy of IoT data. Rathore et al. [3] proposed Blockchain-based secure deep learning system by the convergence of blockchain and DL to provide the security and privacy of IoT data in applications. In device intelligence of proposed architecture, peer to peer blockchain network with AI is used for transferring the data from one IoT device to another in a distributed manner. IoT devices in peer to peer blockchain networks share the storing data to the edge intelligence. Blockchain-based distributed edge networks are supported to processing the IoT data in IoT applications.

Edge Intelligence: Another layer is edge intelligence for converging blockchain and AI for IoT applications. AI uses analytic tools for reliable data mining (feature extraction, scaling, and representation) of big unstructured data from IoT devices. It uses speech and images in IoT applications such as healthcare, transportation, and so on. Blockchain technology provided peer to peer connection to unstructured IoT devices in networks for security and privacy. It offers reliable, efficient learning tasks. Rathore et al. [24] used the convergence of blockchain and DL for IoT network with the secure deep learning approach for mitigating single point of failures issue with higher accuracy in a decentralized form. In edge intelligence of proposed architecture consists of blockchain-based distributed edge nodes which are connected to the fog intelligence and device intelligence. AI-enabled base stations with blockchain are utilizing in blockchain-based distributed edge node which is connected to several sensors and analyze the traffic data from sensors and IoT devices. Data collection and the computational task of the lower layer are shifted to the fog intelligence in a distributed manner. Resource management, scalability of networks, load balancing, and so on issues resolves by edge intelligence with the use of blockchain-based distributed edge networks. The convergence of Blockchain and AI in IoT are used in all edge node, which is providing a distributed and decentralized way for processing the data.

Fog Intelligence: The next intelligence layer of proposed BlockIoTIntelligence Architecture is fog intelligence for converging blockchain and AI for IoT. AI technologies are deployed to train machine learning models and make decisions as rapidly as possible at fog intelligence. Blockchain technology provides a distributed repository in which every device has its copy of the whole ledger. All the parties follow the standard rules and regulations to transferring the data on the IoT network at fog intelligence. Therefore, blockchain provides security and privacy for IoT application in IoT applications. To configure fog intelligence, we refer to Rathore et al. [4] research. It offered security architecture which used the convergence of blockchain, DL, and SDN to ensure an optimal attack detection. This research mitigated the centralization issue with less computation and high accuracy. We proposed a blockchain-enabled intelligence architecture in which several AI-enabled fog nodes are connected with blockchain in fog intelligence. Sharing the intermediate parameters or information of architecture to cloud intelligence by AI-enabled fog nodes. It provides training data in the network by blockchain. From the edge intelligence, the processed data are transferred to the fog intelligence, and it is responsible for processing data to the identity of traffic flow data in the IoT network. Fog node is used for analyzing the data at the fog intelligence. However, AI-enabled fog node has resource management, lack of data, energy consumption, and scalability challenges. Blockchain-based distributed fog networks are used and provide high availability, real-time data delivery, high complex computing to address these challenges.

Cloud Intelligence: Finally, cloud intelligence is used for proposed BlockIoTIntelligence architecture of converging Blockchain and AI for IoT. Intelligent agents of AI are used in cloud intelligence to collect, select, analyze the data from ambient environments using centralized methods. Blockchain provides the distributed pattern for secure big data analysis in IoT. Xu et al. [21] proposed blockchain-based decentralized resource management framework to addressed energy-aware resource management problem by the energy consumed by the request scheduler. To configure cloud intelligence, we refer to Xu et al.'s [21] research in our proposed architecture. Cloud intelligence consists of AI-enabled data centers. These are connected to the blockchain technology to provide decentralized and secure big data analysis of IoT applications in the proposed architecture. It is adopting for the IoT to solve various issues such as security, immutability, anonymity, and persistence. For cloud intelligence, every IoT device sends their data to the cloud server for big data analysis in the network. It provides high energy consumption, communication bandwidth to IoT data. Blockchain-enabled decentralization in cloud intelligence is used for providing high security with high accuracy to big data analysis of IoT applications.

3.2. Methodological flow of the proposed BlockIoTIntelligence architecture

A methodological flow of the proposed BlockIoTIntelligence architecture is illustrated in Fig. 4, where IoT platform is described as a combination of six layers: the physical layer, communication layer, link control layer, service layer, management layer, and application layer. The physical layer is correspondence to device intelligence, communication, and link control layer is related to edge intelligence, service, and management layer is connected to fog intelligence and application layer is relevant to cloud intelligence of proposed architecture. The physical layer used for identifying the data such as temperature, location, pollution, weather, motion, and agriculture in cloud intelligence. This information acquired from various sensor devices such as RFID, Barcode, and Infrared. This layer has different kinds of security threats and issues such as transferring the information from one place to another place, which makes it unsecure from malicious persons. To mitigate these issues, the concept of blockchain and AI is used where the transaction is in the form of bitcoin, lite coin, and Ethereum. The collected data transferred to the communication layer, which used as a medium for transferring information from one device to another device. It is done by implementing several advanced technologies such as wi-fi, Zigbee, radio, and infrared wave. This layer has security and privacy issues, blockchain and AI technology are used in point to point networks, and ubiquitous broadband used for encryption and authentication. Lin et al. [34] proposed that the communication layer is used primarily for transferring the information from the physical layer to the link layer in IoT. This layer has properties flow and error control and energy optimization.

The convergence of blockchain and AI for IoT use consensus protocols for scalability and security. It provides distribution and decentralization mechanism. Information is stored in decentralization form by using this layer [35]. Stored data is transferred to the service layer, which provides essential services such as decision support, database support, service composition and organization, virtual entity resolution, IoT service monitoring for IoT applications. The convergence of blockchain and AI for IoT uses distributed cloud and intelligent storage, micro-server, and smart contracts for secure authentication and validation in this layer. This information transfer to the management layer provides management of data, software, criteria, and infrastructure between networks to the application layer. With the convergence of blockchain and AI for IoT, it provides digital identity, hash function, micro-server, and scripting code for encryption. Finally, information shared with the application layer serves to ensure the global management of the applications used in IoT applications such as smart city, smart vehicle, smart healthcare, smart farming, intelligent transportation and others [36]. The convergence of blockchain and AI for IoT use some other techniques such as analytics intelligence, deep learning, machine to machine learning, and programmable learning used in smart technology [37,38]. Some of the significant features, as shown in Fig. 4, leverage blockchain and AI for IoT, which are summarized as follows:

Analytics Intelligence: A massive amount of data in IoT applications are generated or collected by billions of sensing devices in various fields. These devices provide the output in the form of significant data streams. Analytics intelligence is applied to these data streams to find new information ecosystem and give a prediction for the future scenario in IoT applications by deep learning, machine to machine learning, and programmable finance learning methods. Control decision is an essential method for IoT data stream, and it is used to provide the information in good quality. Therefore, AI is beneficial for IoT applications such as smart city, smart vehicle, and smart healthcare, and it

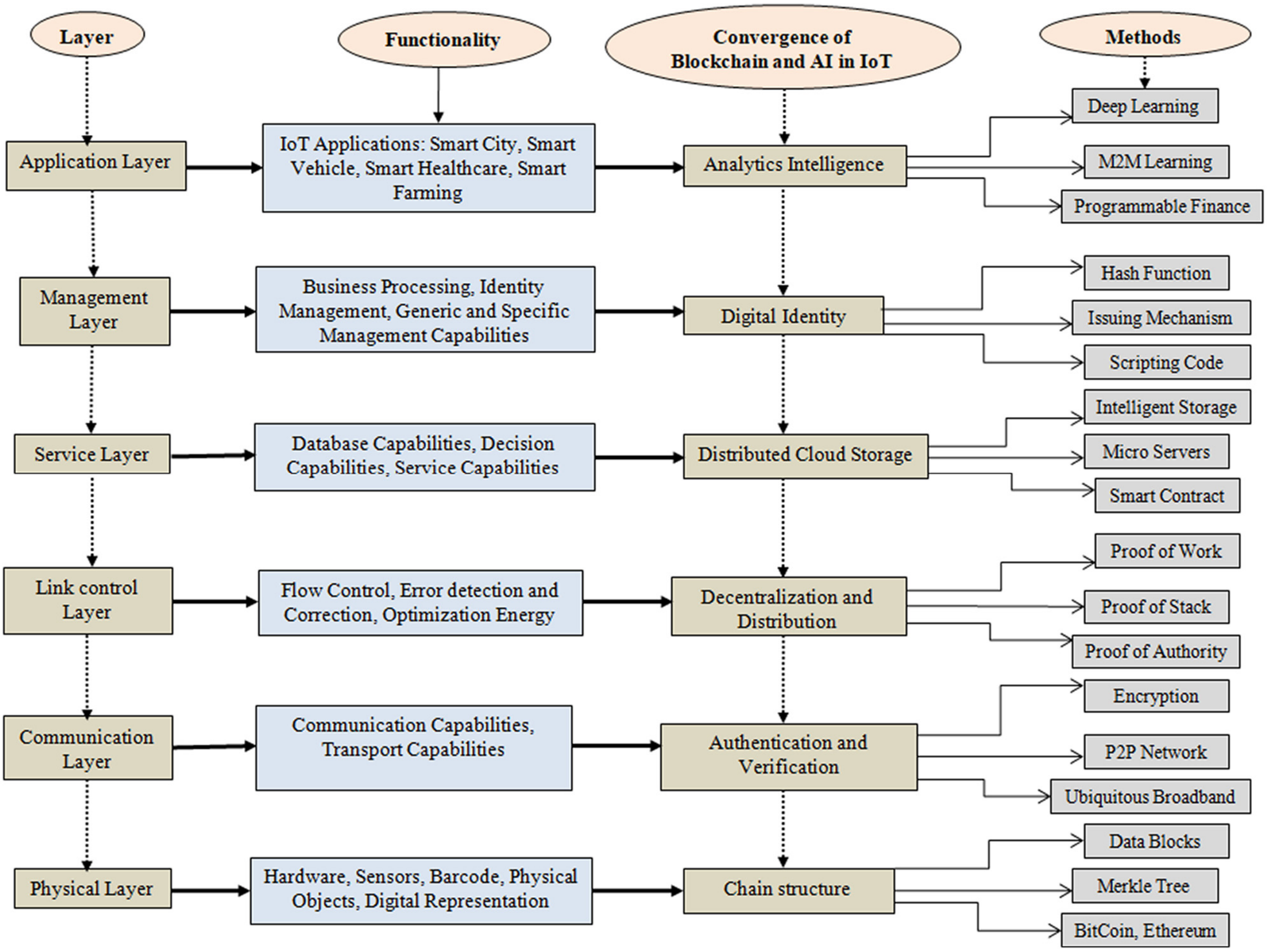

Layer
Functionality
Convergence of Blockchain and AI in IoT
Methods
Application Layer
IoT Applications: Smart City, Smart Vehicle, Smart Healthcare, Smart Farming
Analytics Intelligence
Deep Learning
M2M Learning
Programmable Finance
Management Layer
Business Processing, Identity Management, Generic and Specific Management Capabilities
Digital Identity
Hash Function
Issuing Mechanism
Scripting Code
Service Layer
Database Capabilities, Decision Capabilities, Service Capabilities
Distributed Cloud Storage
Intelligent Storage
Micro Servers
Smart Contract
Link control Layer
Flow Control, Error detection and Correction, Optimization Energy
Decentralization and Distribution
Proof of Work
Proof of Stack
Proof of Authority
Communication Layer
Communication Capabilities, Transport Capabilities
Authentication and Verification
Encryption
P2P Network
Ubiquitous Broadband
Physical Layer
Hardware, Sensors, Barcode, Physical Objects, Digital Representation
Chain structure
Data Blocks
Merkle Tree
BitCoin, Ethereum

Fig. 4. The methodological flow of the proposed BlockIoTIntelligence Architecture.

is a part of deep learning. The convergence of blockchain and AI for IoT represents an exceptional opportunity for the private and public sector. Every sector is capable of exploiting these technologies and has a chance for continuous enhancement of the existing process and finds new business strategies for developing innovative services in a new generation of consumers. It is based on the production of new thoughts or information. Analytics intelligence and blockchain technology may convert any environments such as hospitals, airports, school to a smart environment where decision-making capabilities and learning capabilities are used for all operations automatically quickly and securely.

Digital Identity: Digital identity is an emerging method used for various IoT applications. It mainly provides a unique identification address for the devices by the hash function, scripting code, and issuing mechanism methods. All devices interact with each other in a real-time, secure, and decentralized manner. When any company such as Flipkart and e-bay helps us track our packet from shipment to delivery, the barcode on the packet is the digital shipping identity. However, digital identity is a fundamental concept for sensors, automatic control system, and smart vehicle. With the convergence of blockchain and AI for IoT, it provides a digital identity for encrypting the data or converts the data in digital form because it is an encryption part, and anybody cannot use or hack wherever and whenever. Digital identity concept used in management and business layer provides management of data, information, applications in digitally and unique form. Using AI and blockchain for IoT, micro-robots applied on pesticides and herbicides; it captures detail performance of every individual plant [39]. It provides financial, operational advantages such as improved predictability in the crop, reduces crops lost to disease, the time and effort required, and reduces the use and overuse of pesticides and herbicides.

