SUMMARY Blockchain is one of the prominent rapidly used technology in the last decade in various applications. In recent years, many researchers explored the capabilities of blockchain in smart IoT to address various security challenges. Integration of IoT and blockchain solves the security problems but scalability still remains a huge challenge. To address this, various AI techniques can be applied in the blockchain IoT framework, thus providing an efficient information system. In this survey, various works pertaining to the domains which integrate AI, IoT and Blockchain has been explored. Also, this article discusses potential industrial use cases on fusion of blockchain, AI and IoT applications and its challenges.

key words: blockchain, artificial intelligence, internet of things, industrial use cases

1. Introduction

The AI domain branches out into Expert Systems (ES), Natural Language Processing (NLP), Fuzzy Logic, Robotics and Neural Networks (NN). Also, the classification of AI tasks consists of formal, mundane and expert. The formal task is mostly applied for mathematics, games and theorem proving. The mundane task is applied for image processing, speech recognition, NLP, reasoning and Robotics. The expert task is applied in engineering domains, fault detection and analysis, medical diagnostics and creativity [1]. The ride apps like Uber uses heavy Machine language programming for its efficient working [2]. The best example is how Uber computes the surge pricing. The earliest usage of AI was in the airline sector where the concept of autopilot was deployed. Most of the boeing flights are driven by robots [3]. The future of AI would make human life simpler by automating most of our daily tasks. One such example is the emergence of self-driven cars which has gained a huge market and is under research currently. The top automobile companies such as Daimler AG, BMW etc. have already started investing huge on this project [4], [5]. The smart traffic lights which is one of the component of smart city project aims to reduce the waiting time to 40% [6]. The research of AI usage has stepped even into education wherein the assignments submitted by the students go through an automated plagiarism check and also immersive learning [7] is gaining much popularity especially during this pandemic phase of COVID-19.

On the other hand, blockchain is a distributed or a decentralized ledger technology that maintains secure and immutable records of data and transactions done by the users of the block [8], [9]. Since blockchain provides a transparent environment, there is no necessity of intermediate nodes to validate the transactions. The data recorded in these shared ledgers are distributed securely on multiple nodes which are located across the world. The main feature which differentiates blockchain with database system is the aggregation of distribution, decentralization, and a consensus mechanism. A block in a blockchain consists of the following elements: index - which gives the position of the block in the chain; Timestamp - gives the information about when that block was created; Previous Hash - this is used to link all the blocks in the chain; Data - which consists of the record of transactions; Nonce - a number used to determine a valid hash [10]. The bitcoin network was the first implementation of blockchain technology. Microsoft Azure-hosted blockchain is an example of blockchain technology which can be deployed as public, private or permissioned network [11]. Blockchain works on hashing technique and each block has a unique hash code that identifies the block and its contents [12]. All the blocks are connected to each other with the hash of the previous block. Blockchain also uses cryptographic hashes such as SHA256 or SHA512 to secure the data record stored in the block [13]. The cryptographic hashes serves as a digital fingerprint and also as a checksum in securing data stored in the blocks [14]. Elliptic Curve Digital Signature Algorithm is deployed in the blockchain which uses a strong public-private key-pair generation technique for uniquely validating the data stored in the blockchain [15]. Blockchain uses various types of consensus algorithms which decide on how blocks are updated or managed. Blockchain uses Interplanetary File System (IPFS) protocol which is used to retrieve the file stored. IPFS is a peer-peer protocol where every node stores a group of hashed files. To retrieve a file, a hash of the file is called and the IPFS analyses the validity of the hash and delivers the file to the client [16], [17]. AI and Blockchain can work together to provide advantages in healthcare and industry sectors too. When we integrate IoT network along with AI and Blockchain, more features can be explored.
In general, Internet of things aims to connect all the objects and these objects range from electronic products, electrical appliances, humans, animals, mechanical devices and are often termed as “things”. Each object or thing is assigned a unique identifier through which it is recognised in the internet. The major purpose of connecting these things is to create an autonomous environment and enabling the things to be controlled remotely [18]. The IoT infrastructure includes smart devices which uses embedded system consisting of sensors, processors, and network devices. It aggregates the data that are sent to the cloud for processing and storage through a gateway. The IoT aids in creating a comfortable lifestyle of the people and makes the environment smarter for better decision process [19]. The challenges of security in IoT is addressed by coordinating blockchain’s interplanetary file system. The authors in [20] considered systematic review of smart contracts over IoT in specific and presented meta-analysis to show how the smart contract improves security in IoT.

