Future Generation Computer Systems 141 (2023) 16–27

Contents lists available at ScienceDirect

Future Generation Computer Systems

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

Blockchain-based trust mechanism for digital twin empowered Industrial Internet of Things

Sasikumar A. [a], Subramaniyaswamy Vairavasundaram [b,*], Ketan Kotecha [c], Indragandhi V. [d], Logesh Ravi [e], Ganeshsree Selvachandran [f,*], Ajith Abraham [g]

[a] Department of Electronics and Communication Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, India
[b] School of Computing, SASTRA Deemed University, Thanjavur, India
[c] Symbiosis Centre for Applied Artificial Intelligence, Symbiosis International (Deemed University), Pune, India
[d] School of Electrical Engineering, Vellore Institute of Technology, Vellore, India
[e] SENSE, Vellore Institute of Technology, Chennai, Tamilnadu, India
[f] Faculty of Business and Management & Institute of Actuarial Science and Data Analytics, UCSI University, Jalan Menara Gading, 56000, Cheras, Kuala Lumpur, Malaysia
[g] Machine Intelligence Research Labs, Auburn, WA 98071, USA

ARTICLE INFO

Article history:
Received 10 February 2022
Received in revised form 26 October 2022
Accepted 4 November 2022
Available online 10 November 2022

Keywords:
Digital twin
Industry 5.0
Industrial Internet of Things
Blockchain technology
Proof of authority

ABSTRACT

Emerging technologies such as blockchain and digital twins are essential for the rapid development and employment in Industry 5.0 revolution. With the growing number of industrial IoT nodes, optimizing the network and availing of limited resources to enable secure transmission is difficult. A digital twin is the virtual representation of a physical device that completely depends on sensor data for the critical decision-making simulation process. To this end, we combine a blockchain-based distributed network with a digital twin for the Industrial Internet of Things (IIoT) applications. This paper proposes a blockchain-based Proof of Authority (PoA) trust mechanism to provide high-quality services such as security and data privacy in IIoT. Furthermore, to enhance the authority of decentralized digital twin combined blockchain networks, we introduce a Deterministic Pseudo-Random Generation (DPRG) to generate a genesis block. To evaluate the trustworthiness of the proposed system, we simulate the blockchain network with a digital twin using IIoT sensor nodes. The simulation result shows that the PoA-based authority master nodes can reduce energy consumption and enhance data security.

1. Introduction

The very first industrial revolution started in the 1780s with the development of electrical energy from water, heat, and biofuels. In the era of the second industrial revolution during the 1870s, industries with production plants and mass manufacturing units preferred electrical energy. During the third industrial revolution in the 1970s, the idea of automation was introduced to the manufacturing industries via embedded hardware and computing technologies. The development of the Internet of Things (IoT) and soft computing is the backbone for the fourth industrial revolution (Industry 4.0) and served to provide a real-time bridge between the digital and physical worlds through semantic interoperability. Although Industry 4.0 is still developing, several industrial innovators and technological experts are anticipating the beginning of the 5th Industrial Revolution (IR 5.0). Autonomous factories with human brains and computing techniques are the innovations of IR 5.0. By 2025, approximately three billion people are estimated to have access to the Internet because of the rapid expansion and distribution of mobile networks. Hence, it is necessary to integrate various techniques into a single infrastructure for IR 5.0 [1].

In recent years, manufacturers have been competing to meet the ever-changing demands of the market. This necessitates production plants that are adaptable, smart, and dynamic enough to fulfil customer demands. Corporate and production executives are of the opinion that industrial and business operations should be integrated. Such merging implies significant progress in industry processes and strategies. Furthermore, this can only be accomplished by integrating diverse elements of an organization, such as vendors, manufacturing units, and customers. The inception of the concept of Internet of Things (IoT) is said to be one of the greatest innovations of Industry 4.0.

* Corresponding authors.
E-mail addresses: drsasikumara@veltech.edu.in (Sasikumar A.), swamy@cse.sastra.ac.in (S. Vairavasundaram), director@sitpune.edu.in (K. Kotecha), indragandhi.v@vit.ac.in (Indragandhi V.), logesh.r@vit.ac.in (L. Ravi), Ganeshsree@ucsiuniversity.edu.my (G. Selvachandran), ajith.abraham@ieee.org (A. Abraham).

https://doi.org/10.1016/j.future.2022.11.002
0167-739X/

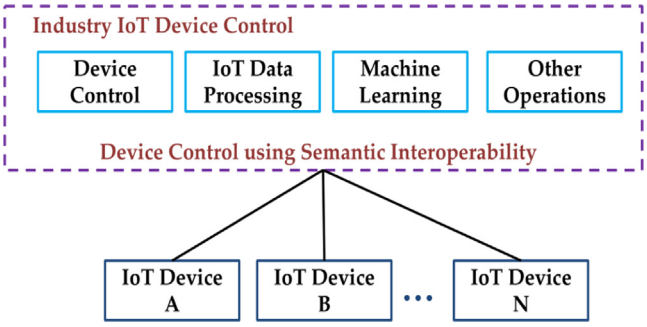

Fig. 1. Industry IoT device control using semantic models.

Industry 4.0 is all about automating routine tasks and using interconnected networks and smart cognitive computing to achieve precision, and effectiveness and enhance the performance of the system [2]. Once the full impact of Industry 4.0 is realized/achieved soon, the reduced need for human labour due to the changes in the production systems will emerge as one of the most serious issues. This is expected to bring fierce opposition from labour unions and policymakers, many of whom will see the gains of Industry 4.0 being offset by the loss of jobs and the reduction in the workforce. Another disadvantage of Industry 4.0 is that it does not concentrate on climate change. The innovations of Industry 4.0 have placed more importance on the enhancement of the related machine learning algorithms to achieve higher productivity and accuracy compared to the environmental sustainability of the world. On the other hand, IR 5.0 interconnects computing technologies with environmental and social control, thereby making it easier to implement the required changes to combat climate change.

IR 5.0 is expected to be a new technical standard of digitalized automation and decentralized control that will be implemented using a variety of frontier technologies such as the Industrial Internet of Things (IIoT), deep learning, data science, and edge computing [3]. In the context of smart manufacturing and smart factories, distributed production is a type of decentralized manufacturing conducted by companies that use digitalization and involves the development of a communication model for data exchange, analysis, and real-time collective decision-making process [4].

For Industry IoT device control, semantic interoperability can be implemented by declarative and fuzzy models encoded in basic knowledge of some sort. The key idea is that by creating these structured semantic models about IoT device A, other devices interconnect with the same techniques and receive an unambiguous perceptive of the device. This unambiguous perceptive is the foundation for other devices to confidently communicate with the IoT system to achieve some desired decisions illustrated in Fig. 1. Hence semantic interoperability is used to enhance the decision process of the IIoT system.

A digital twin model is a digital version/model of a physical operation or real-world system, such as industrial systems, but in a virtual environment. Digital twins are constantly updated with real-time data to match the actual properties and behaviours of the physical object or process that it is representing. In smart manufacturing, a distributed production system is represented in hierarchical tiers using several digital twins [5]: (i) At the operation level, a digital twin is a virtual network used to represent individual items. Digital twins are developed to accurately model the physical devices and understand their physical counterparts within the network. (ii) In the shared network architecture, a group of physical devices is modelled with a sub-system of digital twins that reflects the sub-physical components. The data from sub-system digital twins are transmitted to the next level for further processing.

1.1. Recent challenges on digital twins

The following section describes the recent challenges associated with integrating digital twins with IR 5.0. From the research development point of view, the challenges faced in this aspect are also associated with other technical fields such as data science, machine learning, semantic models for IoT, and blockchain. Some challenges integrated with digital twins are discussed as follows.

(1) Information technology network architecture

The current network infrastructure does not integrate data analysis and IoT communication in the same framework. The digital twin requires a network infrastructure that will enable interconnection between the data processing unit and the IoT platform. These smart networks will enhance the impressive simulation through the digital twin. Without a proper IT network architecture, it is not possible to achieve the desired data simulation or visualization using digital twin technology.

(2) Data inference

The second challenge of the digital twin is the enormous amount of data needed to create the environment for simulation. For this, the data must be in digital form and need a quality sequence of the data stream. Analogue data or signals with noise would cause inconsistent simulation and would cause the digital twin to underperform. Therefore, the quality and consistency of the data and the number of IoT nodes are important parameters in the implementation of digital twins. To improve the performance of the data simulation or visualization process, it is necessary to input the right type and amount of data at specific times.