Distributed Cloud Storage: It is a core part of blockchain technology and used for storing the information in distributed and decentralized form in blockchain networks. These pieces of information can be verified by minors who follow the rules and regulation of a smart contract. This method provides complete traceability, transparency to the cloud in an artificial intelligent manner by intelligent storage, microservers, and smart contract. Distributed cloud storage offers a new solution for a database problem that enhances the size of data from IoT applications by the convergence of Blockchain and AI in IoT. For this process, the prediction concept in AI has a crucial role in the prediction of distributed data in advance and suggests utilizing the data in the future. Distributed cloud storage concept used in the service layer, which is used for providing specific services such as a database, decision making to the IoT applications. In a distributed cloud blockchain IoT networks, the smart contract used in every block executes the transaction in peer to peer configurations without the use of a centralized hub, so adding an extra resilience and defense against cyber-attacks. This process also provides a secure, faster, reliable mode of communication for each other.

Decentralization and Distribution: IoT devices are connecting via public networks, which may be hacked by any third malicious user because IoT systems use centralized server methodology. Usage of blockchain technology resolves the security problem in IoT environments and creates linear files which are indexed continuously and are decentralized by consensus protocols such as proof of work, proof of stack and proof of authority. The convergence of blockchain and AI for IoT use many consensus protocols such as proof of work, proof of stake, delegated proof of stake and distribution, decentralization mechanism for scalability and security, the dispersion of power uses decentralization process. IoT applications have a fundamental role in improving the collection of data from various devices to train the AI system. In this process, security, privacy, and energy consumption are significant challenges, with the convergence of blockchain and AI solve these problems.

Authentication and Verification: Authentication and verification are any methods such as when a bank verifies a part of the secure transaction from one person to another person; it is the concept used traditionally in IoT applications such as medical, smart vehicles and other. The IoT application uses a centralized manner in this process, and it is dependent on the bank. Blockchain technology provides the way for automatic transaction from one person to another with cryptographically signed and verified by all miners. It uses cryptocurrency such as bitcoin, ethereum for authentication. AI is used for intelligent and decision-making capabilities for a specific transaction. The convergence of Blockchain and AI for IoT provides the architecture known as decentralized AI. It is used for an automatic transaction with a secure, authentic manner, and is verified by miners [40]. Authentication and verification are used in the communication layer. With the use of blockchain technology in IoT, devises and gateway may protect the information, which is stored, processed at the node. All information is cryptographically verified in the distributed hyper ledger that is transferred by all participants node, can validate the integrity before accepting them.

Chain Structure: Chain structure is a collection of data in the IoT application, and data block, Merkle tree, bitcoin, and ethereum medium are using for storing the IoT data in the network. It is generated by various sensing devices such as mobiles, wi-fi, and pen drives. The physical layer has a chain structure which is related to the database using smart contract, hash functions, global registration, and distributed identity for blockchain system function of IoT chain structure [41]. Merkle tree is used for the distribution of blocks in blockchain technology. Perception layer is used for identifying the data and information such as temperature, location, pollution, weather, motion, agriculture, and some others from sensor devices (RFID, Barcode, and Infrared). This layer has different kinds of security threats. To mitigate these issues, the concept of blockchain and AI is used where information is in the form of block [42].

4. Evaluation of the proposed BlockIoTIntelligence architecture

In this section, we discuss the evaluation of the proposed BlockIoTIntelligence architecture; which is categorized into two parts: qualitative analysis and quantitative analysis. In qualitative analysis, we present how to use AI and Blockchain in IoT application with "AI-driven Blockchain for IoT" and "Blockchain-driven AI for IoT". We also describe how to mitigate the challenges of blockchain in IoT with AI and conversely, how to address issues of AI with blockchain by high-level taxonomy structures. In quantitative analysis, we present a performance evaluation of the BlockIoTIntelligence architecture to compare existing researches on device, fog, edge and cloud intelligence according to standard parameters such as accuracy, latency, security and privacy, computational complexity and energy cost in IoT applications. An architectural analysis of BlockIoTIntelligence discusses various components such as technology, evaluation parameters, proposed methods, software, and algorithm of IoT with existing researches.

4.1. Qualitative analysis

We described how to resolve the issues of blockchain for IoT application with AI and conversely, how to mitigate challenges of AI for IoT applications by blockchain in this subsection. Blockchain and AI are essential technologies for IoT applications. Blockchain has issues such as energy consumption, scalability, security, and privacy, efficiency, and others. To mitigate these issues, many researchers provide the AI technology such as self-organized map [43], cellular automata and deoxyribonucleic acids computing [30], genetic algorithm [44], federated learning [45], spark machine learning [46], multidirectional recurrent neural network [47]. AI offers intelligent and decision-making capabilities for a machine to human in IoT application. Conversely, AI has also some challenges such as artificial trust, explainable AI, data sharing, security, and privacy. Many researchers have used various blockchain technologies such as distributed ledger [31], deep chain [48], G-coin [37], novel cryptocurrency scheme [38], legacy access control and so on for resolving these challenges. In qualitative analysis, we differentiate "AI-driven Blockchain" and "Blockchain driven AI" for IoT applications. Blockchain offers especially to accelerate and simplify the process of how transactions are recorded, means any asset can be transparently transacted using a completely decentralized system and distributed manner. On the other hand, AI can boost blockchain, technology as some of the most compelling prediction and decision-making use cases applications of Blockchain. Therefore, how AI mitigate the issues of Blockchain is known as "AI-driven Blockchain" and how Blockchain mitigate the issues of AI is known as "Blockchain-driven AI". We are describing the difference between AI-driven Blockchain" and "Blockchain driven AI" for IoT application with high-level taxonomy in the subsequent sub-sections:

4.1.1. AI-driven blockchain for IoT

Here, we discuss the utilization of AI for Blockchain in IoT applications. Nowadays, the utilization of IoT in many applications such as smart city, healthcare, transportation, agriculture, and so on is increasing rapidly worldwide. Blockchain technology is being used for security and privacy. However, there are many limitations, such as network size, complexity, high transaction cost, and so on. To mitigate these limitations, integration of AI and Blockchain play a significant role in recent years, and these limitations are classified into seven categories, which are shown in Fig. 5. The first category is energy consumption, where the power is consumed by crypto-currency miners in blockchain networks. The second category refers to scalability that describes the capability of nodes of blockchain networks to grow and manage increasing demand–supply for productivity. The third category includes security and privacy that supports secure and cryptographically signed transfer of a transaction from one node to another in the blockchain. The fourth category contains efficiency, where a comparison between the input value and the output value is carried in terms of electricity, timing in IoT applications. The fifth category refers to the hardware that delivers the information to utilize the devices for IoT application used by AI and blockchain technologies. The sixth category discusses lack of talent where finds the knowledge related talent and use the automatic machine from the concept of machine learning. The last type covers data gates where all data will be available on a blockchain network, and enterprises will be directly sold or purchase them from us.

Energy Consumption

Blockchain techniques such as bitcoin, litecoin, and others have constraints that at least 51% of miners on the blockchain network should be verified for the particular transaction [49]. These

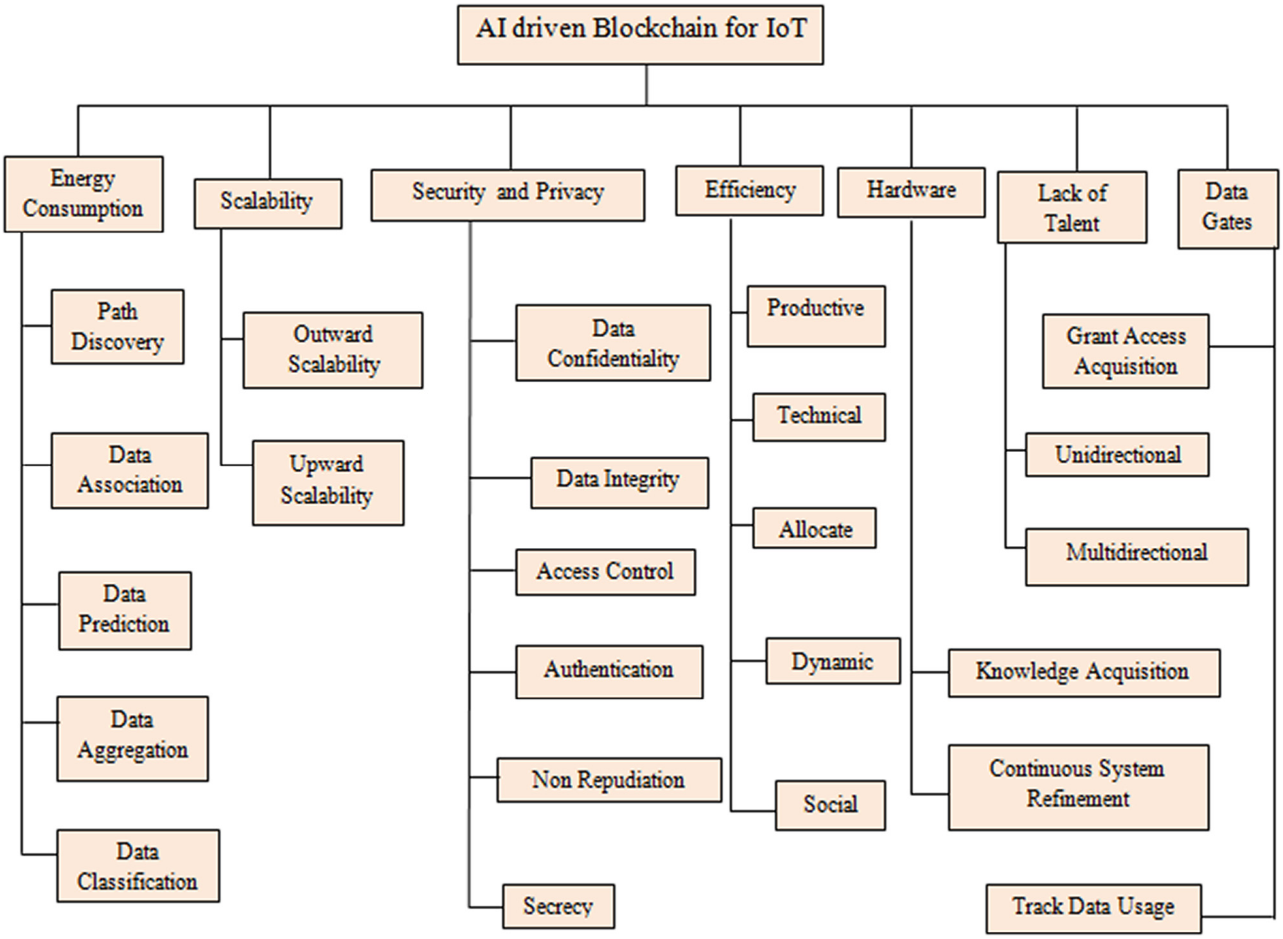


Fig. 5. Hierarchical Taxonomy of AI-driven Blockchain for IoT.

miners need mining the blocks by solving a complex mathematical problem to complete the transaction in the blockchain network. The successful miner transfers the solution on blockchain networks. Therefore, energy is consumed in this operation because of at least 51% of miners used in the blockchain network. Wu et al.'s research [50], energy consumption mining is a complex task that requires millions of energies to complete the job. However, blockchain technology is not sufficient for energy consumption. To address this problem, many researchers use AI technology for blockchain in IoT. It is already proven to be very efficient in optimization energy consumption by path discovery, data association, data prediction, data aggregation, and data classification.

Path Discovery: IoT is a continuously growing technology in which billions of smart devices connected anywhere and anytime [51]. The centralized hub is introduced that stored all essential information regarding IoT devices and maintain the transactions by finding efficient path discovery for IoT devices. However, it is very confused due to the centralized hub might be damaged then all processing might be stopped, so the system is not robust. Jesus et al. [52] provided the blockchain concept where the merkle tree is using to discover the energy-efficient path to resolve this problem. It is like a complete binary tree, and the inner node value is a one-way function of its children, and it must produce $2 * \log_2 M$ hashes, where M is the number of the transaction for discovering an efficient path in blockchain. However, energy-efficient path discovery problem is not entirely resolved by blockchain technology. Enami et al. [43] provided the concept of SOM-Self Organized Map neural network in which neurons organized in the regular low dimensional grid; each neuron is showing by an n-dimensional weight vector. Every input vector activates a neuron in the output layer based on its similarity and resolves energy-efficient path discovery problem.

Data Association: Data association is the partition of the sensors data into sets of many observations produced for the specific target in IoT application. Therefore, it is a limitation of IoT because IoT is a collection of billions of data in the network. To mitigate this problem, use blockchain technology (hyper-ledger) in which every block connects to the previous block and has four parts determine transaction, last and current block hash value, and timestamp [53]. However, blockchain technology has also some limitation for data association such as privacy, security, and collection of massive data. Yang et al. [45] provided the federated learning algorithm where data are partitioning in vertically for resolving this problem. This algorithm uses cooperative statistical analysis, association rule mining, secure linear regression for data association, and provides a solution for the collection of a vast amount of data.

Data Prediction: IoT provides the platform for transferring the interrelated data in the network. It has an ability of data prediction, but this is not proper for all situations in the system. Sagirlar et al. [54] described that the blockchain also has the limitation for data prediction in some IoT applications such as weather forecasting, fog prediction. To mitigate this limitation, Akbar et al. [55] provided the concept of complex event processing where offer a decentralized and distributed solution for complex a large set of data breaches; it designed for real-time applications such as weather forecasting, fog prediction in IoT applications.