The authors [21] addressed how blockchain transform AI by providing a framework to resolve various challenges. IoT helps in performing the following tasks:

- Ubiquitous access of information.
- Efficient transmission between the connected devices or things.
- Improvised data packets being transferred over the network, thus reducing the overall cost.
- Most of the daily business process are automated which boost the quality of services and reduces the human intervention.

1.1 Summary of Review Papers

The major objective of blockchain is to maintain accurate records securely and process the data or transactions stored in the block. AI is mostly used in decision making process, identifying patterns and seamless communication. Integrating AI in blockchain will help in improving the data accuracy and would aid in decision making especially during the post transaction processing. Any AI application requires timely accurate and authentic information for effective decision making. A blockchain based AI framework can provide this due to the immutability feature in blockchain. The blockchain employs a mining node to compute the best solution and this is added to the block in the distributed ledger. Similarly, AI system also chooses the best possible solution for a given problem during the decision-making process. A blockchain based AI framework will distribute the entire task to several nodes across the globe thus increasing the compute speed and eliminating the single point of failure issue of a centralized deployment. An efficiency of an AI system majorly depends on the amount of data available from varied sources. But most of the data is stored privately due to legal issues. AI systems could greatly change the manner how blockchain networks are managed and can significantly improvise the processing time of the transactions. Let us consider an example of a bitcoin transfer to a node on the same network. The delay incurred in confirming the transaction is huge due to the decentralized nature of the blockchain and the transactions have to be mined and validated by the miners to store them in the block. Since the block sizes are limited, the transactions which goes beyond the capacity of the block would be queued for a longer time. By implementing an AI system, the processing resources could be reduced for confirming these transactions. The hashing algorithms can be trained by the AI system by giving the right amount of data needed. This would significantly reduce the cost and the resources for the blockchain network [22].

1.2 Contribution of This Work

AI and IoT are integrated in smart devices through chatbot which can take voice based instructions from user, for e.g. Alexa [23]. The Blockchain would enable the smart devices to create secure contracts with vendors, without the interference from any financial bodies. IOTA is a distributed ledger which is used to store and process transactions between systems and the IoT devices. The AI algorithms are implemented to reduce the processing time of these transactions. These algorithms may be running in form of mobile agents which would reduce the processing resources in the blockchain [24]. The blockchain technology supports IoT by securing the sensor devices by encrypting the data and then this data is transmitted via public network. So, fusion of Blockchain, IoT, and Artificial Intelligence can be in multiple dimensions like business models, services, and products to get benefited while applying to autonomous agents. Let’s consider an example of autonomous vehicle. The complete deployment runs using the combination of AI, IoT and blockchain. The decision making is done by AI engine taking into account the inputs from different sensors embedded in the vehicle. The data records are stored securely in the blockchain which is accessed by a consensus mechanism by the stakeholders.

1.3 Organization of the Work

The organization of the work as follows.

- Section 1 deals with introduction of AI, IoT and Blockchain.
- Section 2 discuss about fusion of Blockchain, AI and IoT in healthcare and smart city.
- Section 3 talks about various use-cases pertaining to integration of IoT, Blockchain and AI
- Finally, Sects. 4 and 5 concludes highlighting the recent challenges with future directions.

2. Fusion of Blockchain AI IoT in Different Application Domains

This section discusses the application of Blockchain, IoT
and AI in various domains.

2.1 Health Care

Nowadays the use of Information Technology infrastructure in healthcare systems is inevitable. Health care systems stores, shares, and analyses the details of patients using electronic health records (EHR). The convergence of blockchain, IoT and AI ensures security with learning over health care information [25]. Typically the global scenario of COVID-19 provides the proof about the overburdened health care systems and weak disease surveillance systems which is resource-limited and thus the usage of mobile Health (mHealth) care is emerging. Mashamba et al. [26] recommended, the rapid development and deployment of low-cost blockchain with artificial intelligent in mHealth has linked of self-testing and verifying systems as one of the strategic reaction regarding COVID-19.