(3) Data privacy and security

The important challenges of the digital twin associated with industries are data security and privacy because the entire operation of these smart industries depends on the data generated by the system that will be used for the simulation process. Firstly, the system generates a vast amount of data, and this information is very sensitive. A small change in these data poses a security risk to the entire system. To avoid such potential security problems, the digital twins need to be integrated with frontier technologies. This integrated security system will also enable the data transfer between the IoT nodes and the processors. Hence it is necessary to develop data privacy and security in digital twins to overcome the trust and privacy issues within the industries.

(4) Trust

Digital twin-based smart systems have always been associated with the data reliability of the organization and the users. Hence, the next major challenge with digital twins is associated with trust. From the organization's point of view, the end product must satisfy the clients' requirements so that the clients would always trust the product quality of the company as well as the reputation of the company. Digital twin technology must be integrated with a highly secure architecture and must be constantly improved at every level of development to ensure data quality. One of the methods of improving data security is to create smart contract-based digital twin systems that can overcome problems related to data security, privacy, and trust.

(5) Predictions

The real-time implementation of the digital twin in an organization is still a challenging task [6]. The need for a smart IoT system will be able to satisfy the expectations of an organization. Researchers need to develop solid foundations of digital twin

infrastructure to achieve this. For companies, it is not necessary to integrate digital twin with their infrastructure because of recent technological trends. Therefore, the digital twin is also facing a challenge to satisfy the expectations of the companies. These challenges are like those that are already faced by the IoT and blockchain technologies before entering real-time market integration. From organizations' point of view, the challenges for digital twins are completely associated with user privacy and data security.

(6) Standardized modelling

For any technological innovations, researchers need to propose a standard model for practical application purposes. The next challenges of a digital twin physical process are associated with the modelling of smart infrastructure. Starting from data collection and digital twin simulation, companies need to follow the standard model for integrating their system. This integration of the system may be a physical or simulation-based data-driven model. The primary use of standardized modelling is to ensure proper implementation of dynamic semantics digital twin integration with the organization.

(7) Domain modelling

The final challenges of digital twins are associated with domain modelling. The digital twin development must generally be a multi-domain infrastructure [7]. The need for domain modelling is to ensure the correct information transfer to each stage of a digital twin. This domain modelling ensures proper architecture with domains such as data science, machine learning, and IoT embedded into the digital twin system. Hence, domain modelling for digital twin systems will enhance the replication of the different stages in the future.

Several digital twins are used to reflect the updating of industries with physical assets in real-time, such as equipment conditions and history data. The implemented digital twins effectively interact with one another by predicting inherent hazards inside the remote production systems using the optimization of a data-driven approach. The digital twins cooperate by employing data-driven analyses to evaluate the system based on historical information, understand its products using shared knowledge, and update and predict possible errors in real time. Greater awareness of the expected possible risks can help humans reach proper decisions on the semantic-based IoT design patterns of distributed production systems. However, the digital twin paradigm is still in its infancy, and there are numerous obstacles to overcome before it may be adopted. These difficulties include the following parameters [8]:

- Interoperability: The framework and scheme of exchanging information between organizations required to define the digital twins' model and security mechanism.
- Authentication: Most of the time, the digital twins are employed with the help of an individual entity in the decentralized production system. Therefore, verifying digital data in the system requires a cost-efficient security system to collect real-time information among different entities.
- Decentralized decision-making system: A small error in the data causes failure in the centralized system and requires more time to make the correct decision. Decentralization provides a consensus algorithm for the decision-making process while requiring global data from the organizations.
- Feasibility and reliability: An industry needs to adopt numerous digital twins to indicate several system entities such as objects, elements, devices, nodes, humans, and computers. This distributed architecture can be implemented through multiple digital twins since it is necessary to provide feasibility and reliability in digital twins within the manufacturing unit.

Security, a decentralized ledger, information sharing, end-to-end connection, trusted traceability, and scalability are all the benefits of using blockchain with digital twins [9]. Multiple digital twins can collaborate in a hierarchical and granular way utilizing blockchain, employing collective information to control and monitor product assembly data [10]. A smart contract is used to automate some operations to improve data exchange reliability and effectiveness, provide trustworthy data, enable lightweight use of data, and enable activity monitoring for stakeholders in the production of digital twins. Moreover, the previous scientific literature is mostly focused on blockchain adoption for digital twins. It misses alternatives for constructive digital twins based on organizational business intelligence and security measures. There are quite a couple of difficulties that need to be investigated further to recognize, evaluate, and eliminate possible risks in distributed smart factories using the expertise of blockchain-based digital twin-driven operational information.

1.2. Contribution

In IR 5.0, the integration of blockchain and digital twins constitutes the core technologies that enable semantic data acquisition. Moreover, combining these two technologies provides considerable benefits in addressing the issues related to security, such as transparency, privacy, ensuring rights of ownership, and decentralization, among others [11]. The integration of blockchain and digital twin, on the other hand, is still being investigated. Many studies have recommended the adoption of digital twins using a simplified blockchain paradigm, with a focus on centralized manufacturing processes. These research efforts have failed to create digital twin-based distributed processing networks. Furthermore, an appropriate blockchain has not been developed for digital twin technologies to overcome the prediction risks in the system [12]. Instead, researchers have developed a blockchain model that has incorporated a distributed ledger for the decision-making process in the industries [13].

In this study, we develop a smart architecture to enhance the data management unit, user privacy, data security, and digital twin-based virtual maintenance for IR 5.0. The novelty of our proposed system is as follows:

- First, we investigate how blockchain technology is adopted in digital twins while expounding the advantages of integrating these two technologies.
- A Proof of Authority (PoA) based blockchain network is proposed to ensure the security of the sensor nodes and data protection.
- The ever-increasing demand for the integration of such technologies by numerous organizations poses a great challenge to the public blockchain model.

To overcome these issues, we mainly focus on the adaption of a PoA, Authority Masternodes (AM), and Deterministic Pseudo-Random Generation (DPRG) blockchain-based lightweight security for IIoT.

2. Related work

The revolution of Industry 4.0 is almost over, and it has attained multiple successes in intelligent manufacturing system design. IIoT-based systems already predicted that the next innovation revolution could be IR 5.0. If the present-day Industry 4.0 emphasizes the alteration of factories into IoT-enabled smart facilities that apply soft computing methods and interlink these through cloud servers, IR 5.0 is expected to focus on the use of human effort and smart thinking in developing intelligent industrial systems [14].

IR 5.0 is the recent revolution in which human intelligence and machine intelligence are combined to develop automated, intelligent systems for efficient production. Most of the factories have already initiated some aspects of IR 5.0 and are implementing new innovative techniques to improve the performance of machines. Small and medium-scale industries are trying to adapt to Industry 4.0 and incorporate principles of IIoT. Although many companies have started using the latest technologies, they are not ready to retrench their workforce.

The principles of IR 5.0 are simple, and it reduces the overall cost and time for development. However, many manufacturers have this fear of adopting the latest technologies such as soft computing, blockchain, digital twins, and cyber–physical systems would reduce the need for a human workforce and cause massive retrenchment. Industry 4.0, on the other hand, may result in more workforces being recruited, especially in the manufacturing and production divisions. This will allow the company to restructure the workforce to handle only the essential tasks while leaving the machines to handle the automated work intelligently and systematically.

Researchers and practitioners predict that IR 5.0 could start with the interaction of human ability and AI/soft computing techniques. The interconnection of human minds and intelligent machinery are expected to take factories to new levels of accuracy and speed. IR 5.0 could also be more beneficial to the environment as factories begin to implement machines that run on green energy and dispose of waste safely [15].

AI and soft computing techniques can improve the performance of robots and the interaction between human minds and computers. Hence, the integration of human intelligence and factory robots will ultimately increase production efficiency.

The implementation of industrial revolutions depends on the company policy. No matter how fast the companies adapt to the industrial revolutions, some of the basic principles will still be implemented in the manufacturing world. As companies adapt the latest technologies, they will begin to realize exponential production due to capabilities provided by IoT and IIoT systems, cyber–physical systems, and AI approaches [16].

The transformative outcome of digital, data-driven-based companies is reinforced by the principles of Industry 4.0 since it is necessary to develop new revolutions which will adapt to the needs of the company and the industry. The Covid-19 crisis has enlightened the need to restructure the traditional/conventional working model and approaches. It has worsened the vulnerabilities faced by some companies such as breakable strategic value chains, and unstable supply chains, and exacerbated the need to develop innovative methods. To overcome such vulnerabilities, companies need to transition to IR 5.0 and explore the latest frontier technologies that would enable efficient interaction between human intelligence and AI/soft computing techniques. IR 5.0 focuses on implementing technologies that support factories for better integration of the social and environmental system. As a part of the IR 5.0 framework, the following techniques and/or other frontier technologies would be combined [17].