Data Aggregation: Data Aggregation is the process in which collection and aggregation of data according to low power consumption, traffic congestion, and increase accuracy in IoT applications [56]. The sensor devices are used in IoT application for data aggregation, but it is not satisfactory for all requirements. Integration of blockchain and IoT are utilized for data aggregation by the power of work in which collection and aggregation of the individual data in IoT. It provides security in a network by the power of work consensus protocol, but it is not adequate for securely data aggregation in all IoT applications. To mitigate this problem, Kumar et al. [57] provided the concept of AI neural network and fuzzy logic which is based on data aggregation where improves the network lifetime and throughput and calculating the fitness function in the system of IoT applications.

Data Classification: Data classification is a collection of billions of devices connected and sharing the information breach to one device to another device, but IoT devices could not manage a significant breach. Therefore, blockchain technology is used to mitigate this barrier by hyper ledger, but it is not also satisfactory for data collection. To minimize this problem, Gu et al. [58] provided the artificial neural network where data classify for IoT. It has subcategories such as perceptions, backpropagation, probabilistic neural networks, which are used to analyze the classification algorithms for data classification in IoT applications.

Scalability

Scalability is another limitation of IoT application, which has two parts: outward scalability and upward scalability. The blockchain is developing technology at a continuously of 1 MB every 10 min, and it already adds up to 85 GB. It also used for IoT applications such as healthcare, weather forecasting, transportation, and others. Salah et al. [15] provided the first blockchain possible solution for scalability in 2008, but Sagirlar et al. [54] also offered the decentralized learning systems which are based on federated learning to mitigate scalability constraints. Using federated learning enables model training on a large corpus of decentralized data and built a scalable production system in the domain of IoT devices; it is based on the tensor flow.

Outward Scalability: IoT is a combination of devices network that is connected via the internet. It also can transfer and modify the data by many sensors such as RFID, Infrared, and so on. Outward scalability is an expansion of the network as its central location by small open offices which is connecting to the central hub. We are facing a scalability challenge where connecting devices has a massive collection of data with expanding IoT technology. Integration of blockchain and IoT solve this challenge by using open chain in the network for the transaction of data from one person to another person. However, using blockchain technology did not completely reduce the challenge of scalability. To mitigate this problem, Hussein et al. [44] provided a genetic algorithm technique in which optimizes the queuing optimization of the massive amount of data in scalability.

Upward Scalability: Upward scalability means the capability to increase the number of devices and traffic in the networks. IoT applications are using the upward scalability because they are growing devices or users in IoT applications such a medical, transportation, and so on, but upward scalability is a stiff challenge in IoT. The blockchain technology is used for solving this problem that all devices are connecting in a distributed and decentralized manner. However, blockchain technology did not completely resolve the scalability problem. To mitigate this limitation, Hussein et al. [44] provided the axis scaling approach and discrete wavelength transform for improving scalability in IoT applications where anybody interacts with the IoT devices efficiently. Human interaction to the IoT devices provides the automated process for saving time and act more efficiently.

Security and privacy

IoT has the ability to adding internet connectivity to a system of interrelated devices to each other in the network. Every device has a unique address and knowledge to send the data on the web automatically. However, the connection between devices of the internet is open, so it is not secured and challenge for IoT applications. Zyskind et al. [59] provided the blockchain technology; it is a disruptive technology that plays fora primary role in managing, controlling, and securing IoT devices by using bitcoin, and smart contract. Blockchain technology has also some security issue in the network of IoT applications. To address the security issue, use AI where solves the security limitation, and it has subcategorized in data confidentiality, data integrity, access control, authentication, non-repudiation.

Data Confidentiality: IoT applications are growing in various fields such as healthcare, transportation, weather forecasting, and so on. In healthcare, provide the medical facility to billions of disabling patients by body sensors, physiological information, and this information is transferring to the medical staff for medical treatment. However, the patient has data confidentiality limitation in medical therapy in IoT applications. Torre et al. [60] provided decentralized and distributed storage where information stored in the open ledger for solving data confidentiality problem. However, blockchain technology has also some limitation, such as using excessive energy of data confidentiality for security. To mitigate this limitation provided the concept of smart contract testing, ethereum simulator, where formal verification and searching of information is used for data verification insecurity.

Data Integrity: It is the property for best communication that the information must be reliable and accurate over the IoT networks is known as data integrity. RSA, AES, and TDES algorithms are using for security purpose for this communication [61]. However, IoT has the limitation of data integrity in the IoT application. Therefore, Outchakoucht et al. [62] provided the concept of CORDA DLT blockchain methodology in which keep a shared ledger of transactions to resolve this limitation. Devices are continually checking each record line by line after interacting with each other and solve data integrity limitation. However, blockchain technology did not resolve data integrity issue completely. To mitigate this problem, Aru et al. [63] provided the concept of cellular automata and DNA computing methodology where more robust ciphers generated in the network. A cellular automaton is a collection of colored cells on a grid of specified shape that evolves through several discrete time steps according to a set of rules based on the states of neighboring cells.

Access Control: Access control is a security technique in which find, that is the person using the resources such as data, services, computational systems, storage space, and so on in IoT networks and when [64]. However, IoT is a vast network for IoT applications, so access control is a limitation of IoT application. The blockchain technology is used for solving this limitation, where bitcoin transferred from one person to another person easily. However, this technology has also some restrictions for access control. To mitigate this problem, provided state-of-the-art access control mechanism in AI and presents design criteria (dynamism, language, emergency) in a creative environment which evolutionary computation artificial neural network are using for hash function [65].

Authentication: Authentication is a process where any system has individual access based on their identity, such as a private key, symmetric key in a security system. IoT applications are used many authentication methods for security such as X.509 certificates, TPM (Trusted Platform Module), symmetric key, but it is not enough for adequate protection always time. The blockchain technology used for reducing this limitation in which the hash value of the previous block and hash value of current block stored in the immediate neighborhood block, and every block is connected to the last block and forward block also. However, it is also not suitable for authentication in all IoT applications, so it also has a limitation. To mitigate this limitation, Phiri et al. [66] provided adaptive neural–fuzzy inference system and artificial neural network to implement a multi-factor authentication system. The identity attributes are mined by social networks, a set of questionnaires, and application forms from the various services in IoT.

Non-Repudiation: Any device of the IoT cannot deny the performed transaction from one person to another is known as Non-Repudiation because it is already a combination of authentication and integrity. IoT applications are using various non-repudiation methods for security such as digital certificates, hardware-based anchor of trust. However, these methods are not sufficient for adequate protection in all IoT applications. Therefore, the blockchain technology used for mitigating this limitation where the digital signature is presenting the authenticity of digital information. Valid digital signature gives authentication that the sender cannot deny having sent the information. However, it is also not sufficient for non-repudiation insecurity. To mitigate this limitation, Phiri et al. [66] provided the concept of sandboxing is used for non-repudiation in security, where it prevents malware or harmful applications from the negative affecting system and isolates apps from the critical system and other programs.

Secrecy: It is a way of hiding the data from specific one or group of devices in IoT is known as secrecy. However, it is such a difficult task in IoT application because all peripheral devices are connecting via the internet. The blockchain concept is used for secrecy in which blocks have linked to the previous blocks which have hash value (complex mathematical puzzle). However, it has also some limitation for confidentiality because one of the keys is used in blockchain once, data stored which may not be altered (at least, not easily) and this is the property of data secrecy. To mitigate this problem, Black mirror scenario such as smarter phishing scam, malware epidemic, robot as in AI technology where all devices are connecting in the network, but it has a private key. Example: An administrator spends some time on facebook during every workday for building's robot security system.

Efficiency

IoT is the network of devices connected to the internet and among them has a massive amount of data. Increasingly large volumes of data are transfer from very high speed and independently within the network. However, IoT applications use optimized resources for improving efficiency, but it is not sufficient. Therefore, blockchain technology is using to resolve this problem by eliminating the third party and related overheads cost, therefore transaction costs are virtually non-existence. However, this technology is also not entirely sufficient for improving efficiency in IoT applications. To mitigate this situation, AI technology used by various AI techniques such DL for improving efficiency limitation, and it subcategorized in productive, technical, allocate, dynamic, social.

Productive: Any application might be more efficient, cost-effective, and productive on an enormous scale in IoT. For example, various IoT applications such as healthcare industry, IoT devices may be used to accurate update information related to the condition of patients, while in transportation IoT devices may be used to update related to passenger's information and train information. However, productivity is a limitation in the efficiency of IoT. Using distributed ledger, resolve this productivity problem where transactions are stored in a distributed manner, and encryption is utilizing in each transaction update and verification. However, blockchain is not enough for improving productivity; therefore AI technology used for solving this situation where intelligent monitoring, intelligent storage, proactive failures, automated fixes are used for IoT applications. Intelligent monitoring uses a human-to-machine learning interface that combines existing human employee knowledge with real-time data; intelligent storage solutions make more smart decisions on storage optimization.

Technical and Allocate: Many numbers of sensors are used in IoT applications which are continuously increasing day by day. Resource allocation and technically facilities on IoT application are the central limitations of efficiency in IoT. Distribution ledger of blockchain technology is using for reducing this limitation where information stored in the form of token. Byzantine fault tolerance is used consensus protocol in blockchain technology for technically resource allocation. However, blockchain technology is not sufficient for improving resource allocation. Therefore, to mitigate this limitation, Mata et al. [67] provided the concept of the genetic algorithm where proposed novel network architecture for interconnecting a set of IP and MPLS fields and performing routing and flow aggregation, through a flex-grid optical core.

Dynamic and Social: A massive amount of data are generating in IoT due to the fast growth of IoT and Social Network. Collection of information and data from social media and sensor devices have spread thoroughly and dynamically an extensive database of IoT applications. IoT has the limitation of the generated large volume of data from social media. To mitigate this problem, blockchain technology is using where data are stored in a decentralized and distributed manner. Blockchain technology has an open chain and hyper ledger for transferring the transaction securely and efficiently, but it also has some limitation regarding dynamic and social data gathering efficiency. To address this problem, Hoey et al. [68] provided the AI technology (Machine Learning) used in which provide helps to indexed address the scaling, as massive computing power controlled to multiple operations of a collection of interaction data.

Hardware

IoT hardware is another limitation of blockchain for IoT, which subcategorized in two parts: knowledge acquisition, continuous system refinement. Equipment is an essential part of IoT application solution because IoT devices need to transfer, and processes information to the specific centralized database; it is like a cloud. Hardware devices are increasing day by day in IoT application according to the demands of humans, which is not handled by IoT. Therefore, blockchain concepts are used where computational based blockchain systems are used as a consensus protocol. These protocols encourage members in IoT to upgrade their hardware like CPU and ASIC for the solution of this limitation. However, some protocols depend on special hardware features such as trusted environment, SGX-enabled CPU, hyper-ledger, Microsoft coco-framework, and sawtooth lake. This technology is also not completely sufficient. Roth et al. [69] provided the concept of neural network computing used for developing the area of neuron-computer hardware, learning algorithm, and collecting computing for mitigating hardware problem.

Knowledge Acquisition: Knowledge acquisition is a set of rules and regulations in which extracting and organizing the knowledge from many expert's areas and is utilized for various IoT applications. A reconfigurable knowledge acquisition architecture used for integrates the IoT-communication infrastructure into data analysis. However, it is not entirely sufficient for data analysis in the IoT application. Vukobratovic et al. [25] provided a smart contract is used where consensus protocol for organizing, retrieving and transfer the transaction in the blockchain network to mitigate this problem. However, it has also some restrictions, such as self-learning capability. Therefore, AI technology is used in which machine learning analyzes and computing algorithm for organizing, transferring and managing the knowledge for communication infrastructure. Machine learning makes a self-contained review of ML techniques and IoT applications in intelligent transportation systems (ITS) and obtains a clear view of the trends in the fields as mentioned earlier and spot possible coverage needs.

Continuous System Refinement: The continuous system is mapping from one step to another, and refinement is linking to present work to the past activity in IoT applications, both are using in IoT. It is a very crucial part for IoT because all IoT devices linked to each other via the Internet. However, it is not adequate in IoT applications. Therefore, blockchain concepts are used for this limitation where every block is connecting to the previous block; and provide the security and privacy by completing one action to another action. The blockchain concept is not entirely adequate for this limitation. Neural network computing in AI techniques is used where the collection of neurons and linked to each other by refinement action. Neural network computing characterized by containing adaptive weights along paths between neurons that tuned by a learning algorithm that learns from observed data to improve IoT applications.

Lack of Talent

Lack of talent is also a limitation of AI-driven Blockchain in IoT. It categorized into two parts: unidirectional and multidirectional. Connected devices are generating much more vulnerability with cybernetic attacks with details, and lack of talent is in demand for IoT applications. IoT application is plugging to security gaps, and using trainers give the training to the existing employee according to the IoT applications. However, it is not sufficient in IoT, so blockchain concepts are used for improving the talent which provides the knowledge about currencies in the market such as bitcoin, ethereum, open-chain, multichain, hyper-ledger for developing the skill. IoT applications have various advantages by using this skill. However, it is not also wholly sufficient, thus mitigate this problem, AI technology used where provide the knowledge about virtual agents which is used for interacting with the machine to machine and provide new ledger for communicating transactions.