Wang et al. [27] the authors discuss about data sharing in cyberspace for big data, as well as powerful AI. The authors suggested a framework called SecNet, an architecture that can help secure data storing, computing and sharing in the large-scale web environment. This framework is used in a health care scenario to resolve issues in 3 stages. In the first stage, blockchain-based data sharing is implemented which ensures immutability, then in the second stage smart contracts are deployed to regulate the connections between trust-less entities, finally, the third stage uses AI-based processing for behavior analysis to effectively provide data provenance, audits, and control, as well as habits tracking. The authors have evaluated the design of SecNet in two aspects. The first being vulnerability, when struggling notorious network episodes like the Distributed Denial of Service (DDoS) attacks are dealt with and second being the earnings for contributors who provide the security rules on the blockchain. Finally, authors have addressed how to leverage blockchain for the access authorization on data demands by designing a secure and detailed smart contracts for data sharing.

Yan Zhuang et al. [28] discuss security and privacy concerns, data inconsistency, timely access to the right information across multiple health care facilities or Health Details Exchange (HDE). The authors have employed distributed ledger technology which is recognized as “unhackable” and also the authors use the smart-contract feature, which is a programmable personal executing protocol running on a blockchain. Finally, the authors have added a synthetic intelligence component to the blockchain adapters to allow researchers to retrospectively study HDE outcomes by analyzing log files, which can not be accomplished in current HDE systems.

Satamraju et al. [29] considered the data ethics to deal with vulnerability and physical threats over IoT networks. The authors here proposed a unique model that integrates IoT networks with blockchain to address potential personal privacy and security threats. This work has been implemented with conventional cryptographic algorithms on IoT devices and is not future-proof as these devices have resource constrained. The particular performance of this strategy is compared with similar models based on accessibility control, scalability and confidentiality. Finally, the authors concluded with the future focus to make blockchain inclusive to derive the advantages of both the applications resulting in secure social platforms with AI. The integration of blockchain and AI over health care systems has motivated to achieve the following tasks:

- An authentication scheme to confirm confidentiality and security of EHR records of patients.
- To study the methodology/framework of various security restrictions and machine learning models over health care systems.

2.1.1 Potential Models and Lessons

Seong et al. [30] have proposed a new verification framework concerning blockchain algorithms with artificial intelligence to verify the working of authentication mechanisms during access of health care data of Personal Health Record (PHR). The authors have utilized the Hyper POR algorithm in the blockchain and artificial intelligence neural network for the securing the health records. This proposed framework specifically uses Electronic Medical Record and Picture Archiving Communication System over Neural Network verification algorithm for the learning rate and epoch verification. In this particular framework, the author analyzed various techniques of verifying the perceptron concept and blockchain consensus algorithm along with artificial intelligence neuron network. The performance verification is done with the error back propagation and the simulation setup of blockchain decentralised application (DApp) with a wide range of etched artificial intelligence. In the end, the authors provided the potential risks to create technologies with a more secure plus tested infrastructure and established mechanisms for backing the activation of blockchain technology legally.

Bhattacharya et al. [31] proposed a novel framework that integrates lattices, blockchain, and Deep Learning techniques for privacy, confidentiality, and data consistency in healthcare. This framework termed as BinDaas (Blockchain-Based Strong Learning as-a-Service) can integrate blockchain and deep-learning techniques for sharing the EHR records among multiple healthcare users and operates in different steps. Step1 provides integrating DL and blockchain for securely storing the patient EHR data and renders future predictions depending on past repositories, step2 has a lattice-based key and personal verification scheme to resist quantum attacks, and step3 is for validation of the safety scheme and prediction model against existing state-of-the-art infrastructures. The authors have simulated the blockchain using Corda V3.0 and Corda DApp. This framework also deploys a strong learning LSTM which is used for future risk predictions from EHR.

Wang et al. [32] generalize the work related to
consortium Blockchain-based smart healthcare system for the data privacy conserving and sharing, called GuardHealth. Smart agreements are deployed on Blockchain to attain secure and efficient data storage and data sharing. GuardHealth manages privacy, authentication, data conserving and data sharing when handling sensitive information. Also, the authors discuss a trust model that is used for precisely managing the trust of users with the execution of the state-of-art Graph Neural Network (GNN) for anonymous node detection. As per the analysis made by the authors, the increased amount of person nodes and the malicious detection accuracy have been improved over the traditional techniques.