- Individualized human mind and machine interaction
- Digital twins and simulations
- Data science and data analytics methods
- Soft computing techniques
- Semantic-driven edge computing
- Innovative technologies that support renewable energy resources.

Although Industry 5.0 is a relatively recent invention, some early academic material details its primary elements. The research on IR 5.0 reveals a great deal of ambiguity regarding what it will offer and how it will affect businesses in detail, and its potential to tear down barriers between the real and virtual worlds. Based on our research and projections, IR 5.0 is predicted to be characterized by a renewed and broader sense of purpose, moving beyond producing goods and services for profit. Three fundamental parts make up this larger goal: (i) human-centricity; (ii) sustainability; (iii) resilience. Revenue strategies have grown increasingly unsustainable in recent years. A narrow focus on revenue in a globalized society fails to effectively account for environmental and societal costs and benefits. Hence, a company's actual aim must encompass ethical, ecological, and societal factors if it is to become a true generator of genuine prosperity. This comprises ethical development targeted at boosting prosperity for all parties involved: entrepreneurs, employees, customers, community, and the ecosystem, not just or mainly focused on reducing cost or maximizing profit.

From a human-centric perspective, the industry workplace requires skilled and semi-skilled manpower at the heart of the manufacturing operations instead of using emerging technologies as a preliminary step and analysing their potential for boosting efficiency. Rather than asking labourers to adjust their abilities to meet the demands of quickly increasing automation, we want to use innovation to modify the production chain to the demands of the workplace, such as guiding and training them. It also entails ensuring that the use of new technologies does not compromise workers' basic privacy rights, independence, and human dignity.

Industries must be responsible for respecting geographical boundaries. It must create cyclic operations that reclaim, recycle, and reuse natural resources while reducing pollution and effects on the environment. Sustainability entails lowering energy and greenhouse pollution to avoid loss and degradation of environmental biodiversity and to meet the requirements of the present generation while protecting the needs of future generations. AI and 3D printing technology can help here by optimizing energy utilization and reducing waste.

The term "adaptability" refers to the necessity to improve industrial production's resilience, equipping it to better handle interruptions and ensuring that it can offer and support key infrastructure in moments of emergency. The vulnerability of our existing approaches to international production is highlighted by geopolitical developments and ecological calamities, like the Covid-19 outbreak. This should be countered by the development of adequately durable critical value chains, versatile production capabilities, and dynamic business processes, particularly where value chains service essential human needs like medical or protection.

2.1. Digital twin

In 2003, at a Michigan State University lecture on Product Lifecycle Management, Michael Grieves suggested the concept of digital twins for the first time [18]. In 2011, NASA developed the first executable digital twin to predict the structural behaviour of aeroplanes. The main idea is to examine and create virtual items to replicate real-time operations. NASA experts then presented their findings on digital twins in a seminal paper entitled "An interactive multi-physics, multi-scale, probabilistic simulation of a complex system". The white paper by Grieves in [19] also talked about sensor updates for aircraft history, vehicle or device that employs the best quality physical models, among others, to reflect the life of its flying counterpart.

The literature review in [20] outlines the notion of digital twins, their emergence, and how they add value to industries. The technique, which involves the use of digital models to better understand and manage physical assets, how these digital models are well entrenched in certain companies and has the potential to drastically alter logistical operations [21]. Please refer to Fig. 2 for

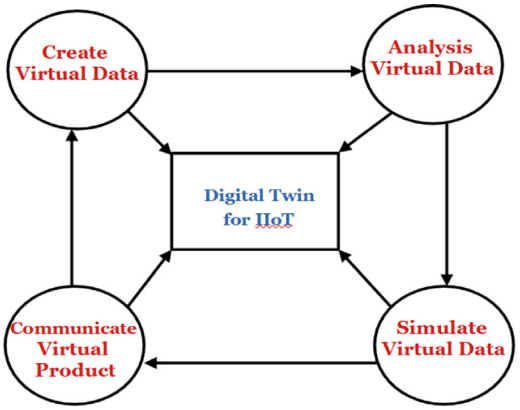

Fig. 2. Digital twin data-driven framework for IIoT applications.

a digital visual illustration. Assume that the number of potential implementations of digital twins grows every day. In such a situation, it becomes clear that the scientific community has yet to agree on what defines a typical digital twin. This might persuade a company to declare it was implementing the latest technologies which contain asset-tracking capabilities as digital twins. This method avoids reducing and underselling the complexity and long-term benefits of a fully functional digital twins system [22].

The qualities listed below suggest what makes a digital twin engaged in advancing understanding of the system and serving as a framework for new scholarly endeavors. These characteristics are confirmed by the results from existing studies. Recent academic research in this area mainly focuses on integrating digital twins for real-time applications [23]. The following are some of the properties or characteristics of digital twins:

- A digital version (or model) of a physical thing or operation is known as a digital twin.
- The digital twins are constantly updated with real-time data to match the actual properties and behaviours of the physical objects or processes that it is tasked to model.
- Digital twins are used for visualizing and analysing physical objects or operations, and deep learning can make further improvements and assumptions to the system.

The aforementioned properties can apply to the design of digital twins for any system that includes small to large sizes of manufacturing units or any other smart applications.

Digital twins are the process of reproducing physical components of an object into digital form. In this replication process, real-time systems such as wind farms, manufacturing units, aircrafts, constructions, and supply chain management, can be represented in digital form using digital twins. The initial concept of digital twins was introduced in 2002. However, it only began to be implemented for real-time applications in recent times because of the IoT and IIoT revolution. IoT made the digital twin a cost-effective process for replicating physical objects or processes [24]. Through industrial IoT (IIoT) systems, real-time signals are converted to their digital form for simulation. This assigning process of real-world physical systems digitally with the help of the digital twin makes it realizable and analyses the digital form to avoid problems before it originates in the real-world objects or processes. The fast progression of machine learning, swarm intelligence, blockchain, and data science models/methods has enabled digital twins to become a cost-effective alternative and increase the overall performance of the system [25].

In IR 5.0, a digital twin can play a major role in the implementation of custom-made equipment in factories. A digital twin can be a well-developed business model with minimal faults and errors and contribute to fast improvement in sales to book profits. The primary use of the digital twin is to overcome technological defects through a digital simulation model. The other benefits of the digital twin are used to restructure the basic model of the manufacturing system and make it possible to predict system faults in the future to prevent large losses to the business. Digital twin-based smart system network design enables companies to visualize financial advantages and increase their profits.

The purpose of integrating digital twins into IR 5.0 is to create a virtual simulation environment to enable real-time data analysis and modify the physical system with the help of IoT and IIoT. Digital simulation-based system customization, on the other hand, enables users to visualize the needs of their products. Hence, the integration of digital twins can eliminate the system faults before it occurs which can improve the business model and increase the profits of the companies.

2.1.1. The impact of digital twins on IIoT

In visualizing IIoT sensor data, it is clear that digital twins integrated into the manufacturing process of factories can be beneficial [26]. Many organizations believe that the introduction of current digital technologies has a favourable impact on visualization, particularly those that modify earlier issues in detecting sensor activities. This is also true in the case of digital twins by offering functional information that may be able to improve system performance. A digital twin, in particular, will significantly enhance the performance measures of accessibility for detecting digital data and visibility for processing, and this aggregate data network of information can be used to organize internal and external faults. However, implementing a semantic digital twin is a dynamic and resource-intensive process that does not necessarily guarantee complete data visualization.

2.1.2. The advantages of digital twins

The potential benefits of the implementation of digital twin systems will vary substantially due to the differing complexity and extent of applications of digital twins. A digital twin enables clients to undertake routine tasks at their twin properties from a distance, thereby maximizing benefits and lowering service expenses. Digital twins can also be implemented to automate repetitive tasks that are sensitive to human mistakes, thus enabling the allocation of resources for more significant operations.

Digital twins have frequently contributed in the following areas: improved decision-making due to more data availability, process optimization, and resource allocation, which allows for the adoption of innovative business practices. For example, a digital twin can facilitate the transition toward intelligent manufacturing and service innovation within firms that could not do this previously, as maintaining an asset through its lifespan gets highly proficient. The list of advantages can be divided into four categories, as described below.

(1) Analytic value

The main benefit of employing digital twins is the capacity to acquire data that is generally hard to quantify, such as information generated from company assets. Relevant choices and suggestions can then be made based on this information to maximize the development of future assets.

(2) Synchronous value

Using digital twins, data from duplicated physical devices can be immediately examined from a distance. Even though this remote monitoring method has several benefits, it may be particularly useful if the physical devices are situated in dangerous or hard-to-reach places.