Unidirectional: In IoT, data can flow in the only unidirectional manner (only upstream from sensor device). IoT applications are secured, but it has some limitations regarding lack of talent. To address this problem, the blockchain technology is used where the transaction is entering in networks and all minors verify the operation in the blockchain network. However, it does not provide ultimately reduce lack of talent limitation. Wu et al. [47] used AI technology used for removing this issue by essentially provided decentralization knowledge and broadcast to all utilize agent in networks.

Multidirectional: A centralized database is mainly used for multidirectional communication in IoT in which every IoT devices is connected to the centralized database in IoT applications. It is also a limitation of IoT because rapidly growing of data continuously; it is vast which may not be handled by centralized form. Therefore, blockchain technology is used in which data or transactions are stored in a decentralized and distributed way for solving this problem. However, blockchain technology is not entirely sufficient for addressing this limitation. To mitigate this problem, Wu et al. [47] provided M-RNN multidirectional recurrent neural network is used in which data streams operate in sequentially because the timing of inputs into the hidden layers is both lagged and advanced.

Data Gates

IoT is a collection of various devices connected by the internet; these devices have a lot of information. If any device wants to share data to another device, then it firstly sends to a centralized controller, after that the controller checks all details of the information then moves to the acquired device. This process is very lengthy, and it is a limitation of IoT. To address this limitation, the blockchain technology is used in which any device that sends information to another device directly in meshed form; no centralized method is used. All data is available on a blockchain and companies can instantly buy them from us, only need for grant access, track data usage, and generally make sense of what happens to our personal information at a computer. It is known as intelligence machines, which are a part of AI Technology. Data gates are categorized into two parts: grant access acquisition and track data usage.

Grant Access Acquisition: Grant access acquisition is the first category of data gate where every device collects the information and is stored in the database. It is a useful advantage in IoT applications, and it is primary to ensure that devices cannot transfer the data to unauthorized devices in IoT applications. However, IoT is an extensive area, so it is not entirely possible. To mitigate this problem, the concept of litecoin and hyper ledger are used where they communicate the transaction from one person to another securely. However, it is not sufficient for entirely secure communication because it has limitations like data stored on a blockchain is not inherently trustworthy. Therefore, events need to be recorded accurately in the first place. To address this limitation, decentralization Intelligence (Tran AI, Neureal, Neuromation, BurstIQ, and AtMatrix) are used in AI technology. Neural AI is peer to peer AI supercomputing, Neuromation is synthetic datasets generation, BurstIQ is healthcare data marketplace; these all are used for grant access acquisition.

Track Data Usage: Track data usage in IoT means that how to manage internet bandwidth or speed for IoT networks and data usage by all devices in the systems. It is a real challenge in IoT because it is generating enormous data rapidly from many IoT applications such as smart city, smart vehicle, and healthcare. To mitigate this limitation, smart contract technology (Ethereum) is used where data are shared in a secure form by controlling the network space. However, it is not also enough to ultimately reduce this limitation. Chander et al. [46] used spark ML AI technology (Machine Learning) in which they share information in the form of neurons and use Apache spark tools to work with a large amount of data efficiently.

4.1.2. Blockchain driven AI for IoT

In this subsection, we discuss how blockchain mitigates the issues of AI is known as "Blockchain-driven AI". We present the taxonomy of blockchain-driven AI for IoT with some specific categories explainable AI, AI effectiveness, data sharing, artificial trust, security, and privacy, as shown in Fig. 6. The first category includes explainable AI, which provides the techniques in AI to be trusted and easily understandable by humans and IoT. Therefore, explainable AI has another name, transparent AI, or interpretable AI. The second category covers AI effectiveness, which provides predictive methods for users in IoT applications. The third category includes data sharing in which sharing data resources from one machinery device to another machinery device is done easily

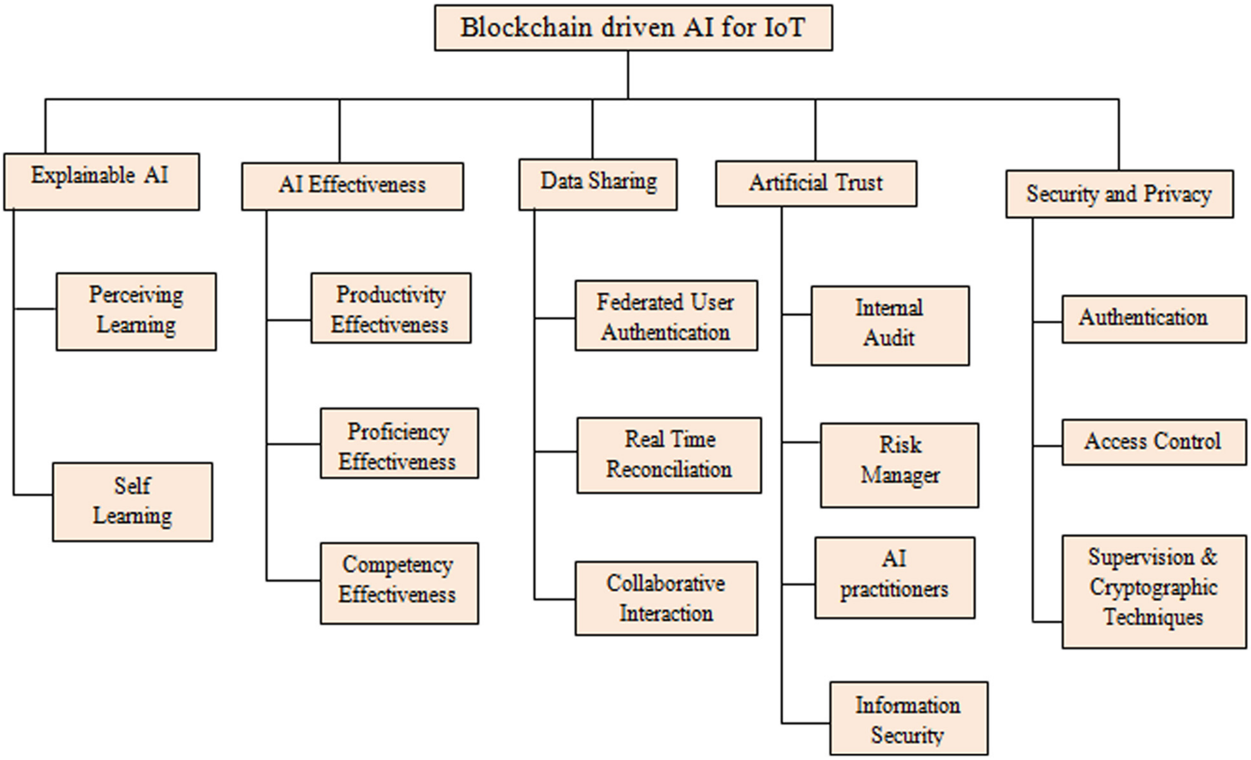


Fig. 6. Hierarchical Taxonomy of Blockchain driven AI for IoT.

and provides many facilities for communication. The fourth category covers artificial trust, which provides methods for solving the problems regarding neuron science in the trustable situation. The last category includes security and privacy in which data is transferred from one device to another device securely and is cryptographically signed. It provides the authorization to the private data or information such as healthcare patient data, transportation passenger's passport, or ARC data.

Explainable AI

Explainable AI is an artificial intelligence program to describe its purpose, rationale, and decision-making process that can be understood by every device or person in device intelligence for IoT applications. Explainable models have various advantages regarding IoT which provide the facilities for IoT applications such as autonomous vehicles, smart healthcare, and enterprises. The functional enhancement of the AI system in the organization for IoT application to shift to augmented intelligence depends on empowering. Study of intelligent agents is a part of AI research where provides the input raw parts, perform action or processing on it, and provide maximum output or chance of success for a specific purpose. With the convergence of Blockchain and AI for IoT, it provides decentralized AI applications and methodology for the secure and confidential platform of decisions data because all information on Blockchain is publicly available. Explainable AI provides transparent AI algorithm for reaching the specific decision. Dinh et al. [48] used distributed ledger in explainable AI where data is transferred and stored cryptographically and validated by all miners. Explainable AI is divided into two categories: perceiving learning and self-learning, which are explained as follows:

Perceiving Learning: Perceiving learning is the complete information about IoT networks with any third party. Due to the continuous improvement of traditional technology, the world internet of computer is a takeover from IoT [70]. To address this situation, Mao et al. [60] presented deep neural networks where they studied pattern recognition and computational theory and built a model from a training set of inputs observations to make data-driven predictions as outputs without explicitly static programs. This technology has some limitations of interpreting a deep neural network model and explaining its predictions of programs, training data, and security [71]. To mitigate this problem, Din et al. [48] presented the concept of Deep Chain because it can automate payment in cryptocurrency and provide access to a shared ledger of data in an explanatory decentralized, secure manner with future prediction and provide complete information about networks with any other party.

Self-Learning: Self-learning means the ability to have complete information about IoT networks itself. IoT applications which are already dependent on self-learning because all works are completed automatically such as an automatic car, robotics, smart city, and intelligent medicine and so on. IoT applications have the main challenge that it is centralized, so decentralizes and distributed decision-making algorithms adopted in substantial IoT application such as robotics, transportation, and others without the need for a central authority. AI technology (deep learning) is used in autonomous systems where self-learning and acts on their part. This technology has some limitation such as it is tough to understand what exactly goes inside the networks, so decision taken by devices in the systems are unexplainable and cannot be verified. Ethereum and smart contract are used to mitigate this problem in which tracked the data in every round for data processing and decision-making chain; it provides insights into tuning black boxes to balance performance and prediction accuracy with the explainability of the network.

AI Effectiveness

AI makes it possible for machines to learn from experience, adjust to new input data, and perform a human-like a task automatically known as AI effectiveness related to proposed intelligence architecture. AI provides simulating intelligent activities in tools for IoT applications. Using machine learning in IoT applications is known as connected intelligence and offers many functions such as predictive analysis, prescriptive analysis, adaptive analysis, and continuous analysis [72]. It is beneficial for both real-time and post-event processing. However, the integration of AI and IoT has limitations like effectiveness in output. To mitigate these limitations, Salah et al. [15] provided a solution based on blockchain technology (hyper ledger and bitcoin) which provides security, scalability, vulnerability and deterministic execution of the transaction by consensus protocols.

Productivity Effectiveness: IoT is an exciting technology for the development of IoT application and improves the productivity for IoT applications such as agriculture, transportation, and other business applications by streamline management. IoT has limitations, such as data analytics, process automation, and security for improving productivity in IoT applications. To mitigate these limitations, deep learning is used for the analysis of data and pattern mining algorithms for the IoT infrastructure and services. However, AI technology has a limitation for enhancing productivity in IoT applications. Therefore, blockchain technology (G-Coin) is used which eliminates a single point failure, increase data transparency, and immutability issues in IoT applications [73].

Proficiency Effectiveness: Integration of AI and IoT are used for various IoT applications by a predictive algorithm and machine intelligence for improvement of operational efficiency and proficiency. AI provides brain and data to IoT according to the needs. It takes smart decisions and utilizes in end devices such as robots and drones. AI cannot replace every task for IoT application because it is a tool that strengthens and boosts the performance and efficiency of an average worker. To mitigate these constraints, Swan et al. [11] presented the concept of Blockchain thinking and Hyper ledger where provides self-mining ecology, proof of intelligence, and fast progress of knowledge in proficiency. Usage of blockchain technology provides maximum power for proficient miner's works in IoT application and multi-application intelligence for different sets of data [74]

Competency Effectiveness*:* IoT provides hassle-free integrated processes which require minimum human interaction with each other and create a seamless flow of information that leads to accurate delivery of information and services to the human in IoT applications. Collaborative filtering provides the facility to IoT, which filters the primary data and uses it in IoT application such as healthcare and agriculture. AI technology is used into the derive a meaningful understanding of nearly unlimited data streamed from IoT devices automatically, but it has significant building trust problem devices in IoT application. To mitigate this problem, Lin et al. [73] presented a novel crypto-currency scheme where IoT transfers digital information in a decentralized, secure, and distributed manner. Digitization is the method of organizational activities, processes, competencies to fully leverage the changes from the convergence of Blockchain and AI for IoT [74].

Data Sharing

Data sharing is the ability in which share the same data resource or information by multiple applications simultaneously in IoT device intelligence of proposed architecture. It has a significant role in continuously increasing of IoT devices, and it has some properties such as storing data, protection of data. The AI-powered network framework is used in data sharing where network task automatically completed by AI technologies. Due to the separation of IoT, data barriers between diverse operators and devices operators are generating bottlenecks in AI. To mitigate these barriers, Zhang et al. [75] provided data sharing framework for the secure environment, and this framework is based on distributed tamper-proof attributes of blockchain. Data sharing framework is a combination of supervision and specific data access control based on the smart contract. Banerjee et al. [16] provided blockchain workflow architecture for enhancing secure data sharing, so all transactions are transparent. Any modifications might be easily traced and detected. Data Sharing is also divided into three parts: Federated user authentication, Real-time reconciliation, and Collaborative interactions.