Chayakrit et al. [33] discussed the integration of blockchain with AI and IoT for data-centric analysis and information flow, its current limitations, and potential cardiovascular applications. The authors have used convolutional neural networks that were trained using ECGs from specific wearable sensors which keeps track of 549 patients health conditions, and provided cardiologist-level diagnostic accuracy. The authors also infer that blockchain might also be susceptible to malicious attack, a situation in which a malicious user acquires majority control. This would be a major challenge which should be addressed by formulating proper guidelines and the regulators will have to think about a very wide range of issues on data security, scalability, data integrity, and computational resources.

Ismail et al. [34] have proposed a lightweight blockchain model based on demographic cluster models. They have introduced one ledger for every cluster which maintains un-forked healthcare transactions on all the nodes in cluster that results in low overhead consumption and faster computation processing. Authors have introduced canals concept from 0 to 2 that provides more secure, better privacy and authentication methods for medical record transactions in particular canal members. Canal 0 was maintained as a public blockchain ledger that allows all the users to access and view the medical records in network. In every cluster, one node is selected as blockchain manager in order to reduce the latency and to avoid unnecessary communications problems in hospitals networks. The blockchain model was simulated using NS3 and compared with bit-coin networks over 100 constant nodes by scaling-up blocks from 10 to 50 at an interval of 10 nodes. The authors infer that their proposed model is 1.13 times faster than the existing models while performing replication of data and ledger updates. However, this model lacks real time implementation to address security, privacy and performance.

Dwivedi et al. [35] have proposed a hybrid model which combines ARX algorithms, lightweight Digital Ring Signature model and Diffie Hellman Key Exchange. The ring signature and public key sharing algorithm is used to provide security services such as privacy, integrity and availability for the electronic patient health records in blockchain architecture. The proposed model contains five modules such as Cloud storage, smart contracts, Overlay networks, healthcare providers and patient wearable devices. Initially, the wearable devices are equipped to the registered patients in network in order to monitor blood pressure, insulin, etc. The collected raw health information through wearable devices are encrypted and sent to the smart phone for formatting the data. Full formatted medical data is analysed with smart contract based on threshold values. The significance of threshold value is for identifying patient health record status. If the health record is abnormal, then smart contract will send an alert to the network and to the patient. However, this model further can extend on scalability, energy optimization and time complexity [36].

Mubarakali et al. [37] discussed an attribute-based privacy model with token based robust blockchain architecture for secure cloud healthcare records. The proposed model follows a set of healthcare wearable devices to collect samples from patients by using mobile devices and the data is encrypted with the public cryptography methods prior to uploading the patient information in the cloud health servers. The uploaded documents are reviewed by the doctors to get clinical test and genetic related data. The decrypted patient information will be accessed by doctors. The simulations are done on small banks datasets that improves 28% success rate as compared with existing models such as Ethereum, Hyperledger and Parity. In future, this can be extended to e-commerce applications in order to address privacy, delivery and payment options.

Kurdi et al. [38] introduced Healthy-Broker-Trust-Building architecture for Multi-Cloud Patient-Centric eHealth Services (MCPCS). The proposed model contain two stages of trust assessment in distributed ledger. In the first phase, the transparency is attained for all the transactions and feedbacks are received from different users by performing auditing and tracking operations. In phase 2, trusted-worthy patient information is taken into consideration in order to process the entries in distributed ledger. The simulations are performed on datasets of 50,000 patient treatment records, 25,000 benchmark medical records and 50 medical care team. The following malicious attacks such as feedback malicious isolated and feedback malicious collective data sets are defended by Health-Broker Multi-Cloud Model. However, the light-trust centric methods consumes more service time.

Yazdinejad et al. [39] have developed decentralized authentication based blockchain framework for patients, doctors and nurses in distributed hospital networks. This system reduces authentication time and increases throughput in inter-hospital networks. The authors evaluated their model using NS-2 simulator over the 3000 health record transactions and the metrics considered were response time, throughput, energy optimization and time overhead. This work doesn’t support scalability property of blockchain.

Tripathi et al. [40] deployed blockchain architecture for smart healthcare system (SHS) in cloud-based storage model. The authors have collected patient treatment records from various sources such as wearables, HealthApps, Lab data and E-Health Information from hospitals. The generated patient information will be encrypted via standard
blockchain model and stored in decentralized cloud storage system rather centralized model. The Electronic Health Transaction (EHT) gets stored in immutable cloud blocks. The proposed method provides transparent health data to all the stake holders without compromising the privacy of patients. It resists tampering of patient valuable information from malicious attackers. However, this model suffers from the scalability and bottlenecks of blockchain transaction processing.