(3) Predictive value

The possibility of producing reliable predictions of an ecosystem in which digital twins will be extremely useful. The large amounts of data generated by digital twins can be used to predict the future direction or allocation of physical resources. The most sophisticated forms of virtual data can forecast and provide solutions to issues that will arise. Intelligent devices that can make an independent decision about which resources to develop to optimize the profits generated for staff and stakeholders will almost certainly require digital twins.

2.2. Blockchain

Blockchain technology has the potential to provide tremendous value to IR 5.0 in the upcoming years. In IR 5.0, a centralized system of a massive number of diverse linked devices is a major difficulty. Through establishing distributed authority, blockchain can be utilized to construct decentralized and distributed organizational structures [27]. Secure peer-to-peer interactions allowed by blockchain provide an irreversible ledger for safekeeping records [28]. Furthermore, in the implementation of IR 5.0, the irreversible ledger supports operational integrity and responsibility for critical occurrences.

Integrity is extremely important for the resolution of disputes in the IR 5.0 environment. Smart contracts can be utilized for privacy preservation in IR 5.0 operations, such as data verification and programmed manufacturing operations. A segmented and decentralized method using blockchains can also provide a higher level of security to receive and collect data and protect transactions.

For automated customer maintenance in IR 5.0, blockchains can be utilized to create secure user identities for various individuals and businesses. This is required for network access and user authentication in any industrial activity that takes place over a public network [29]. Additionally, these digital identities can be used to manage rights, assets, items, and activities. In addition to registering intellectual properties, blockchain technology can be used to catalog and store creative work [30]. By regulating the consensus procedures among different stakeholders, blockchain-based smart contracts can help to automate the contractual process.

Furthermore, blockchain decentralized ledger-based manufacturing process allows machine-to-machine communication and data exchange. Distributed ledgers and consensus mechanisms are employed to automate and add a dynamic nature to the contractual process by regulating agreement activities among the various stakeholders. Smart contracts are utilized in the IR 5.0 process to enhance security, which includes identity verification and automating customer operations.

Blockchain is a digital system that is transparent, unchangeable, decentralized, and safe when it comes to storing information. It also consumes more energy because data mining at its nodes necessitates the use of more resources. However, it provides data protection by using cryptography hashes of earlier records.

In IR 5.0, blockchain seems to have the ability to significantly contribute to security and privacy issues. On the other hand, blockchain technology requires a large amount of energy. Hence, the number of sensor nodes in blockchain-based IR 5.0 process developments may need to be reduced. To prevent this, a lightweight blockchain platform that separates the infrequently used data from the network and stores it on a sidechain could be built. Quantum computing can also be utilized to effectively secure cyber–physical systems [31].

2.3. Integration of blockchain with digital twins

In some organizational sectors, the digital twin has been connected with blockchain technology for secure transactions [32]. ManuChain is a suggested iterative approach based on the integration of blockchain technology into decentralized production [33]. Based on the decentralized nature of the network, the ManuChain model has been implemented with less concentration on the self-automotive process and more optimization process for the coarse-grained system. Makerchain is another digital twin-based blockchain technology approach that was developed to handle the cyber credit of social manufacturing among different producers [34].

In the Makerchain network, a digital twin has been implemented to synchronize different data tags and guarantee security for the transactions between different vendors. The digital twin-based blockchain of things model has been implemented for the manufacturing process to provide a secure, transparent, and decentralized system [35]. This framework also concentrated on the data-driven approach for decentralized manufacturing processes and updating network security through tags. In [36], the authors proposed an ExplorerChain-based blockchain network model for the healthcare domain. The explorer chain consists of machine learning, metadata of agreement, and the consensus mechanism to provide high-quality services.

Tao et al. [37] developed a smart framework for industrial manufacturing units which uses digital twin and blockchain technology. In this framework, a blockchain network is used to overcome the challenges of security service in the smart manufacturing system. Aguilar-Ramirez et al. [38] investigated the blockchain-based consensus mechanism and digital twin for supply chain security management. In [38], a review is conducted for supply chain management and found that digital twin integrated blockchain technology provides transparency and security.

Wang et al. [39] discussed the sensor information collection and management model to deploy digital twins for real-time application. To protect sensor data from unknown users, this work implements blockchain network-based digital twins architecture for IoT devices. Sadman Akash et al. [40] present a blockchain-based framework for healthcare digital twins. Leveraging the security of blockchain, the model seeks to collect details of patients and manage it with proper mathematical delineation. The aforementioned blockchain framework for digital twins mostly focuses on the security and management of data than the consensus mechanism.

Most of the digital twin integration with the blockchain model approach is discussed to develop security architectures in smart industries. Still, none of the studies implement the adoption of digital twins based on the blockchain network technology to enhance the trust mechanism in the decentralized smart IIoT applications.

3. Proposed blockchain trust mechanism for digital twin based IIoT

3.1. Blockchain-based security and trust mechanism

In terms of information exchange, function, and controls, the production process was commonly depicted as a "black box" until the era of smart IIoT. For each equipment, activity, and procedure, this black box can be effectively split into smaller "black boxes". Emerging technologies, such as improved sensors and digital twins are allowing these "black boxes" to become more accessible [41]. The partnership among companies, on the other hand, can provide potential advantages to all parties in the system. However, in the old model of centralized operations, the

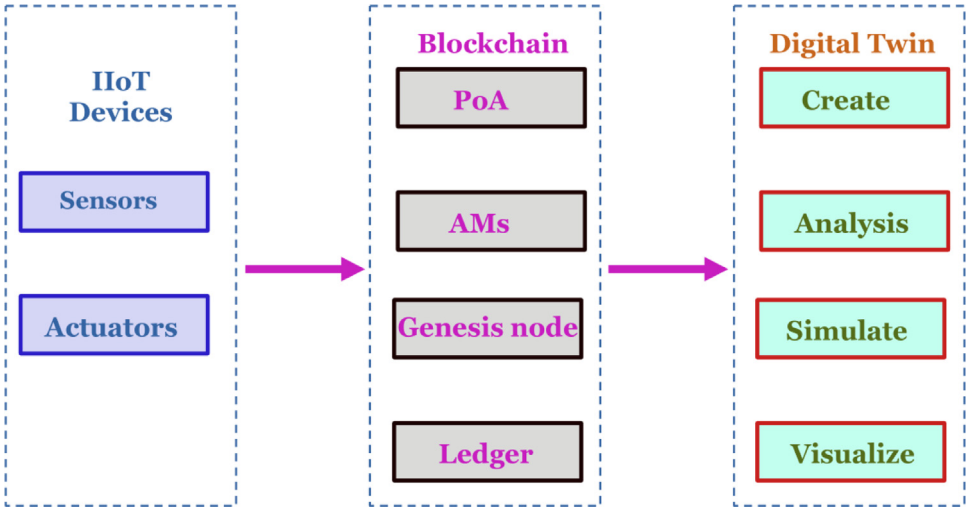

Fig. 3. The proposed integration of blockchain and digital twins for the IIoT network.

idea of constructing a single hub to govern every node stymied collective bargaining. The loosely organized manufacturing environment can quickly come apart if a tiny delay or error occurs if there is not enough trust.

On a worldwide scale, a lack of confidence stifles cooperative production innovative behaviour, profitability, and effectiveness. Blockchain technology can solve the problem of trustfulness. Participants share transaction information over a public of untrustworthy nodes rather than deciding on a single trusted party.

Blockchain provides an appropriate platform for exchanging data from many parties and performing calculations relevant to cross-organization partnerships. The exchanges among hubs in the public blockchain are what give them their trustworthiness. Members in the blockchain platform depend on the ledger technology and infrastructure to mediate interactions among producers in the same shared system, rather than a centralized location or any third-party entity.

To alleviate the significant "trust cost" placed on companies, some production data can be transferred to a public blockchain network. Information security and creative associate dependability are two areas where companies may improve their trustworthiness. The possibility of blockchain to lower trust costs in trades is well-known. Numerous transactions take place between a company and its customers, agencies, vendors, resellers, mobile operators, and other producers during the development and assembly of the products, and the support life cycle of the products.

In the view of information security, asymmetric cryptography requires private and public keys to encrypt and decrypt data transferred in the network. Another important mechanism to enhance the security in the information system is developed through hashing functions. This will also create new blocks in the blockchain network and provide integrity to the transactions. These security mechanisms will increase the trustworthiness of the network and provide guaranteed transaction security among stockholders. Crypto systems have been used to represent the digital data of untrusted variables such as task information, contact details, identification data, transaction records, property information, and contract data. It is linked to the blockchain to fulfil privacy and identity validation needs. The blockchain will be updated with the newly validated block. After being propagated, it will be kept by all network nodes, and a consensus will be reached on the most recent blockchain.