Federated User Authentication: Federated user authentication is Single-Sign-On (SSO). It accesses services with a single login by users in any organization of IoT applications. It provides economic advantages as well as convenience to organizations and their users in IoT application such as healthcare, transportation, and others. AI provides the facility to users of an organization in IoT applications of resultant cost savings and consolidations of resources. However, it has limitation like federated identity in centralization form of users in the organization. To mitigate this limitation, Dinh et al. [48] implemented DLT architecture to extend the federated identity in not only centralized form but also decentralized form to verify the authenticity. Distributed ledger technology (DLT) is a digital system for recording the transaction of assets in which the transactions and their details are recorded in multiple places at the same time.

Real-Time Reconciliation: Real-time reconciliation is a process where an organization accountant reviews the general ledger of a company and determines the movement of the transaction in IoT applications. It is the flow of data sharing in IoT applications complicated because it has a vital priority for commercial works of IoT applications [75]. AI (i.e., Sigma IQ's matching engine) is used for complete automation in the reconciliation process and removing the need for the accounting team to reconcile transaction in IoT applications. However, AI technology has limitations, such as millions of data are available in IoT applications. To mitigate these limitations, Hyper-ledger and Litecoin are implemented in which data are stored in a decentralized form, and every block is connected to the backward direction to the neighborhood block.

Collaborative Interactions: Collaborative interactions of data sharing are a type of communication which allows devices to work together in the resolution of a problem in IoT applications. Information is sent from one person to another person in IoT applications using collaboration interaction, such as mobile, robotics, cloud, and healthcare. IoT has several challenges such as latency and efficiency of data. To mitigate these challenges, Chander et al. [46] used collaborative robots (COBOTS) for service implementation and integration with IoT network service composition is of importance when new cognitive devices are becoming active participants in IoT applications. COBOTS are the methods of AI technology, but it has limitations such as security, huge data usability, building trust because many devices work together in collaboration. To mitigate these problems, Vermanson et al. [76] presented the concept of distributed ledger and smart contract in which converging, sensing and decentralized and autonomous applications interact in collaboration manner and allow AI-based edge and cloud-based intelligence solutions for low latency communication.

Artificial Trust

Artificial trust is a method for analyzing and ingest a massive amount of data by AI-powered system. Traditionally, inventory management in an IoT relies heavily on the audit of inventory every day and a centralized database tracks the delivery conditions such as traveling data speed to predict lead time better, and the artificial trust built within the IoT system. Autonomous virtual agents and transparent audit managed the task in IoT system with the help of bots to trust each other to increase fake trust. It also eventually increases every machine to machine interaction and transaction. Blockchain techniques provide help to AI's resolutions to be more transparent, trustworthy, explainable, and all data on the blockchain is available publicly. AI techniques are the key to provide users with confidentiality and privacy by using a machine learning system [77]. Artificial trust is divided into four categories: Internal audit, Risk manager, AI practitioners, and Information security.

Internal Audit: Automated patient health information is a confidential report for every patient in IoT applications [78], so an internal audit is used in healthcare application because various health information trust challenges arise. An internal audit is methods for evaluating, understanding risk, and opportunities related to any healthcare organizations objectives [79]. If IoT application healthcare wants to participate in the AI revolution, it needs to grow in fields such as natural language processing, application program interfaces (recognition, image analytics, and text analytics), and robotics. Internal audit is used to help an enterprise to evaluate, understand, and communicate the degrees to which artificial intelligence affects the enterprise's ability to create value in short, medium, and long term. AI has limitation like building trust in healthcare application where the confidential report of the patient can be sent to a third person. To address this problem, Fenwick et al. [79] presented an internal audit in artificial trust with a novel crypto-currency scheme, which includes security and data analytics in a decentralized and distributed manner. It requires recording and examining of all hardware and software activities that deal with EPHI and consists of internal audit rules and regulations.

Risk Manager: Today's scenario, all things are connected to the internet. IoT is used to create, analyze, and communicate data between a device to device with the use of any third party. However, IoT has increased the risk to data security as sensitive data is created and stored on the network; to mitigate the risks, we implement a risk manager in IoT. It is a part of the artificial trust and the need to make big data and AI central to all task. Risk managers are required to ask themselves if there is a risk that no adoption of AI by their business has competitive more advantage in IoT applications. The blockchain is the foundation technology for the future of risk management, and it is used in permissionless blockchain and permissioned blockchain networks. Permissionless blockchains allow any device without any vetting to participate in the network of IoT. Permissionless blockchains start with a pool of cryptocurrency to pay service providers or miners, to participate in the system. Permissioned blockchain has evaluated the participation of an entity on the blockchain framework [80].

AI Practitioners: The integration of AI and IoT is rapidly growing for digital ecosystems based on today's IoT applications. Internal data analysis is based on four types: stream data visualization, the accuracy of time series of data, predictive analysis, and logistic data analysis. Roth et al. [69] present AI practitioners such as deep learning, neural network, and backpropagation for artificial trust in IoT. AI practitioners have the in-depth technical knowledge, which is comfortable for the IoT environment, whereas adopting AI in IoT applications requires a significant level of business understanding. AI techniques have limitations such as security and AI human interface because the stream of data is not secured, and AI human interface is not entirely suitable for networks. Blockchain technology in which open ledger or hyper ledger is used for secure communication of transaction and provided a better human interface to each other in the network for coordination of untrusting devices and secure data transaction in IoT application.

Information Security: Information security is another part of Blockchain driven AI for IoT. AI techniques such as genetic algorithm and deep learning are used for information security, but they have many limitations, such as information security [81]. An AI coded in IoT applications with specific smart contracts able to only perform those actions which are used to reduce catastrophic risk scenario. To address these problems, Kahan et al. [82] provided the blockchain technology in which the hash value of the previous block and current block stored in the current block and every block connect to every last block. Blockchain technology has been increasing interest that is dependent on cryptocurrency (Moreno, Bitcoin Gold, BitCoin NG) for information security in IoT applications.

Security and Privacy

With the advancement of IoT applications such as smart cities, smart home, smart agriculture, and smart everything, IoT has essential techniques for incredible impact, promising, and growth. However, these IoT devices have a limitation that any malicious persons can easily hack them. These IoT devices have limited storage, computing power, network capacity, and so it is vulnerable to attacks such as smart cameras, smartphones, and tablets. To mitigate this limitation, provide AI technology in which AI and ML give specific CAPTCHAs (collection of squiggly letters, characters, and images) and this CAPTCHAs types in the text box and find device-related information. However, it has constraints regarding security and privacy. To address this problem, Khan et al. [82] provided the latest concept of blockchain which resolves many security problems by bitcoin, ethereum and smart contract in IoT applications such as healthcare, smart cities, whether prescription and agriculture. Blockchain technology also used distributed public ledger in peer to peer network for providing the security and privacy to the IoT devices, Security and privacy divided into three parts: authentication, access control, supervision, and cryptographic techniques.

Authentication: Authentication is verifying the identity of any device or person in IoT applications. The authentication process of security and privacy are very significant; it is used in various cases in the IoT application. An example is where a person enters a username and password when he is opening any device such as a computer, smartphone. If they enter the correct login information, it lets the machine identify which person is accessing the device [83]. Authentication is a part of IoT application providing new premium services with enhanced security and intuitive user experience based on data analytics, machine learning. Dorri et al. [84] presented Blockchain-based approaches for a secure tamper-proof distributed ledger which assigns a unique ID for each device and record them into the blockchain so authentication might be easy without the central authority.

Access Control: Access control is an essential mechanism of security because it determines who can use or view IoT device resources in a computing environment. It is a fundamental concept that minimizes risk in many IoT applications such as smart grid, smart farming, smart grid, and so on. AI technology uses RBAC (Role-based access control) for security and provides a creative environment in various IoT applications. RBAC is inadequate for a productive environment regarding interaction and efficiency because it focuses on the role only; it does not integrate another important issue, which is authentication [84]. Blockchain technology is beneficial for this limitation where it is vulnerable to various attacks and in some cases, can easily be broken. Dorri et al. [84] provided the concept of Legacy Access control and is used for a local and private blockchain to provide secure access control to the IoT devices and their data. Blockchain generates an immutable time-ordered history of transactions that is linkable to other tiers for giving specific services.

Supervision and Cryptographic Techniques: With the continuous development of IoT, it provides benefits to users in different

IoT applications such as smart transportation, smart agriculture, and smart vehicle. Without proper protection, the development of IoT applications is not possible; therefore, supervision and cryptographic techniques of security are used in IoT applications. It is a technique which provides secure computation and data privacy. Cryptographic tools are used for balancing transparency and confidentiality in transferring the data from one IoT device to another for security. Rodriguez et al. [85] proposed the concept of adversarial neural cryptography (GAN) emerging technique which enables secure communication between different IoT devices, but it has limitation because it does not offer full security for IoT applications. Qian et al. [16] presented the solution of Blockchain technology where Ethereum, Hyper ledger, Bitcoin are used with built-in Turing complete programming language and allows the functioning of smart contracts and decentralized applications for more security and private communication.

4.2. Quantitative Analysis

In this subsection, we present a performance evaluation of the BlockIoTIntelligence architecture to compare existing researches on device, fog, edge and cloud intelligence according to some parameters such as accuracy, latency, security and privacy, computational complexity and energy cost in IoT applications. To carry out quantitative analysis, we refer to existing researches [3, 4,21,24]. Each research provides a big data analysis at the device, edge, fog, and cloud intelligence. In research [3], BlockDeepNet provided DL systems to mitigate security and privacy at the device intelligence. For edge intelligence, Rathore et al. [24] proposed a distributed deep learning-based blockchain network for a single reduced point of failures and accuracy issues of IoT applications. The decentralized AI blockchain-based security architecture at the edge intelligence discussed in which resolved a security attack in the IoT applications in Rathore et al.'s research [4]. Xu et al. [21] suggested blockchain-based decentralized resource management framework for resolving the resource management issues in cloud intelligence. The proposed architecture of BlockIoTIntelligence is used with various components of IoT: devices intelligence, fog intelligence, edge intelligence, and cloud intelligence. An application of big data analysis is deployed on the BlockIoTIntelligence to analyze the compatibility of collaborative AI and Blockchain in IoT. We described the review of existing research shown in Table 2, according to the proposed architecture of BlockIoTIntelligence.

Device Intelligence: Rathore et al. [3] proposed the system, which is the convergence of blockchain and deep learning, and it is used for providing the security and privacy to the IoT devices in the edge layer. Covergential DL is mainly used to improve security and privacy and obtain plenty of IoT data for IoT applications. On the other hand, Go-ethereum blockchain platform is adopted to ensuring confidentiality and integrity of collaborative DL in IoT applications. Edge cloud, cluster, access point components are utilized in device intelligence. Raspberry Pi computers are used as a front end and edge cloud cluster used as a backend in the research. In this research, evaluate the performance of object detection application with four measurements; accuracy, security analysis, time delay, and computational complexity. Mean precision accuracy of object detection measured using 5 and 10 Raspberry Pis and observed that accuracy is increased in proportion to the number of IoT devices and use 2745 instances. The authors evaluated latency with total time cost measured for eco-operation and noted latency increases continuously with an increasing number of Raspberry Pis. The BlockDeepNet system provided security and privacy analysis where data similarity index calculated by Euclidian distance. It estimated that similarity decreases and privacy decrease with the find the Euclidian distance calculation. Finally, computational complexity evaluated based on measurement of CPU and Memory. With BlockDeepNet, additional CPU and memory resources are utilized to using blockchain and deep learning operations.