2.1.2 Smart Cities

Last few decades, the advancements in industry, infrastructure, Information and Communication Technology (ICT), socio-economics created a huge impact in development of urban cities. There is a need of minimizing energy, wastage, pollution in air and water. The cities have to provide good water from different sources, to do public work programs, and to implement proper waste management systems to maintain clean environment. And also keeping in mind the density of the population in urban cities, the needs have to be addressed with new transformation. To develop an urban city, there are ideas coined in early years in the name of the garden city by Ebenezer Howard in 1898 and Le Corbusier has planned “Ville Contemporaine” in 1922. To address the current and future generation requirements, there is a need for transformation in the methods employed which implements sustainability in order to build efficient smart cities.

Tanwar et al. [41] discuss distributed ledger which has the probability to be deployed on various smart apps that are used to manage and monitor different parameters of smart cities operation. The particular combination AI, IoT and blockchain can provide highly precise results. Within this work, the author presented a comprehensive study on ML adoption for making blockchain based smart applications more resilient against attacks. These technologies can be combined in smart applications such as intelligent grid, smart metropolitan areas and so on.

Rahman et al. [42] considered the IoT deployment which revolutionized the industrial sector and the authors proposed a blockchain centred infrastructure to securely manage the data being generated. This specific support deals to secure services for IoT empowered nodes, uses AI for processing and extracting important event information of smart city and also provides semantic digital analytics. An integration of blockchain and AI over IoT in the smart city applications have motivated in performing the following tasks

1. To use secure mechanisms with blockchain and AI over smart city and its IoT data.
2. To study the potential models having various security restrictions based on blockchain and applying machine learning over IoT data in the smart city.

2.1.3 Potential Models and Lessons

Recently, smart cities are incorporating more and more advanced Internet-of-Things (IoT) infrastructures resulting in a huge amount of data gathered from various IoT devices that can be used for effective deployment mechanisms in smart cities. In IoT, using various tasks statistics with blockchain elucidations, large volume of data in various IoT devices can provide AI based decisions.

Shen et al. [43], proposes a privacy-preserving SVM training scheme over blockchain-based encrypted IoT data called a secureSVM. The authors has addressed a rigorous security analysis to prove that the suggested structure ensures the privacy of delicate data for every data provider as well as the SVM model parameters for data analysts. This work focuses on the novelty towards combining Paillier cryptosystem and blockchain methods collectively to address the uncertainties about data privacy, integrity and ownership, while training the machine learning classifiers using IoT data from different devices. Finally, the authors have given future direction intended to develop a generalized framework which allows constructing a variety of privacy-preserving ML training algorithms on multi-part encrypted datasets.

Mishra et al. [44] the authors generalize the work related to smart gas monitoring in the smart cities through Machine Learning and Neural Network technologies with blockchain based data security and privacy implemented in the IoT network. This helps to implement intelligent gas monitoring system. The bottlenecks consider are high sensitivity, selectivity for specific gas, higher response time and lower recovery time. Further, the authors conclude that the malicious invaders are unable to tamper the sensor data stored in the blockchain. The distributed storage of the IoT data helps to perform powerful AI computation effectively.

Pradip et al. [45] discussed the integration of blockchain with AI to meet the challenges of restricted training data in order to obtain high accuracy. The authors have addressed a multi-layer distributed security framework for sustainable smart city by leverage the features of blockchain and associated learning with IoT data. The structure of blockchain designed with multiple layers with classification of dataset using federated learning on the various scenarios were discussed.

3. Use Cases on Integration of Blockchain, AI and IoT

In this section use cases of applications and scenarios which integrated Blockchain, AI and IoT are discussed, and the same is represented in Fig. 1.