The shorter chain will be rejected if the blockchain causes a partial conflict. The blockchain has discovered secure file formats that can support industrial partnerships. The consensus mechanism could provide a method for untrustworthy participants to collaborate in a trustworthy manner. Predetermined external circumstances, like tasks, can activate a shared ledger. Rules that are very well defined can cooperate among participants.

3.2. Enabling technologies and significant components

This section goes through three essential technological solutions for the use of blockchains in industrial automation: smart contracts, IoT, and consensus mechanisms. Smart contracts are designed to operate on blockchains. The contract terms in smart contracts cannot be changed without the consent of all the parties involved. Smart contracts can accomplish tasks that would otherwise be labour-intensive in a regular environment. As a result, it also has the potential of making the production method extremely cost-effective, efficient, and profitable, and private. Smart agreements can be used at any point in the planning, manufacturing, product, or operation life cycle.

A smart contract between a supplier and a distributor can be reached regarding how well goods should be packed, carried, distributed, and maintained. A smart contract can be formed by adopting best practices and budget control between a marketing firm and an actual sales company based on blockchain data coupled with argument principles. Finally, the company and its authorized suppliers can form an agreement on how and when the device should be serviced, replaced, improved, and so on. It is worth noting that, while smart contracts in their current form are not necessarily smart or connected to legal agreements, a potentially important future research direction is figuring out how to make them intelligent. Fig. 3 shows the pictorial representation of the proposed architecture for IIoT networks.

To store information recorded through the sensor nodes, blockchains can be combined with IIoT systems [42]. A constructed functionality in IBM's Watson IoT gateway enables chosen information to be put into a private blockchain [43]. This private blockchain is shared among company partners who can then authenticate every activity, ensuring that each partner is held responsible and accountable for their actions. Ericsson used blockchain technology to create a new system called "keyless signature infrastructure" to improve data integrity [44].

In the concept of decentralization, the consensus process overcomes the problem of mutual trust between nodes. Proof of

work (PoW), proof of stake (PoS), and a lightweight consensus mechanism have all been suggested as common ways of an agreement. The characteristics of node authenticity control, energy savings, and attacker-accepted power have all been thoroughly examined, and improved solutions have been proposed. Some specific consensus-based procedures should be investigated to achieve blockchain-based manufacturing systems. Smart manufacturing may make collaborations more efficient, active, safe, and convenient.

3.3. Proof of authority

The main challenge of a public blockchain model is developing consensus mechanisms concerning application needs. The consensus algorithm defines how blockchain networks agree on the new node development. Another challenge of a public blockchain is to incorporate the governance model which will be implemented on the same consensus algorithm. The recent development of governance principles is completely integrated with decentralization networks.

In this study, a Proof of Authority (PoA) based consensus model for IIoT applications is proposed. The PoA-based blockchain model is suitable to adapt the governance model that can avoid anonymous node creators [45]. In this governance model, every block can be authorized by Authority Masternodes (AM) to enhance the security of the network.

To be an AM in the blockchain network, a single node or group of nodes deliberately discloses their identity to the IoT base station. Since the base station is a validator to authorize the AM and produces new blocks. Once an AM is authorized by its industries, then it has the right to transfer the data between the node and verify the results. For any organization, PoA-based AM gives additional security and reduces the overall transaction time. From an industry's point of view, each AM must go through a governance model philosophy which will be developed by a set of committees in the organization. Therefore, PoA-based blockchain technology will enhance the security of AM.

Assume that the company IoT architecture schedules a new sensor node to be created once every α seconds. We set time $\alpha = 20$, which is based on the IoT network usage time of adding new nodes. Let us consider t_0 assigned as the timestamp of the source node. The timestamp of each node consists of height t_h when $h > 0$, and the term h satisfies $h = t_0 + m\alpha$, where $m \in R$ and $R \geq h$.

In the initial period of operations, PoA gives equal rights to AM to allow it to generate and verify nodes. To achieve this, we proposed a Deterministic Pseudo-Random Generation (DPRG) to select any node present in the network. We also introduce "active/inactive" AM status to check a particular AM denoted as a is willing to verify and generate a node $(h,)$ which includes height and timestamp parameters. The timestamp also satisfies the condition $(t - t_0 mod\alpha = 0)$. The general expression for DPRG to produce a pseudo-random number $\gamma\,(h, t)$ is computed using Eq. (1):

$$\gamma\,(h, t) = DPRG\,(h, t) = hash\,(h \circ t) \tag{1}$$

where circular dot terms represent the concatenate of two-byte arrays. We have generated pseudo-random number values using concatenate operation between height h and timestamp t.

Let A_B represent the sorted set of AMs with the active mode in the state related to block B. Note that in blockchain framework a fixed index number is assigned to each AM and the values are utilized to sort elements in A_B. To validate whether a is an authorized AM for producing the given status that generate $B\,(h, t)$, the value of the expression given in Eq. (2) need to be determined.

$$A^a_{B(h,t)} = sort\left(A_{PA(B(h,t))}\right) \cup a \tag{2}$$

In Eq. (2), the value of $PA\,(.)$ returns the value of the parent node. The next process is to compute an index $i^a\,(h, t)$ using Eq. (3).

$$i^a\,(h, t) = \gamma\,(h, t)\ mod\ \left\|A^t_{B(h,t)}\right\|. \tag{3}$$

An AM node a is the authorized generator of $B\,(h, t)$ if and only if $A^a_{B(h,t)}\,[i^a\,(h, t)] = a$. The term "active" is to highlight the status of AM which does not directly indicate the physical state of a particular AM because this status signal is simply copied from the incoming data of the network.

3.3.1. AM status update

In the AM status update process, we need to consider the latest node $B\,(h, t_1)$ and its parent node $B\,(h-1, t_0)$. For any $t_0 < t < t_1 \wedge (t - t_0)\ mod\alpha = 0$, the network calculates the value of AM using Eq. (4).

$$A^{a_t}_{B(H,t_1)}\left[i^{a_t}\,(h, t)\right] = a_t \tag{4}$$

where a_t must be marked as "inactive" in the mode corresponding to $B\,(h, t_1)$. Furthermore, the network always sets the state of the AM which creates $B\,(h, t_1)$ as "active". Note that we set all the nodes of AMs as "active" at the initial stage of the smart contract.

3.3.2. Genesis block selection

The next process of PoA is to select a genesis node from any two authorized blockchain branches. Since in this proposed PoA-based blockchain technology, we are not performing any energy competition to select the longest chain as a new node. Alternatively, we have introduced PoA based node as one authorized by more items.

To achieve this, we calculate the accumulated witness number (AWN) denoted as π for the node $B\,(h, t)$ using Eq. (5).

$$\pi_B\,(h, t) = \pi_{PA(B(h,t))} + \left\|A_{B(h,t)}\right\| \tag{5}$$

Initially, $\pi_{B_{genesis}} = 0$ because $\left\|A_{B(h,t)}\right\|$ calculates the number of AM nodes with "active" status related to $B\,(h, t)$. This could be considered as the greater number of AMs authorized by the creation of $B\,(h, t)$. Therefore, based on the PoA principles, the node with the larger AWN is considered as the genesis node. When the AWNs are matched, the branch with lowest length is selected. Later, the AWN is updated in the block header with the total score.

For example, consider two branches denoted by B_1 and B_2 with their latest nodes $B_1\,(h_1, t_1)$ and $B_2\,(h_2, t_2)$, respectively. These nodes first compute the values of the AWNs such as π_{B_1} and π_{B_2}. The network then chooses the genesis node based on the following conditions:

- Select B_1 as the genesis if $\pi_{B_1} > \pi_{B_2}$, or choose B_2 as the genesis if $\pi_{B_1} < \pi_{B_2}$.
- Suppose the value of $\pi_{B_1} = \pi_{B_2}$, select B_1 if $\$h_1 < \$h_2$, else choose B_2 if $\$h_1 > \$h_2$.
- Finally, if $\$h_1 = \$h_2$, keep the current node as genesis.