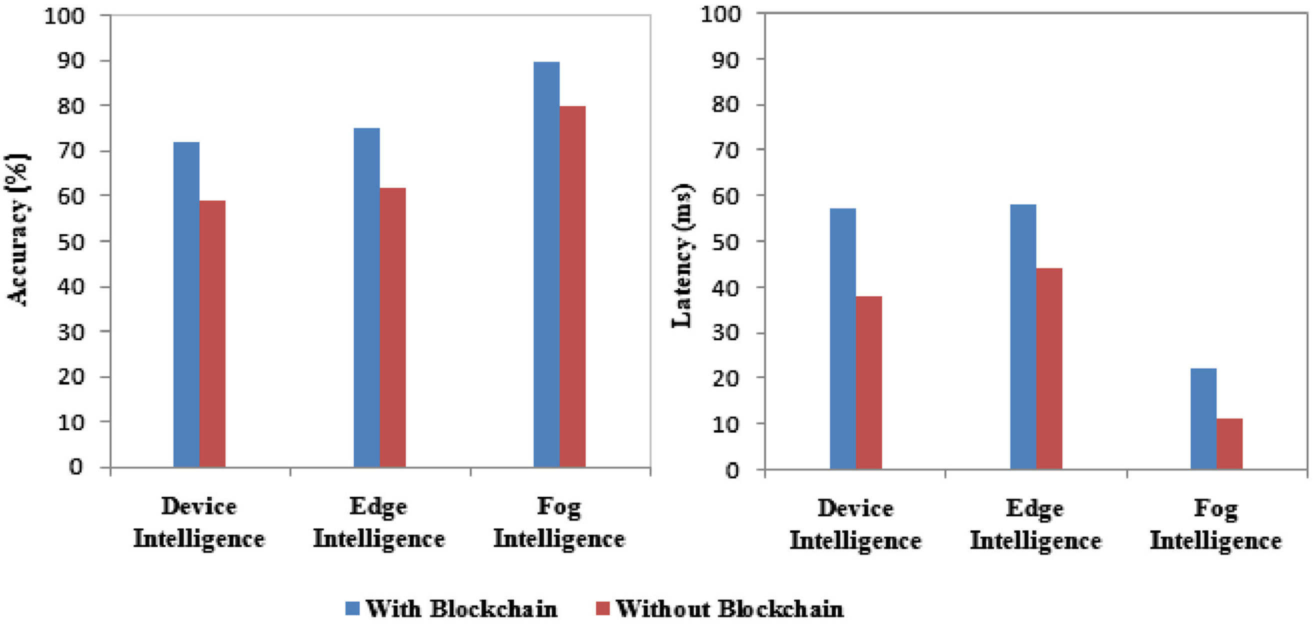
Edge Intelligence: Rathore et al. [24] provided a secure deep learning approach for the IoT networks adopted where the DL operation are describing in edge intelligence with blockchain technology. Go-ethereum blockchain provides the DL operations on edge intelligence and removes the centralization problem in IoT network. Tensor Flow 1.7.0, numpy version 1.14.0, python 3.6.4 are used for deep learning operation in edge intelligence. Solidity language is adopted for learning and mining contract of blockchain technology. The experimental feasibility of object detection in various Raspberry Pi evaluated in terms of four metrics: latency delay, accuracy, privacy, and security analysis for DeepBlockNet approach. Accuracy measurement of object detection application is evaluated and noted that increases the accuracy if the number of edge nodes is increased in the edge intelligence and 5518 instances are used for DL operation. The participation of more edge nodes to increase the training dataset and also increased the accuracy of the object detection compare than without DeepBlockIoTNet approach. The authors evaluated a variation object detection time against the total number of edge nodes in the edge intelligence to elaborated the latency improvement and shorter detection time realized with DeepBlockIoTNet approach compare than without approach. Security and privacy evaluated by similarity index with calculated the Euclidian distance of objects in the IoT network in the smart cities, the similarity index value is decreased. Therefore, security and privacy of objects in IoT networks are increased due to the decrease of similarity indexed value.

Fog Intelligence: Rathore et al. [4] proposed a decentralized security architecture based on Blockchain, AI, and SDN for IoT networks in the smart cities in fog intelligence. SDN is mainly adopted for analyzing the incoming data of IoT networks and provided an excellent attack detection model. Ethereum blockchain is used to delivering the decentralized attack detection of big data analysis to mitigate the centralization issue. Fog and mobile computing are supported for attack detection at the fog node and mitigate storage, computation, and latency constraints. Mining provides the simulation environment to simulate the IoT devices, and POX is adopted for the machine learning algorithm such as classification for analyzing huge data for attack detection. The architecture's performance evaluated in six parameters: accuracy, detection rate, computational resources, predictive value, Mathew correction coefficient, and area under the curve. According to a flooding attack, the authors observed lower time to addressed attack using decentralized architecture. Blockchain distributed architecture provides an efficient way to address attacks in smart networks such as smart transportation. The computational complexity is evaluated by memory and CPU utilization in IoT networks of the architecture with blockchain operations. It notices the average usage of computational power things such as CPU and memory by the fog node in fog intelligence. The centralized and distributed architecture shows the output in blockchain decentralized inaccuracy, latency parameters.

Cloud Intelligence: Xu et al. [21] proposed a Blockchain-based decentralized resource management framework to handle the resource management issues in cloud intelligence where green energy with uncertain capacity is utilized in IoT networks. In this framework, reduce the energy cost by the request scheduler and also proposed reinforcement learning methods in a smart contract to minimize the computational cost. This method has one property that it has already historical knowledge regarding IoT devices. Experimental evaluation on google cluster traces and real-world electricity price described that significantly reduce the

Table 2
Architecture analysis of Existing research.

Intelligence	Parameters						
	Technology	Evaluation Parameters	Application	Proposed method	Blockchain platform	Additional software	Process/Algorithm
Device Intelligence [3]	Blockchain, Deep Learning	Accuracy, Privacy and Security, Computational Complexity	Object Detection	Blockchain-based Secure Deep Learning	Go-ethereum	Raspbian, Solidity	Collaborative DL, Candidate block generation
Edge Intelligence [24]	Blockchain, Deep Learning	Accuracy, Latency delay, Security and Privacy measurement	Object Detection	Secure Deep Learning with Blockchain	Go-ethereum	Raspbian, Solidity	Distributive DL, DeepblockIoTNet
Fog Intelligence [4]	Blockchain, SDN, Machine Learning	Accuracy, Computational resources	Attack Detection	Blockchain-based decentralized Security	Ethereum	Linux, Pox as a controller, Mininet	Traffic flow analyzer, Traffic flow classifier, Blockchain-based attack detection and mitigation, and Model fusion
Cloud Intelligence [21]	Blockchain, Reinforcement Learning	Energy Consumption, Resource Management	Weather forecasting	Blockchain-based resource management	Ethereum, Smart Contract	Windows, Solidity	Dynamic voltage frequency scaling (DVFS)



(a) Accuracy analysis

(b) Latency analysis

Fig. 7. Comparative analysis of proposed BlockIoTIntelligence.

cloud datacenter's cost compared than other algorithms. Server and data center level and dynamic voltage frequency scaling (DVFS) algorithm are used to reducing the energy cost for resource management. With the real-world data traces on renewal power, grid price, and workload evaluate the framework. The learning rate of the framework algorithm considered on 0.8 and researcher normalized the cost to the result of Round-Robin algorithm where data centers have taken the available requests and save 50 percent more energy cost than Round-robin algorithm and 20 percent than MiniBrown algorithm.

Quantitative analysis is described in Table 3, wherein we refer the quantitative results from existing researches [3,4,21,24] to measure the feasibility of proposed BlockIoTIntelligence architecture in terms of standard parameters such as accuracy, latency, security and privacy, computational complexity, and energy cost. Accuracy is showing 72% at device intelligence, 75% at edge intelligence, 90% at fog intelligence, and 68% at cloud intelligence according to existing researches. Latency is divided into two parts: minimum and maximum, 56.2 ms minimum and 57.4 ms maximum at device intelligence, 56.0 ms minimum and 58.0 ms maximum at edge intelligence, 0.0 ms minimum and 11.0 ms maximum at fog intelligence according to existing researches. Security and privacy are measured by finding the value of the similarity index with maximum and minimum. In device intelligence, similarity index is varying from 1.0 to 0.01, 0.62 to 0.4 at edge intelligence, 09 to 0.1 at fog intelligence. Computational complexity percentage measured by CPU utilization and memory utilization in Table 3 with existing research. CPU utilization for IoT devices are changing from 3.1% to 4.3%, and edge server 33.0% at device intelligence, 3.4% to 4.5%, and edge server 36.0% at edge

Table 3
Quantitative analysis.

Intelligence	Parameters							
	Accuracy (%)	Latency (ms)		Security and privacy (SI)		Computational complexity (%)		Energy cost (%)
		Min.	Max.	Max.	Min.	CPU utilization	Memory utilization	
Device Intelligence [3]	72	56.2	57.4	1.0	0.01	IoT Devices: 3.1–4.3 Edge Server: 33.0	IoT Devices: 11.0–14.7 Edge Server: 24.0	–
Edge Intelligence [24,51]	75	56.0	58.0	0.62	0.4	IoT Devices: 3.4–4.5 Edge Server: 36.0	IoT Devices: 11.5–14.4 Edge Server: 25.0	–
Fog Intelligence [4]	90	0.0	11.0	0.9	0.1	90	91	–
Cloud Intelligence [21,48]	68	–	–	–	–	–	–	50% compare than Round Robin Algorithm 20% compare than MiniBrown Algorithm

intelligence, and 90% at fog intelligence. Memory utilization for IoT devices are changing from 11.0% to 14.7%, and edge server 24.0% at device intelligence, 11.5% to 14.4%, and edge server 25.0% at edge intelligence, and 91% at fog intelligence from the study of existing research. According to Xu et al.'s [48] research, energy cost 50% reduced compare than round-robin algorithm and 20% MiniBrown algorithm.

Comparative analysis of device, edge and fog intelligence in the proposed BlockIoTIntelligence is shown in Fig. 7. It has two parts: (a) Accuracy analysis, and (b) Latency analysis. With the use of blockchain technology, accuracy is varying from 0 to 72% in device intelligence, 0 to 75% in edge intelligence, and 0 to 90% in fog intelligence. Without using blockchain technology, accuracy is changing from 0 to 59% in device intelligence, 0 to 62% in edge intelligence, and 0 to 80% in fog intelligence. Therefore, researchers use different applications, but the accuracy percentage is always high with the use of blockchain for IoT applications. Latency value is converting 0 to 57.4 ms in device intelligence, 0 to 58.0 ms in edge intelligence and 0 to 22 ms in fog intelligence with blockchain technology and 0 to 38.0 ms in device intelligence, 0 to 44.0 ms in edge intelligence and 0 to 11 ms in fog intelligence without blockchain technology. Therefore, the researcher used various types of applications such as object detection, attack detection for big data analysis at device, edge and fog intelligence, but latency is high with the use of blockchain.

Finally, we conclude the quantitative analysis of proposed BlockIoTIntelligence architecture in Fig. 8. In this analysis, we are using four parameters such as accuracy, latency, security and privacy, and centralization related to device intelligence, edge intelligence, fog intelligence, and cloud intelligence. Accuracy fluctuates from cloud intelligence to device intelligence (High to low), it shows that we get accurate value in device intelligence compare than others. Security and privacy are measured by similarity index value, which also varies cloud intelligence to device intelligence (High to low). It shows that IoT data is maximum secured and private at device intelligence compare than others. Latency value and centralization problem reduced from device to cloud intelligence. Latency value is minimum in device intelligence. Therefore, accuracy, latency, centralization, and security and privacy issues mitigated by our proposed BlockIoTIntelligence architecture.

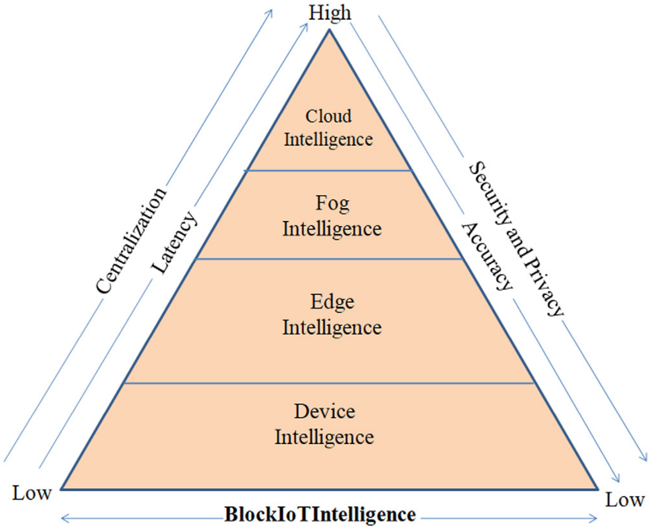


Fig. 8. Architectural Analysis of the BlockIoTIntelligence.

5. Research challenges and possible solutions

We also discuss the most important challenges for the proposed BlockIoTIntelligence architecture of Blockchain and AI for IoT applications. It is well defined in Table 4 that most of the challenges in BlockIoTIntelligence architecture for blockchain and AI in IoT applications mitigated with clear define known solutions. However, most of the solutions, such as BitCoin NG, Bitcoin, Novel crypto-currency Scheme, Self-Evolving network, SON, and CNN, cannot be completely adopted by blockchain and AI. The main reason for this is that the processing security for these solutions is quite high compared to other traditional solutions, such as Mixing techniques, decentralization, and distributedDB. Security, privacy, and scalability are the main issue in blockchain and AI for IoT applications. AI analyzes the massive amount of data in IoT applications, but there is a chance of data being corrupt or hacked by the third party. Blockchain is unable to analyze such data, but as it provides the decentralized and distributed database, it can protect every data related to AI which results into enhancing security and transparent operation by given solutions in Table 4. User alertness in IoT applications can be skilled inactivity by regularly finding recent news about various Blockchain and AI challenges updates in IoT such as new techniques, software, user importance, and mechanism and prevention tools. We also summarize the overall architectural analysis of the proposed BlockIoTIntelligence in terms of centralization, latency, and security in Fig. 8.

Table 4
Research challenges & possible solutions.