Use Case 1: Supply Chain Network and Logistics

A supply chain network (SCN) includes different stakeholders who are agents, raw material suppliers, and producers. This is a complex management network to gain minute deals of every task performed at each and every stage. The transaction processing system in the supply chain network consists of various levels of invoice generation and processing which incurs delay in the delivery process. Due to the complexity involved, majority of the organizations deploy an IoT framework to manage the shipment process. Blockchain
integrated with IoT can aid in improvising the robustness and tracking feature of the network. The best example of supply chain network is the Golden State Food supplier for huge food chain supply across the globe [46]. The research in terms of usage of intelligent blockchain in operations and supply chain management areas such as e-commerce, smart farming and public service is emerging rapidly in the recent years [47]. The organizations are analysing the deployment of blockchain for securing the existing integral infrastructure of AI and IoT especially in domains using SCN. An interview conducted with the top supply chain professionals revealed that the integration of the AI, IoT and Blockchain technologies will reform the supply chain business processes [48].

**Use Case 2: Oracle Smart Cloud**
The Oracle Blockchain Cloud Service [49] is a platform which enables integration of IoT network, intelligent data analytics and blockchain mechanism for managing data storage effectively and securely. This platform renders the following services:

1. Enterprise level services with elasticity feature
2. Ease of deploying and integrating with current infrastructure by providing various software frameworks and APIs.
3. Ease of deploying smart contracts with stakeholders.
4. Uses the proven Oracle identity management service for data privacy protection.

**Use Case 3: Smart Building and Planning**
The company Van Dorp takes care of managing and providing air conditioning and lighting services in cooperate buildings in and around Netherlands. TimeSeries is the management wing of Van Dorp which provides logistics and IT infrastructure. TimeSeries utilizes blockchain, Mendix, artificial intelligence (AI), and IoT technology to manage and analyze the services in each building. The organizations can track the systems running in their building remotely and in real time. [50], [51].

**Use Case 4: Intelligent logistics using IoT Blockchain**
SmartLog is a company dealing with providing an efficient framework to reduce the cargo transportation overhead cost. The SmartLog novel framework uses blockchain to securely record the cargo transactions and each shipment is management by an IoT network for remote monitoring the goods and an AI enabled smart contract is deployed for data access by the stakeholders. This makes the entire process of cargo management and tracking effective [52].

**Use Case 5: Smart IoT with Blockchain**
Bumble Bee Foods explores the usage of blockchain with IoT for its tracking of tuna products, right from where it was caught to how it was packed. They also built an app which integrates IoT, Blockchain and chatbot to communicate with the fishing crew to figure out the accumulation of fishes based on demographics [53].

**Use Case 6: Blockchain and IoT for smart parking**
A consortium of NetObjex, Advantech, and PNI Sensor Corp developed a model integrated with smart IoT and Blockchain which would overcome the parking issues. Each vehicle is embedded with crypto wallets for automating the parking transaction process. IoT enabled smart sensors would be deployed in the parking spots to notify the drivers about the availability of the parking space. The sensor data processing and the transactions would be recorded in the cloud and will be available to the users through a mobile app. This entire system eases the parking problem faced by many users especially in malls [54].
Use Case 7: Blockchain and smart IoT for water wastage management

The company Aquai has implemented a novel system to end water wastage by using smart IoT network which stops the flow of water upon detection of a leakage. This system uses cloud for sensor data processing and blockchain is used to store the processed immutable records [55].

Use Case 8: Blockchain and smart sensors to monitor river effluents

The companies Libelium and Airlab have collaborated to provide a cost effective solution for detection and monitoring of effluents in Volga river, Russia. The system consists of drones embedded with smart sensor for detecting the chemical levels of the water pollutants and transmitting this data to the cloud where the machine learning algorithms would compare the water quality and send this information to the private blockchain for further actions to be taken by the environmental scientists [56].

4. Challenges

This section highlights the challenges in integrating blockchain, AI and IoT. The current IoT networks have been employed with devices which are smart and have the capability of decision making, thanks to the various AI techniques implemented. Data reliability and scalability [57] are still a major challenge considering the huge amount of data inflow. The present world is using IoT for most of the application domain due to the vast connectivity option it provides. As IoT follows centralized client/server model, security and scalability are the biggest challenges due to the humongous nodes which are processing/generating data continuously. As blockchain follows decentralized approach [58], integrating IoT with blockchain solves the security issues, but scalability still remains a huge challenge. Ubiquitous computing is achieved using IoT which spans the connectivity across the public network. Since the internet is not secure, deploying a blockchain framework would be an efficient secured solution. As blockchain uses Proof of Work (PoW) concept, it is not suitable for several applications and thus not adapted by many industries [59]. Also embedding AI techniques in this framework adds to the overall delay in processing the transactions. Another challenge in integrating AI is the communication overhead and also the AI procedures have to be stored in the cache for dynamic routing decision, thus increasing the complexity and resource consumption [60].