The proposed twin platform is used to monitor and manage IIoT devices. The platform serves as a central virtual control unit for static and dynamic sensor data by continuously receiving the updates on the static device information with the dynamic real-time data from the connected IoT sensors. The collected data is visualized in a digital three-dimensional model. The platform can also monitor and provide virtual data analytics to aid IIoT device optimization. We have proposed a PoA-based smart contract to enable a trust mechanism in the developed digital twin platform. The PoA-based node creation in the IIoT devices addresses the information of the digital sensors in the digital platform. In the 3D visualization, the sensor data can then be converted to the

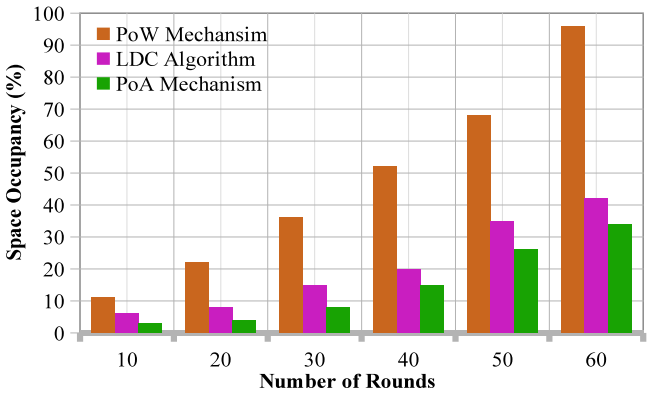

Fig. 4. Space occupancy percentage of different trust mechanisms.

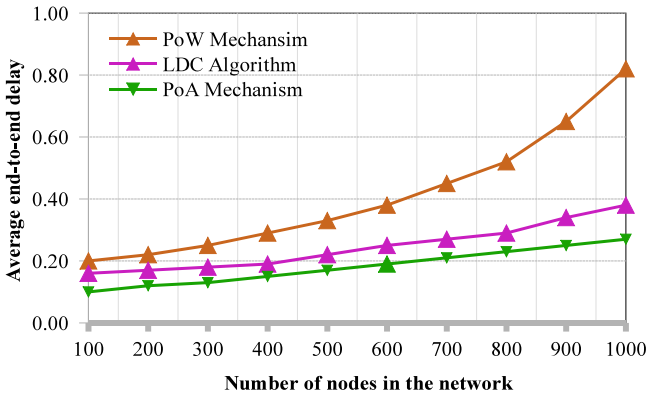

Fig. 5. Average end-to-end delay of different trust mechanisms.

actual physical address of the IoT devices, appropriate actual objects, and locations. To register their physical addresses in the smart contract, relevant sensors can be updated. The appropriate sensor data are then communicated to the blockchain after being retrieved from the digital twin platform.

4. Performance analysis

To evaluate the feasibility of the blockchain-based trust mechanism, a PoA-based consensus model for IIoT devices is proposed. To overcome the security issues of the public blockchain-based industries' automation process, digital twin and smart contracts are integrated. The implementation of the proposed PoA model is developed with Java 1.8 code in the Windows 11 PC with an i5 processor and 8 GB RAM. For the evaluation of our proposed PoA model, an alpha blockchain platform to implement and deploy authority-based smart contracts is considered. A decentralized PoA scheme is proposed to enhance the data privacy and security for the digital twin simulation process. The main reason to introduce Authority Masternodes (AM) based PoA trust mechanism for IIoT devices is to reduce overall transaction time and power consumption. PoA is a trust mechanism that has AM nodes and Deterministic Pseudo-Random Generation (DPRG) to select genesis nodes in the smart contracts. To simulate the digital twin data of the IIoT devices, we used a blockchain-based approach for collecting secure information. To develop smart contracts, we used a PoA-based accumulated witness number, which is a high number of authorized nodes.

To analyse the space occupancy of the proposed PoA mechanism, 1000 IIoT devices with random distribution were considered and the results obtained were then compared with results produced by existing methods such as a lightweight data consensus algorithm [46] and PoW mechanism [47]. The space occupancy increases concerning period and the percentages of the proposed mechanism were found to be higher than in other models. As the PoW methods require high energy, this will increase the rate of space storage. An LDC algorithm is implemented with the help of lightweight nodes, and this occupies smaller storage space. Compared with the other two mechanisms, our proposed model uses AM nodes to reduce the storage spaces. Fig. 4 demonstrates the proposed mechanism.

Fig. 5 Shows the average end-to-end delay in the networks related to the number of transmissions. The delay of the minimum number of nodes in the PoW-based network is very low when compared to a greater number of nodes. To overcome this drawback, our proposed PoA-based network reduces the end-to-end delay because of the deployment of AM nodes. Compared with the other two mechanisms, the proposed model provides a lesser delay in the network.

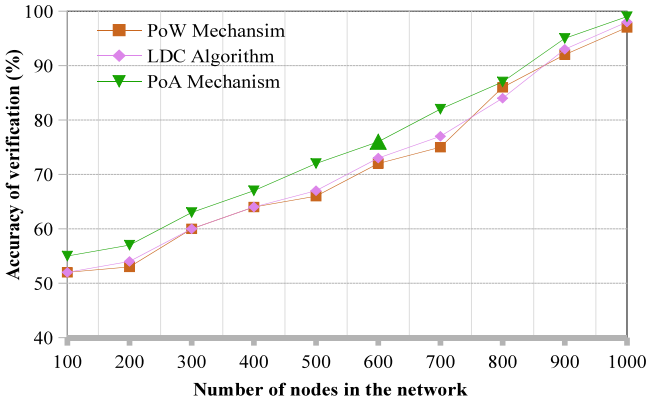

Fig. 6. Average verification percentage of different trust mechanisms.

We analysed the verification accuracy of the proposed mechanism with the help of several nodes present in the network. Fig. 6 shows the results of verification accuracy for different trust mechanisms. Generally, in the PoW mechanism, higher-length nodes take more time to verify and is more difficult to validate the nodes due to the network delay. In the case of lightweight data consensus algorithms, the difficulty level varies with different network delays. Compared with the existing mechanism, the proposed model was found to provide better verification accuracy.

Fig. 7 shows the power consumption result of the proposed trust mechanism and the other two existing models. As the number of IoT devices increases, PoW and lightweight algorithms may require more computing resources to validate the nodes. This will cause more power consumption in an exciting trust mechanism. The energy consumption result of the proposed PoA mechanism in validating genesis nodes has the advantage to reduce power consumption because it requires fewer computing resources.

Finally, the various performance analysis of the proposed blockchain-based digital twin empowered IIoT network shows trust mechanism increases data privacy and protection. Overall, the proposed trust mechanism scheme is most suitable for digital twin based IIoT applications to visualize systems digitally with high security.

5. Conclusion

In this paper, a blockchain-based trust mechanism through proof of authority for a digital twin-empowered IIoT network is

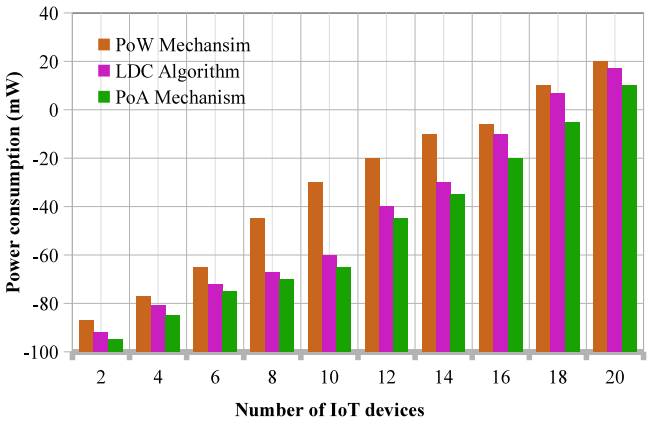

Fig. 7. Power consumption result of different trust mechanisms.

proposed. The proposed deterministic pseudo-random generation-based block creation will enhance data protection and system security. The status update of authority master nodes in the network provides high-quality service in real-time applications. Further, we generate a genesis node based on the accumulated witness number and number of master nodes to authorize it. Specifically, the PoA agreements-based blockchain model for digital twin IIoT network implemented with less energy consumption, lightweight, and highly secure architecture. We have addressed the benefits of PoA with digital twin technologies for IIoT applications. Finally, the simulation results show that the proposed integration of digital twin and blockchain provides better feasibility in terms of decentralization, scalability, and data privacy.

CRediT authorship contribution statement

Sasikumar A.: Conceptualization, Methodology, Writing – original draft, Formal analysis, Investigation, Visualization. **Subramaniyaswamy Vairavasundaram:** Conceptualization, Methodology, Writing – original draft, Formal analysis, Investigation, Resources. **Ketan Kotecha:** Formal analysis, Validation, Project administration, Funding acquisition. **Indragandhi V.:** Data curation, Visualization, Formal analysis, Investigation, Software, Supervision. **Logesh Ravi:** Resources, Formal analysis, Investigation, Software, Supervision. **Ganeshsree Selvachandran:** Writing – review & editing, Validation, Software. **Ajith Abraham:** Writing – review & editing, Validation, Project administration.

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.

Data availability

No data was used for the research described in the article.

Acknowledgements

The authors gratefully acknowledge the Science and Engineering Research Board (SERB), India, Department of Science & Technology, India for financial support through Mathematical Research Impact Centric Support (MATRICS) scheme (MTR/2019/000542). The authors also acknowledge SASTRA Deemed University, Thanjavur for extending infrastructural support to carry out this research work.