Possible solution	Challenges									
	Scalability enhancement	Security and privacy	Storage capacity	Processing power	Energy efficiency	Accuracy and speed	Throughput and latency	Resource management	Data flow	Function integration
Bitcoin NG, Bitcoin, Bitcoin Gold, Monero	√	√	√		√		√			
Micro block, Mixing techniques	√	√				√		√	√	
Novel crypto-currency Scheme	√					√	√			
Mix Coin, Coin-join, Coinshuffle, Zero-coin, Zero-cash		√								√
Aigorand					√	√				√
IOTA, Gridcoin	√	√		√		√		√		
Intel SGX, TEEs										
Solidity and Chaincode								√		
Etherem Code	√	√	√		√				√	
GHOST, Off-chain solution			√			√		√		
Bigchain DB and IPFS, HyperNET		√	√		√					√
Hawk compiler, Multichain, Rockchain		√			√					
Hyperledger Fabric	√	√			√					
Open ledger		√		√					√	
Edge computing, Cloud computing			√					√		
Self Evolving Network, SON, SFOT		√			√					√
Plasma, Web3Stack, Cross-chain	√						√			
CNN(AlexNet)						√				
MiniBlockchain, GPU, FPGA				√	√		√			
SHA-256 Hashing, Eris, steller, Ripple		√								√
CoNISK, Google's Certificate		√				√		√		
HardFork, Single Miner, Mini BC“-”-“-”-”-				√	√					
ECDSA, Decentralization, DistributedDB		√	√	√		√			√	

As a future direction for convergence of blockchain and AI for IoT challenges, a variety of prevention mechanisms, architecture can be used to monitor and analyze the information transferred by IoT devices in IoT applications. These mechanisms are mainly used for removing challenges and issues generated in Blockchain and AI. Moreover, various security, privacy and scalability solutions [22,23] are proposed for secure communication in large area of IoT application such as, address space solution [19] that have been used for maximum huge data in IoT, traffic monitoring solution that have been used to remove information collision, and mining and energy efficiency solution that have been used for gaining maximum efficiency. According to Zheng et al. [8] and Sallah et al. [15] research, Blockchain and AI in IoT is capable to deliver many real-time IoT applications such as smart city, healthcare, smart transportation, intelligent precision farming, smart vehicle, banking and finance, Intelligent ocean bed exploration, and future energy industry leveraging capabilities. However, these applications have some issues or challenges such as privacy leakage, selfish mining smart contracts vulnerabilities, deterministic execution, Lack of standards, scalability, trusted oracles, which can be mitigated by using existing solutions for Blockchain and AI for IoT [84], [86].

6. Conclusion

In this paper, we proposed a BlockIoTIntelligence architecture of converging blockchain and AI to achieve the goal of scalable and secure IoT with cloud intelligence, fog intelligence, edge intelligence, and device intelligence. We presented possible general motivations behind the convergence of AI and Blockchain to provide scalable and secure IoT applications such as smart healthcare, smart city. We analyzed evaluation pf proposed architecture into two ways: qualitative and quantitative. In qualitative analysis, we differentiated “Blockchain driven AI”, and “AI-driven Blockchain” with high-level taxonomy. We presented an experimental quantitative evaluation of BlockIoTIntelligence architecture with secure, decentralized big data analysis tasks in IoT applications and provided efficiency in terms of accuracy, centralization, security, and privacy, and latency. Our finding suggests that BlockIoTIntelligence is mitigating the existing challenges and obtain high accuracy with acceptable latency and security with decentralized way. We identified research challenges such as scalability enhancement, interoperability, resource management, lack of standard, anonymity, the integrity of data flows, heterogeneity, costs and capability constraints, energy efficiency, and traffic monitoring in using BlockIoTIntelligence architecture of converging blockchain and AI for IoT and provide some possible solutions. However, the convergence of AI and blockchain for IoT resolves all issues such as accuracy, latency and security and privacy, but computational power and latency issues are not completely mitigated with the proposed architecture. BlockIoTIntelligence architecture can be enhanced with machine intelligence concepts such as feature extraction and scaling and classification in a decentralized way to address these issues.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (NRF-2019R1A2B5B01070416).

References

[1] Proof point, Proof point uncovers internet of things (IoT) cyber attack. Proof point release, 2014. https://www.proofpoint.com/us/proofpoint-uncovers-internet-things-iot-cyberattack/. (Accessed 31 October 2017).

[2] C.M. Chung, C.C. Chen, W.P. Shih, T.E. Lin, R.J. Yeh, I. Wang, Automated machine learning for Internet of Things, in: IEEE International Conference on Consumer Electronics-Taiwan, ICCE-TW, 2017, pp. 295-296. https://doi.org/10.1109/ICCE-China.2017.7991112.

[3] S. Rathore, Y. Pan, J.H. Park, BlockDeepNet: A blockchain-based secure deep learning for IoT network, Sustainability 11 (2019) 3974, http://dx.doi.org/10.3390/11143974.

[4] S. Rathore, B.W. Kwon, J.H. Park, BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network, J. Netw. Comput. Appl. (2019) http://dx.doi.org/10.1016/j.jnca.2019.06.019.

[5] H.F. Atlam, R.J. Walters, G.B. Wills, Intelligence of things: opportunities & challenges, in: 3rd Cloudification of the Internet of Things (CIoT), 2018, pp. 1–6, http://dx.doi.org/10.1109/CIOT.2018.8627114.

[6] S.W. Lee, O. Prenzel, Z. Bien, Applying human learning principles to user-centered IoT systems, Computer 46 (2) (2012) 46–52, http://dx.doi.org/10.1109/MC.2012.426.

[7] Y.S. Jeong, J.H. Park, IoT, and smart city technology: Challenges, opportunities, and solutions, J. Inf. Process. Syst. 15 (2) (2019).

[8] Z. Zheng, S. Xie, H.N. Dai, X. Chen, H. Wang, Blockchain challenges and opportunities: a survey, Int. J. Web Grid Serv. 14 (4) (2018) 352–375.

[9] R. Kefa, Convergence of AI, IoT, big data and blockchain: A review, Lake Inst. J. 1 (1) (2018) 1–18.

[10] K.L. Wright, M. Espinoza, U. Chadha, B. Krishnamachari, SmartEdge: A smart contract for edge computing, in: IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2018, pp. 1685-1690. https://doi.org/10.1109/Cybermatics_2018.2018.00281.

[11] M. Swan, Blockchain thinking: The brain as a DAC (decentralized autonomous organization), in: Texas Bitcoin Conference, 205, pp. 27–29.

[12] N. A. Team, NEBULA AI (NBAI)—Decentralized Ai Blockchain Whitepaper, 2018.

[13] D. Gil, A. Ferrández, H. Mora-Mora, J. Peral, Internet of things: A review of surveys based on context-aware intelligent services, Sensors 16 (7) (2016) 1069, https://www.mdpi.com/1424-8220/16/7/1069.

[14] Liam Tung, AI will create $13 trillion in value by 2030. https://www.zdnet.com/article/mckinsey-ai-will-create-13-trillion-in-value-by-2013. (Accessed 15 June 2019).

[15] K. Salah, M.H.U. Rehman, N. Nizamuddin, A. Al-Fuqaha, Blockchain for AI: review and open research challenges, IEEE Access 7 (2017) 10127–10149, http://dx.doi.org/10.1109/ACCESS.2018.2890507.

[16] Y. Qian, Y. Jiang, J. Chen, Y. Zhang, J. Song, M. Zhou, M. Pustišek, Towards decentralized IoT security enhancement: A blockchain approach, Comput. Electr. Eng. 72 (2018) 266–273, https://www.sciencedirect.com/science/article/pii/S0045790618300508.

[17] N. Kshetri, Can blockchain strengthen the internet of things? IT professional 19 (4) (2017) 68–72, http://dx.doi.org/10.1109/MITP.2017.3051335.

[18] A. Reyna, C. Martín, J. Chen, E. Soler, M. Díaz, On blockchain and its integration with IoT. Challenges and opportunities, Future Gener. Comput. Syst. 88 (2018) 173–190, http://dx.doi.org/10.1016/j.future.2018.05.046.

[19] M. Banerjee, J. Lee, K.K.R. Choo, A blockchain future for the internet of things security: A position paper, Digit. Commun. Netw. 4 (3) (2018) 149–160.

[20] X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen, A survey on the security of blockchain systems, Future Gener. Comput. Syst. http://dx.doi.org/10.1016/j.future.2017.08.020.

[21] C. Xu, K. Wang, M. Guo, Intelligent resource management in blockchain-based cloud datacenters, IEEE Cloud Comput. 4 (6) (2017) 50–59, http://dx.doi.org/10.1109/MCC.2018.1081060.

[22] J. Lin, Z. Shen, A. Zhang, Y. Chai, Blockchain, and IoT based food traceability for smart agriculture, in: Proceedings of the 3rd International Conference on Crowd Science and Engineering, ACM, 2018, p. 3, http://dx.doi.org/10.1145/3265689.3265692.

[23] Y. Lu, Blockchain: A survey on functions, applications, and open issues, J. Ind. Integr. Manag. 3 (04) (2018) 1850015, http://dx.doi.org/10.1142/S242486221850015X.

[24] S. Rathore, J.H. Park, DeepBlockIoTNet: A secure deep learning approach with blockchain for the iot network, Trans. Ind. Inform. (2019).

[25] D. Vukobratovic, D. Jakovetic, V. Skachek, D. Bajovic, D. Sejdinovic, G.K. Kurt, I. Fischer, CONDENSE: A reconfigurable knowledge acquisition architecture for future 5g IoT, IEEE Access 4 (2016) 3360–3378.

[26] H. Sundmaeker, P. Guillemin, P. Friess, S. Woelfflé, Vision and challenges for realizing the internet of things. A cluster of European research projects on the internet of things, Eur. Comm. 3 (3) (2010) 34–36.

[27] J.H. Hartman, I. Murdock, T. Spalink, The Swarm scalable storage system, in: Proceedings. 19th IEEE International Conference on Distributed Computing Systems (Cat. No. 99CB37003), 1999, pp. 74-81, https://doi.org/10.1109/ICDCS.1999.776508.

[28] Y. Yuan, F.Y. Wang, Towards blockchain-based intelligent transportation systems, in: 2016 IEEE 19th International Conference on Intelligent Transportation Systems, ITSC, IEEE, 2016, pp. 2663–2668, http://dx.doi.org/10.1109/ITSC.2016.7795984.

[29] L. Atzori, A. Jera, G. Morabito, The internet of things: A survey, Comput. Netw. 54 (15) (2010) 2787–2805, http://dx.doi.org/10.1016/j.comnet.2010.05.010.

[30] E.M. Dogo, A.F. Salami, C.O. Aigbavboa, T. Nkonyana, Taking cloud computing to the extreme edge: A review of mist computing for smart cities and industry 4.0 in Africa, in: Edge Comput., Springer, Cham, 2019, pp. 107–132.

[31] P.K. Sharma, M.Y. Chen, J.H. Park, A software-defined fog node based distributed blockchain cloud architecture for IoT, IEEE Access 6 (2017) 115–124, http://dx.doi.org/10.1109/ACCESS.2017.2757955.

[32] S. Rathore, P.K. Sharma, J.H. Park, XSSClassifier: An efficient XSS attack detection approach based on machine learning classifier on SNSs, J. Inf. Process. Syst. 13 (4) (2017).

[33] H. Gupta, A. Vahid Dastjerdi, S.K. Ghosh, R. Bhavya, iFogSim: A toolkit for modeling and simulation of resource management techniques in the internet of things, edge, and fog computing environments, Softw. - Pract. Exp. 47 (9) (2017) 1275–1296, http://dx.doi.org/10.1002/spe.2509.

[34] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, W. Zhao, A survey on the internet of things: Architecture, enabling technologies, security, and privacy, and applications, IEEE Internet Things J. 4 (5) (2017) 1125–1142, http://dx.doi.org/10.1109/JIOT.2017.2683200.

[35] R. Shanbhag, R. Shankarmani, Architecture for the Internet of Things to minimize human intervention, in: 2015 International Conference on Advances in Computing, Communications and Informatics, ICACCI, 2015, pp. 2348–2353, https://doi.org/10.1109/ICACCI.2015.7275969.

[36] R. Khan, S.U. Khan, R. Zaheer, S. Khan, Future internet: the internet of things architecture, possible applications, and key challenges, in: 10th International Conference on Frontiers of Information Technology, 2012, pp. 257–260. https://doi.org/10.1109/FIT.2012.53.

[37] Ahmed Banafa, IoT, AI and blockchain: Catalysts for digital transformation, IEEE Internet Things Mag. 1 (1) (2018) http://dx.doi.org/10.1109/IOTM.2018.1700011.

[38] T. Yang, F. Zhai, J. Liu, M. Wang, H. Pen, Self-organized cyber-physical power system blockchain architecture and protocol, Int. J. Distrib. Sens. Netw. 14 (10) (2018) 1550147718803311, http://dx.doi.org/10.1177/1550147718803311.

[39] J. Sunthonlap, P. Nguyen, Z. Ye, Intelligent device discovery on the internet of things-enabling the robot society, 2017, arXiv preprint arXiv:1712.08296.

[40] P.K. Sharma, S. Rathore, J.H. Park, Multilevel learning-based modeling for link prediction and users' consumption preference in online social networks, Future Gener. Comput. Syst. (2017) http://dx.doi.org/10.1016/j.future.2017.08.031.

[41] S.K. Singh, M.M. Salim, M. Cho, J. Cha, Y. Pan, J.H. Park, Smart contract-based pool hopping attack prevention for blockchain networks, Symmetry 11 (2019) 941, http://dx.doi.org/10.3390/sym11070941.

[42] TuchindaRattapoom, Access control mechanism for intelligent environments, Bitstream J. (2002).

[43] N. Enami, R.A. Moghadam, K. Dadashtabar, M. Hoseini, Neural network-based energy efficiency in wireless sensor networks: A survey, Int. J. Comput. Sci. Eng. Surv. 1 (1) (2010) 39–53.