5. Conclusion

In last decade, the blockchain frameworks are used prominently in various IoT smart devices. There are many researchers who contributed significant models for various research challenges in IoT domain. This work provided a systematic review on integration of blockchain, AI and IoT technologies to address the various challenges such as security, scalability, data reliability and integrity. Also, this article discussed potential models for various use cases on fusion of blockchain, AI and IoT. The future work lies in solving the further challenges such as scalability, overhead and processing delay while integrating IoT, Blockchain and AI in industry 4.0 applications.

References

Srinivas Koppu received the M.Tech. degree under the major of information technology with specialization in human–computer interaction from IIIT Allahabad, India, and the Ph.D. degree from the Vellore Institute of Technology (VIT), Vellore, India. He has been working as an Associate Professor with the School of Information Technology and Engineering, VIT. He has more than 14 years of experience in teaching. He was a Visiting Professor with the Neusoft Institute Guangdong, China, in 2018. He has published more than 30 international/national journals and conferences. He is a Life Member of the Computer Society of India. His research interests include blockchain technologies, the IoT, data analytic, cryptography, medical image processing, image security analysis, video processing and computer vision, and high-performance computing.

Kumar K is working in VIT–Vellore as Associate professor. He has completed his PhD in Software Engineering area. He has received his PG M.Tech. (CSE) from Pondicherry University and B.E. (CSE) from Madras University. He has 15 years of teaching/research experience and 3 years of industry experience in which he worked as a Software Engineer. His area of research includes Advanced Software Engineering, Formalizing Requirement Patterns, Recommender system and design for engineering problems. He is also interested to work on Machine Learning and its usage in various systems. He has several publications on international conferences and Journals. He has expertise in accreditation and assessment.

Siva Rama Krishnan Somayaji is a research member in Centre for Ambient Intelligence and Advanced Networking Research (AMIR). He has working experience in Centre for Development and Advance Computing (C-DAC) (Ministry of Science and Technology, Govt. of India), as research intern in data center technologies. He is also certified by EMC corp. as a proven professional in Information Storage and Management. Currently an EMC academic alliance faculty and played a key role in establishing a MoU between VIT University and EMC corp. He had proposed and developed an Intelligent Network design framework for building small and large-scale network. He also developed an efficient and secure framework for IP Storage network for C-DAC. His current interest includes e-waste management in India, wireless networks and cloud computing.

Iyapparaja Meenakshisundaram received Ph.D in Anna University, Chennai, BE and ME degree from the same. Presently, He is an Associate Professor in School of Information Technology and Engineering, VIT, Vellore. He has 12 years of experience in Teaching and Big data, Software testing and software Engineering field. He received University Rank holder award for his ME degree. His research interests include Software Testing, Software Engineering, Big data, Machine learning, cloud computing and Agile Testing. He is life time member of ISTE.

Weizheng Wang received the B.S. degree in software engineering from Yangzhou University, Yangzhou, China, in 2019, the M.S. degrees in computer science and engineering from the University of Aizu, Aizu-Wakamatsu, Japan, in 2021. Now he is a Research Associate in University of Aizu and pursuing the Ph.D. degree at the Department of Computer Science, City University of Hong Kong, Hong Kong. His research interests include applied cryptography, blockchain technology and IoT system.

Chunhua Su received the B.S. degree for Beijing Electronic and Science Institute in 2003 and received his M.S. and PhD of computer science from Faculty of Engineering, Kyushu University in 2006 and 2009, respectively. He is currently working as a Senior Associate Professor in Division of Computer Science, University of Aizu. He has worked as a postdoctoral fellow in Singapore Management University from 2009–2011 and a research scientist in Cryptography & Security Department of the Institute for InfoComm Research, Singapore from 2011–2013. From 2013–2016, he has worked as an Assistant professor in School of Information Science, Japan Advanced Institute of Science and Technology. From 2016–2017, he worked as Assistant Professor in Graduate School of Engineering, Osaka University. His research interests include cryptanalysis, cryptographic protocols, privacy-preserving technologies in machine learning and IoT security & privacy. He has published more than 100 papers in international journals and conferences.