References

[1] S. Nahavandi, Industry 5.0 - human-centric solution, Sustainability 11 (16) (2019) 4371.
[2] P. López Martínez, R. Dintén, J.M. Drake, M. Zorrilla, A big data-centric architecture metamodel for industry 4.0, Future Gener. Comput. Syst. 125 (2021) 263–284.
[3] F. Longo, A. Padovano, S. Umbrello, Value-oriented and ethical technology engineering in industry 5.0: A human-centric perspective for the design of the factory of the future, Appl. Sci. 10 (12) (2020) 4182.
[4] F. Aslam, W. Aimin, M. Li, K. Ur Rehman, Innovation in the era of IoT and industry 5.0: Absolute innovation management (AIM) framework, Information 11 (2) (2020) 12.
[5] X. Li, H. Liu, W. Wang, Y. Zheng, H. Lv, Z. Lv, Big data analysis of the Internet of Things in the digital twins of smart city based on deep learning, Future Gener. Comput. Syst. (2022) 128, http://dx.doi.org/10.1016/j.future.2021.10.006.
[6] W. Luo, T. Hu, Y. Ye, C. Zhang, Y. Wei, A hybrid predictive maintenance approach for CNC machine tool driven by digital twin, Robot. Comput.-Integr. Manuf. 65 (2020) 101974.
[7] G.P. Agnusdei, V. Elia, M.G. Gnoni, A classification proposal of digital twin applications in the safety domain, Comput. Ind. Eng. 154 (2021) 107137.
[8] M. Liu, S. Fang, H. Dong, C. Xu, Review of digital twin about concepts, technologies, and industrial applications, J. Manuf. Syst. 58 (2021) 346–361.
[9] Y. Lu, X. Huang, K. Zhang, S. Maharjan, Y. Zhang, Low-latency federated learning and blockchain for edge association in digital twin empowered 6G networks, IEEE Trans. Ind. Inform. 17 (7) (2020) 5098–5107.
[10] B. Putz, M. Dietz, P. Empl, G. Pernul, EtherTwin: Blockchain-based secure digital twin information management, Inf. Process. Manage. 58 (1) (2021) 102425.
[11] C. Mandolla, A.M. Petruzzelli, G. Percoco, A. Urbinati, Building a digital twin for additive manufacturing through the exploitation of blockchain: A case analysis of the aircraft industry, Comput. Ind. 109 (2019) 134–152.
[12] M. Li, Z. Li, X. Huang, T. Qu, Blockchain-based digital twin sharing platform for reconfigurable socialized manufacturing resource integration, Int. J. Prod. Econ. 240 (2021) 108223.
[13] C. Zhang, G. Zhou, H. Li, Y. Cao, Manufacturing blockchain of things for the configuration of a data-and knowledge-driven digital twin manufacturing cell, IEEE Internet Things J. 7 (12) (2020) 11884–11894.
[14] X. Xu, Y. Lu, B. Vogel-Heuser, L. Wang, Industry 4.0 and industry 5.0—Inception, conception and perception, J. Manuf. Syst. 61 (2021) 530–535.
[15] P.K.R. Maddikunta, Q.V. Pham, B. Prabadevi, N. Deepa, K. Dev, T.R. Gadekallu, M. Liyanage, Industry 5.0: A survey on enabling technologies and potential applications, J. Ind. Inf. Integration (2021) 100257.
[16] F. Aslam, W. Aimin, M. Li, K. Ur Rehman, Innovation in the era of IoT and industry 5.0: Absolute innovation management (AIM) framework, Information 11 (2) (2020) 124.
[17] P. Fraga-Lamas, S.I. Lopes, T.M. Fernández-Caramés, Green IoT and edge AI as key technological enablers for a sustainable digital transition towards a smart circular economy: An industry 5.0 use case, Sensors 21 (17) (2021) 5745.
[18] M. Grieves, J. Vickers, Digital twin: Mitigating unpredictable, undesirable emergent behavior in complex systems, in: F.J. Kahlen, S. Flumerfelt, A. Alves (Eds.), Transdisciplinary Perspectives on Complex Systems, Springer, Cham, 2017, http://dx.doi.org/10.1007/978-3-319-38756-7_4.
[19] M. Grieves, Digital twin: Manufacturing excellence through virtual factory replication, White Paper 1 (2014) 1–7.
[20] N. Deepa, Q.-V. Pham, D.C. Nguyen, S. Bhattacharya, B. Prabadevi, T.R. Gadekallu, P.K.R. Maddikunta, F. Fang, P.N. Pathirana, A survey on blockchain for big data: Approaches, opportunities, and future directions, Future Gener. Comput. Syst. (2022) http://dx.doi.org/10.1016/J.FUTURE.2022.01.017.
[21] F. Tao, H. Zhang, A. Liu, A.Y.C. Nee, Digital twin in industry: State-of-the-art, IEEE Trans. Ind. Inform. 15 (4) (2019) 2405–2415.
[22] A. Rasheed, O. San, T. Kvamsdal, Digital twin: values, challenges and enablers from a modeling perspective, IEEE Access 8 (2020) 21980–22012.
[23] 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.
[24] M.J. Kaur, V.P. Mishra, P. Maheshwari, The convergence of digital twin, IoT, and machine learning: transforming data into action, Digit. Twin Technol. Smart Cities (2020) 3–17.

[25] Z. Jiang, Y. Guo, Z. Wang, Digital twin to improve the virtual-real integration of industrial IoT, J. Ind. Inf. Integration 22 (2021) 100196.
[26] V. Souza, R. Cruz, W. Silva, S. Lins, V. Lucena, A digital twin architecture based on the industrial internet of things technologies, in: 2019 IEEE International Conference on Consumer Electronics (ICCE), 2019, pp. 1-2.
[27] J. Sengupta, S. Ruj, S.D. Bit, A comprehensive survey on attacks, security issues and blockchain solutions for IoT and iIoT, J. Netw. Comput. Appl. 149 (2020) 102481.
[28] M. Liu, F.R. Yu, Y. Teng, V.C.M. Leung, M. Song, Performance optimization for blockchain-enabled industrial Internet of Things (iIoT) systems: A deep reinforcement learning approach, IEEE Trans. Ind. Inform. 15 (6) (2019) 3559–3570.
[29] Y. Jiao, P. Wang, D. Niyato, K. Suankaewmanee, Auction mechanisms in cloud/fog computing resource allocation for public blockchain networks, IEEE Trans. Parallel Distrib. Syst. 30 (9) (2019) 1975–1989.
[30] M. Dai, S. Zhang, H. Wang, S. Jin, A low storage room requirement framework for distributed ledger in blockchain, IEEE Access 6 (2018) 22970–22975.
[31] T.M. Fernández-Carames, P. Fraga-Lamas, Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks, IEEE Access 8 (2020) 21091–21116.
[32] C. Zhang, G. Zhou, H. Li, Y. Cao, Manufacturing blockchain of things for the configuration of a data-and knowledge-driven digital twin manufacturing cell, IEEE Internet Things J. 7 (12) (2020) 11884–11894.
[33] J. Leng, D. Yan, Q. Liu, K. Xu, J.L. Zhao, R. Shi, L. Wei, D. Zhang, X. Chen, ManuChain: Combining permissioned blockchain with a holistic optimization model as bi-level intelligence for smart manufacturing, IEEE Trans. Syst. Man Cybern. 50 (1) (2019) 182–192.
[34] J. Leng, P. Jiang, K. Xu, Q. Liu, J.L. Zhao, Y. Bian, R. Shi, Makerchain: A blockchain with chemical signature for self-organizing process in social manufacturing, J. Clean. Prod. 234 (2019) 767–778.
[35] C. Zhang, G. Zhou, H. Li, Y. Cao, Manufacturing blockchain of things for the configuration of a data-and knowledge-driven digital twin manufacturing cell, IEEE Int. Things J. 7 (2020) 11884–11894.
[36] T.T. Kuo, The anatomy of a distributed predictive modeling framework: Online learning, blockchain network, and consensus algorithm, JAMIA Open 3 (2) (2020) 201–208.
[37] F. Tao, Y. Zhang, Y. Cheng, J. Ren, D. Wang, Q. Qi, P. Li, Digital twin and blockchain enhanced smart manufacturing service collaboration and management, J. Manuf. Syst. 62 (2022) 903–914.
[38] J.E. Aguilar-Ramirez, J.A. Marmolejo-Saucedo, R. Rodriguez-Aguilar, Digital twins and blockchain: Empowering the supply chain, in: Proceedings of the International Conference on Intelligent Computing & Optimization, 2021, pp. 450-456.
[39] C. Wang, Z. Cai, Y. Li, Sustainable blockchain-based digital twin management architecture for IoT devices, IEEE Internet Things J. (2022) http://dx.doi.org/10.1109/JIOT.2022.3153653.
[40] S.S. Akash, M.S. Ferdous, A blockchain based system for healthcare digital twin, IEEE Access 10 (2022) 50523–50547.
[41] S. Suhail, R. Hussain, R. Jurdak, C.S. Hong, Trustworthy digital twins in the industrial internet of things with blockchain, IEEE Internet Comput. 26 (3) (2021) 58–67.
[42] L. Bai, M. Hu, M. Liu, J. Wang, BPIIoT: A light-weighted blockchain-based platform for industrial IoT, IEEE Access 7 (2019) 58381–58393.
[43] M. Aggarwal, M. Madhukar, IBM's Watson analytics for health care: A miracle made true, in: Cloud Computing Systems and Applications in Healthcare, 2017, pp. 117–134.
[44] Ericsson, Data integrity assurance user guide - implementation of service in predix user guide, 2016.
[45] K. Toyoda, K. Machi, Y. Ohtake, A.N. Zhang, Function-level bottleneck analysis of private proof-of-authority ethereum blockchain, IEEE Access 8 (2020) 141611-141621.
[46] W. Zhang, Z. Wu, G. Han, Y. Feng, L. Shu, LDC: A lightweight dada consensus algorithm based on the blockchain for the industrial internet of things for smart city applications, Future Gener. Comput. Syst. 108 (2020) 574–582.
[47] X. Xu, C. Pautasso, L. Zhu, V. Gramoli, The blockchain as a software connector, in: The 13th Working IEEE/IFIP Conference on Software Architecture, WICSA, IEEE, 2016, pp. 182–191.