[44] A.F. Hussein, N.A. Kumar, G. R.Gonzalez, E. Abdulhay, J.M.R. Tavares, V.H.C. Albuquerque, A medical records managing and securing blockchain-based system supported by a genetic algorithm and discrete wavelet transform, Cogn. Syst. Res. 52 (2018) 1–11.

[45] Q. Yang, Y. Liu, T. Chen, Y. Tong, Federated machine learning: Concept and applications, ACM Trans. Intell. Syst. Technol. (TIST) 10 (2) (2019) 12, http://dx.doi.org/10.1145/3298981.

[46] A. Chander, R. Srinivasan, S. Chelian, J. Wang, K. Uchino, Working with beliefs: AI transparency in the enterprise, in: IUI Workshops, 2018.

[47] Q. Wu, Z. Zeng, J. Lin, Y. Chen, AI-empowered context-aware smart system for medication adherence, International Journal of Crowd Science 1 (2) (2017) 102–109, http://dx.doi.org/10.1108/IJCS-07-2017-0006.

[48] T.N. Dinh, M.T. Thai, Ai, and blockchain: A disruptive integration, Computer 51 (9) (2018) 48–53, http://dx.doi.org/10.1109/MC.2018.3620971.

[49] P.K. Sharma, S. Rathore, Y.S. Jeong, J.H. Park, SoftEdgeNet: SDN based energy-efficient distributed network architecture for edge computing, IEEE Commun. Mag. 56 (12) (2018) 104–111, http://dx.doi.org/10.1109/MCOM.2018.1700822.

[50] L. Wu, K. Meng, S. Xu, S. Li, M. Ding, Y. Suo, Democratic centralism: A hybrid blockchain architecture and its applications in energy internet, in: IEEE International Conference on Energy Internet, ICEI, 2017, pp. 176–181, https://doi.org/10.1109/ICEI.2017.38.

[51] E.F. Jesus, V.R. Chicarino, C.V. de Albuquerque, A.D.A. Rocha, A survey of how to use blockchain to secure internet of things and the stalker attack, Secur. Commun. Netw. (2018) http://dx.doi.org/10.1155/2018/9675050.

[52] L. Wu, K. Meng, S. Xu, S. Li, M. Ding, Y. Suo, Democratic centralism: A hybrid blockchain architecture and its applications in energy internet, in: IEEE International Conference on Energy Internet, ICEI, 2017, pp. 176–181. https://doi.org/10.1109/ICEI.2017.38.

[53] A. Pieroni, N. Scarpato, L. Di Nunzio, F. Fallucchi, M. Rasho, Smarter city: smart energy grid based on blockchain technology, Int. J. Adv. Sci. Eng. Inf. Technol. 8 (1) (2018) 298–306.

[54] G. Sagirlar, B. Carminati, E. Ferrari, J.D. Sheehan, E. Ragnoli, Hybrid-IoT: Hybrid blockchain architecture for the internet of things-pow sub-blockchains, 2018, arXiv preprint arXiv:1804.03903.

[55] A. Akbar, A. Khan, F. Careez, K. Moessner, Predictive analytics for complex IoT data streams, IEEE Internet Things J. 4 (5) (2017) 1571–1582, http://dx.doi.org/10.1109/JIOT.2017.2712672.

[56] H. Rahman, N. Ahmad, I. Hussain, Comparison of data aggregation techniques in the internet of things (IoT), in: International Conference on Wireless Communications, Signal Processing, and Networking, WiSPNET, IEEE, 2016, pp. 1296–1300, http://dx.doi.org/10.1109/WiSPNET.2016.7566346.

[57] H. Kumar, P.K. Singh, Comparison and analysis on artificial intelligence based data aggregation techniques in wireless sensor networks, Procedia Comput. Sci. 132 (2018) 498–506, http://dx.doi.org/10.1016/j.procs.2018.05.002.

[58] X.F. Gu, L. Liu, J.P. Li, J. Lin, Data classification based on artificial neural networks, in: International Conference on Apperceiving Computing and Intelligence Analysis, 2008.

[59] G. Zyskind, O. Nathan, Decentralizing privacy: Using blockchain to protect personal data, in: 2015 IEEE Security and Privacy Workshops, IEEE, 2015, pp. 180–184.

[60] I. Torre, F. Koceva, O.R. Sanchez, G. Adorni, A framework for personal data protection in the IoT, in: 2016 11th International Conference for Internet Technology and Secured Transactions, ICITST, IEEE, 2016, pp. 384–391, http://dx.doi.org/10.1109/JIOT.2018.2878658.

[61] G. Matsemela, S. Rimer, K. Ouahada, R. Ndjiongue, Z. Mngomezulu, Internet of things data integrity, in: IST-Africa Week Conference, IST-Africa, IEEE, 2017, pp. 1–9, http://dx.doi.org/10.23919/ISTAFRICA.2017.8102332.

[62] A. Outchakoucht, E.S. Hamza, J.P. Leroy, Dynamic access control policy based on blockchain and machine learning for the internet of things, Int. J. Adv. Comput. Sci. Appl. 8 (7) (2017) 417–424.

[63] Iyke Aru, Blockchain integration will improve corporate efficiency and transparency, 2018, https://www.ccn.com/how-blockchain-integration-will-improve-corporate-efficiency-and-transparency/, (Accessed June 2019).

[64] S. Rathore, A.K. Sangaiah, J.H. Park, A novel framework for internet of knowledge protection in social networking services, J. Comput. Sci. 26 (2018) 55–65, http://dx.doi.org/10.1016/j.jocs.2017.12.010.

[65] H.W. Kim, Y.S. Jeong, Secure authentication-management human-centric scheme for trusting personal resource information on mobile cloud computing with blockchain, Hum.-Cent. Comput. Inf. Sci. 8 (1) (2018) 11.

[66] J. Phiri, T. Zhao, J.C.H. Zhu, J. Mbale, Using artificial intelligence techniques to implement a multifactor authentication system, Int. J. Comput. Intell. Syst. 4 (4) (2011) 420–430.

[67] J. Mata, I. De Miguel, R.J. Duran, N. Merayo, S.K. Singh, A. Jukan, M. Chamania, Artificial intelligence (AI) methods in optical networks: A comprehensive survey, Opt. Switch. Netw. 28 (2018) 43–57, http://dx.doi.org/10.1016/j.osn.2017.12.006.

[68] J. Hoey, T. Schröder, J. Morgan, K.B. Rogers, D. Rishi, M. Nagappan, Artificial intelligence and social simulation: Studying group dynamics on a massive scale, Small-Group Res. 49 (6) (2018) 647–683, http://dx.doi.org/10.1177/1046496418802362.

[69] M.W. Roth, Survey on neural network technology for automatic target recognition, IEEE Trans. Neural Netw. 1 (1) (1990) 28–43.

[70] S. Rathore, J.H. Park, Semi-supervised learning based distributed attack detection framework for IoT, Appl. Soft Comput. 72 (2018) 79–89, http://dx.doi.org/10.1016/j.asoc.2018.05.049.

[71] W. Samek, T. Wiegand, K.R. Müller, Explainable artificial intelligence: Understanding, visualizing and interpreting deep learning models, 2017, arXiv preprint arXiv:1708.08296.

[72] Bruncard Phil, The future of IoT is AI, article, 2018, https://www.techuk.org/insights/opinions/item/13827-the-future-of-iot-is-ai.

[73] Y.P. Lin, J. Petway, J. Anthony, H. Mukhtar, S.W. Liao, C.F. Chou, Y.F. Ho, Blockchain: the evolutionary next step for ICT E-agriculture, Environments 4 (3) (2017) 50, http://dx.doi.org/10.3390/environments4030050.

[74] R. Li, T. Song, B. Mei, H. Li, X. Cheng, L. Sun, Blockchain for large-scale internet of things data storage and protection, IEEE Trans. Serv. Comput. (2018) http://dx.doi.org/10.1109/TSC.2018.2853167.

[75] G. Zhang, T. Li, Y. Li, P. Hui, D. Jin, Blockchain-based data sharing system for Ai-powered network operations, J. Commun. Inf. Netw. 3 (3) (2018) 1–8.

[76] O. Vermesan, A. Bröring, E. Tragos, M. Serrano, D. Bacciu, S. Chessa, P. Simoens, Internet of robotic things: converging sensing/actuating, hypoconnectivity, artificial intelligence and IoT platforms, 2017.

[77] M. Kubendiran, S. Singh, A.K. Sangaiah, Enhanced security framework for e-health systems using blockchain, J. Inf. Process. Syst. 15 (2) (2019).

[78] M. Fenwick, E.P. Vermeulen, Technology and Corporate Governance: Blockchain, Crypto, and Artificial Intelligence. Lex Research Topics in Corporate Law & Economics Working Paper, (2018-7).

[79] N. Kaaniche, M. Laurent, A blockchain-based data usage auditing architecture with enhanced privacy and availability, in: 2017 IEEE 16th International Symposium on Network Computing and Applications, NCA, IEEE, 2017, pp. 1–5, http://dx.doi.org/10.1109/NCA.2017.8171384.

[80] S. Rathore, J.H. Ryu, P.K. Sharma, J.H. Park, DeepCachNet: A proactive caching framework based on deep learning in cellular networks, IEEE Netw. (2019) http://dx.doi.org/10.1109/MNET.2019.1800058.

[81] M.A. Khan, K. Salah, IoT security: Review, blockchain solutions, and open challenges, Future Gener. Comput. Syst. 82 (2018) 395–411.

[82] Q. Feng, D. He, S. Zeadally, M.K. Khan, N. Kumar, A survey on privacy protection in the blockchain system, J. Netw. Comput. Appl. (2018) http://dx.doi.org/10.1016/j.jnca.2018.10.020.

[83] A. Dorri, S.S. Kanhere, R. Jurdak, P. Gauravaram, Blockchain for IoT security and privacy: The case study of a smart home, in: IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom workshops, 2017, pp. 618–623, https://doi.org/10.1109/PERCOMW.2017.7917634.

[84] Jesus Rodriguez, These three security trends are key to decentralize artificial intelligence, 2018, https://hackernoon.com/these-three-security-trends-are-key-to-decentralize-artificial-intelligence-f22d9cf38d69/.

[85] T.M. Fernández-Caramés, P. Fraga-Lamas, A review on the use of blockchain for the internet of things, IEEE Access 6 (2008) 32979–33001, http://dx.doi.org/10.1109/ACCESS.2018.2842685.

Sushil Kumar Singh received his M.Tech. degree in Computer Science and Engineering from Uttarakhand Technical University, Dehradun, India in 2018. He also received M.E. degree in Information Technology from Karnataka State University, Mysore, India in 2011. Currently, he is pursuing his Ph.D. degree under the supervision of Prof. Jong Hyuk Park at the UCS Lab, Seoul National University of Science and Technology, Seoul, South Korea. He has more than 9-year experience of teaching in the field if computer science. His current research interests include Blockchain, Artificial Intelligence, Big Data, and Internet of Things. He is a Reviewer of the IEEE SYSTEMS JOURNAL, FGCS.

Shailendra Rathore is a Ph.D. student in the Department of Computer Science at Seoul National University of Science and Technology (SeoulTech.), Seoul, South Korea. Currently, he is working in Ubiquitous Computing Security (UCS) Lab under the supervision of Prof. Jong Hyuk Park. His broadly research interest includes Information and Cyber Security, SNS, AI, IoT. Previous to joining Ph.D. at SeoulTech, he received his M.E. in Information Security from Thapar University, Patiala, India.

Dr. James J. (Jong Hyuk) Park received Ph.D. degrees in Graduate School of Information Security from Korea University, Korea and Graduate School of Human Sciences from Waseda University, Japan. From December, 2002 to July, 2007, Dr. Park had been a research scientist of R&D Institute, Hanwha S&C Co., Ltd., Korea. From September, 2007 to August, 2009, He had been a professor at the Department of Computer Science and Engineering, Kyungnam University, Korea. He is now a professor at the Department of Computer Science and Engineering and Department of Interdisciplinary Bio IT

Materials, Seoul National University of Science and Technology (SeoulTech), Korea. Dr. Park has published about 200 research papers in international journals and conferences. He has been serving as chair, program committee, or organizing committee chair for many international conferences and workshops. He is a steering chair of international conferences — MUE, FutureTech, CSA, CUTE, UCAWSN, World IT Congress-Jeju. He is editor-in-chief of Human-centric Computing and Information Sciences (HCIS) by Springer, The Journal of Information Processing Systems (JIPS) by KIPS, and Journal of Convergence (JoC) by KIPS CSWRG. He is Associate Editor/Editor of 14 international journals including JoS, JNCA, SCN, CJ, and so on. In addition, he has been serving as a Guest Editor for international journals by some publishers: Springer, Elsevier, John Wiley, Oxford Univ. press, Emerald, Inderscience, MDPI. He got the best paper awards from ISA-08 and ITCS-11 conferences and the outstanding leadership awards from IEEE HPCC-09, ICA3PP-10, IEE ISPA-11, PDCAT-11, IEEE AINA-15. Furthermore, he got the outstanding research awards from the SeoulTech, 2014. His research interests include IoT, Human-centric Ubiquitous Computing, Information Security, Digital Forensics, Vehicular Cloud Computing, Multimedia Computing, etc. He is a member of the IEEE, IEEE Computer Society, KIPS, and KMMS.