Sasikumar A. is serving as an Assistant Professor in the Department of Electronics and Communication Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, India. He has received the B.E. degree in Electronics and Communication Engineering from Anna University, Tamil Nadu in 2011 and M.E. degree in VLSI Design from Anna University, Tamilnadu in 2013. He received his Ph.D. (Analog VLSI) at SASTRA, Thanjavur, India in 2020. He has more than 6 years of experience in the Research and Teaching. He has published more than 12 international journal papers and 5 international conferences papers. His research interest includes Analog Design Automation, Domain Specific Architecture, Digital VLSI, Swarm Intelligence, and Internet of Things.

Subramaniyaswamy Vairavasundaram is currently working as a Professor in the School of Computing, SASTRA Deemed University, India. In total, he has 18 years of experience in academia. He has received the BE degree in Computer Science and Engineering and M.Tech. degree in Information Technology from Bharathidasan University and Sathyabama University, India respectively. He received his Ph.D. degree from Anna University, India in 2013. He has published more than 100 papers in reputed international journals and conferences. His research interests include recommender systems, electric vehicle, big data analytics, and machine learning.

Ketan Kotecha is currently an Administrator and a Teacher of deep learning. His research interests include artificial intelligence, computer algorithms, machine learning, and deep learning. He has expertise and experience in cutting-edge research and projects in A.I. and deep learning for the last 25 years. He has published more than 100 widely in several excellent peer-reviewed journals on various topics ranging from cutting edge A.I., education policies, teaching–learning practices, and A.I. for all. He was a recipient of the two SPARC projects worth INR 166 lakhs from MHRD Government of India in A.I. in collaboration with Arizona State University, USA, and The University of Queensland, Australia. He was also a recipient of numerous prestigious awards, like the Erasmus+Faculty Mobility Grant to Poland, the DUO-India Professors Fellowship for research in responsible A.I. in collaboration with Brunel University, U.K., the LEAP Grant at Cambridge University, U.K., the UKIERI Grant with Aston University, U.K., and a Grant from the Royal Academy of Engineering, U.K., under Newton Bhabha Fund. He has published three patents and delivered keynote speeches at various national and international forums, including at the Machine Intelligence Laboratory, USA, IIT Bombay under the World Bank Project, the International Indian Science Festival organized by the Department of Science and Technology, Government of India, and many more. He is an Associate Editor of the IEEE Access journal.

Indragandhi V. completed B.E in Electrical and Electronics Engineering from Bharathidasan University in the year 2004. She received M.E in Power Electronics and Drives from Anna University and awarded Gold Medal for the achievement of university first rank. Subsequently, she is awarded with Doctor of Philosophy at Anna University, Chennai in the year 2015.At present she is serving as an Associate Professor in the School of Electrical Engineering, Vellore Institute of Technology, Vellore, Tamilnadu. She has been engaged in research work for the past 10 years in Power Electronics, Renewable Energy Systems and Computational Intelligence.

Logesh Ravi received his B.Tech. degree in Computer Science and Engineering and M.Tech. degree in Networking from Pondicherry University, India. He was conferred Ph.D. degree in Artificial Intelligence and Recommender Systems from the SASTRA (Deemed University), India. Currently, he is an associate professor at Department of Computer Science and Engineering, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of science and Technology, Avadi, Chennai, India. His research was funded and sponsored by Science and Engineering Research Board, Department of Science and Technology, New Delhi, India. He serves as Academic Coordinator, and he is Active Participant in Academic Administration and Research in Computing Sciences. He has published more than 100 papers in reputed international journals and conferences. His research interests include artificial intelligence, recommender systems, big data, machine learning, social computing, information retrieval and human–computer interaction. He also serves as a Guest Editor to many reputed international journals.

Ganeshsree Selvachandran received the B.Sc. (Hons.), M.Sc. and Ph.D. in mathematics from the National University of Malaysia (UKM), Bangi, Malaysia, in 2009, 2010 and 2013, respectively. She is currently a Professor with the Institute of Actuarial Science and Data Analytics and Faculty of Business and Management, UCSI University, Kuala Lumpur, Malaysia, and is a certified professional technologist with the Malaysia Board of Technologists. She has more than 10 years of experience in academia. She has authored more than 60 research articles in top-ranked international journals and has published papers in prominent journals including IEEE Transactions on Fuzzy Systems, Applied Soft Computing, Artificial Intelligence Review, Neural Computing and Applications, International Journal of Fuzzy Systems, Air Quality, Atmosphere and Health, Journal of Ambient Intelligence and Humanized Computing and IEEE Access. Her research interests include fuzzy mathematics, fuzzy computing, artificial intelligence, machine learning, deep learning, and evolutionary computing. She is also an active reviewer and has reviewed close to 100 journal articles for more than 30 WoS and Scopus indexed international journals.

Ajith Abraham is the Director of Machine Intelligence Research Labs (MIR Labs), a Not for-Profit Scientific Network for Innovation and Research Excellence connecting Industry and Academia. The Network with HQ in Seattle, USA has currently more than 1,000 scientific members from over 100 countries. As an Investigator/ Co-Investigator, he has won research grants worth over 100+ Million US$ from Australia, USA, EU, Italy, Czech Republic, France, Malaysia, and China. Dr. Abraham works in a multi-disciplinary environment involving machine intelligence, cyber–physical systems, Internet of things, network security, sensor networks, Web intelligence, Web services, data mining and applied to various real-world problems. In these areas he has authored/ coauthored more than 1,400+ research publications out of which there are 100+ books covering various aspects of Computer Science. One of his books was translated to Japanese and few other articles were translated to Russian and Chinese. About 1,100+ publications are indexed by Scopus and over 900+ are indexed by Thomson ISI Web of Science. Some of the articles are available in the ScienceDirect Top 25 hottest articles. He has 1,100+ co-authors originating from 40+ countries. Dr. Abraham has more than 38,000+ academic citations (h-index of 93 as per google scholar). He has given more than 100 plenary lectures and conference tutorials (in 20+ countries). For his research, he has won seven best paper awards at prestigious international conferences held in Belgium, Canada Bahrain, Czech Republic, China, and India. Since 2008, Dr. Abraham is the Chair of IEEE Systems Man and Cybernetics Society Technical Committee on Soft Computing (which has over 200+ members) and served as a Distinguished Lecturer of IEEE Computer Society representing Europe (2011–2013). Currently Dr. Abraham is the editor-in-chief of Engineering Applications of Artificial Intelligence (EAAI) and serves/served the editorial board of over 15 International Journals indexed by Thomson ISI. He is actively involved in the organization of several academic conferences, and some of them are now annual events. Dr. Abraham received Ph.D. degree in Computer Science from Monash University, Melbourne, Australia (2001) and a Master of Science Degree from Nanyang Technological University, Singapore (1998). More information on Prof. Abraham can be found at: http://www.softcomputing.net/.