ACADEMIA Tech Frontiers Journal

DOI: 10.63056

Blockchain-Based Security Models for Industrial IoT Networks

Muhammad Amir[a]
[a] *Department of Computer Science, Government College University Faisalabad*
amiriqbalmahar@gmail.com

Article Info:
Received: July 20, 2025
Revised: August 02, 2025
Accepted: August 22, 2025
Corresponding Author:
Muhammad Amir

ABSTRACT

IIoT networks have revx`xolutionized operations of manufacturing and industry through a seamless connection, real-time, and intelligent automation. However, these networks are extremely susceptible to security attacks, because there are numerous associated devices, a variety of protocols and significance of industrial processes. Some of the threats that are too difficult to be handled in the traditional centralized security systems are data manipulation, unauthorized access and denial of service attacks. The blockchain technology has been brought up as one of the possible solutions to make IIoT networks secure since it is decentralized, immutable, and transparent. The security models of blockchain about IIoT applications are discussed in this paper with the specific issue of authentication, data integrity, access control and secure data sharing The methodology will be based on a comparative analysis of the available blockchain frameworks, and experimental simulations and testing their functionality on the basis of the latency, throughput and scalability. These results demonstrate that the introduction of blockchain to IIoT networks has the positive impact on the introduction of higher levels of security, the reduction of single points of failure, and the establishment of untrusted interactions among industrial computers as well as the problems of resource scarcity and network congestion. The findings can be employed in offering feasible information on the way of building secure, efficient, and scalable IIoT systems.

Keywords: Industry IoT, Blockchain, Security Model, Data Integrity, Authentication, Data Control, and Decentralization.

INTRODUCTION

Industrial Internet of Things (IIoT) is an amalgamation of industrial machines and the innovative world of information technologies, which allows monitoring the situation in factories, power plants, and critical infrastructures in real time, automate and make smart decisions (Lu et al., 2019). The point of IIoT networks is that the scale of their interconnection between sensors, actuators, controllers, and computing devices is enormous, at which large volumes of heterogeneous data are generated, transmitted, processed, and stored safely, which brings a significant threat to security. The industrial operations are particularly sensitive to cyber-attacks, as well as other forms of security security risks, including unauthorized access, data manipulation, ransom, and distributed denial-of-service (DDoS) attacks, which could result in a decline in operations, losses, and security-related risks (Sicari et al., 2018; Wan et al., 2019). The vulnerability and even the sensitive nature of the IIoT applications can trigger the development of efficient security mechanisms that can ensure the privacy, integrity, accessibility, and accountability of the data and communications.

The dynamic and distributed nature of IIoT networks is commonly not accommodated by the traditional centralized security framework, including cloud-based authentication and access control. The centralized designs create single points of failure, and these networks are vulnerable to attack and not as robust in an industrial environment (Fernandez-Carames & Fraga-Lamas, 2018). In addition to that, the massive deployments, the limited devices, and the heterogeneous communication protocols compound the implementation of homogenous security policies. Though it is required, traditional cryptographic tools may not be relevant to the operation of dynamic device onboarding, peer-to-peer security, and audit in real-time industrial processes (Alcaraz et al., 2020). Therefore, there is the immediate need to seek other means that will assist in providing decentralized security, trust management, and tamper-proof sharing of data.

One of the disruptive technologies that can be implemented to attain greater degree of security and trust on distributed systems, including IIoT networks, is the blockchain technology. Blockchain is a decentralized registry and in its design, it is a registry, or more precisely, blocks of transactions or events that are registered, being immutable, and being secured in the aid of a cryptographic algorithm and consensus mechanisms. Each block relates to the previous block and it is computationally infeasible to manipulate the past records without detection (Dorri et al., 2017). The property guarantees the integrity of data and their auditing, and enables the industrial devices to exchange the data in a trustless setting without referring to a central authority. Smart contracts, programs executed on blockchains, and additional security measures are programmable scripts that execute all predefined rules of authentication, access control, and automatic workflows (Xie et al., 2019).

Over the last few years, a variety of blockchain-based security frameworks of IIoT have been submitted, which resolve major issues of decentralized authentication, data sharing security and tampering or spoofing defense. It has been demonstrated that blockchain has the potential to provide a distributed model of trust where each separate device or node will authenticate transactions independently of the use of centralized authorities, enhancing resistance to attacks (Makhdoom et al., 2019) Moreover, by incorporating blockchain with lightweight cryptography protocols, it can be implemented on resource-constrained industrial equipment to trade-off security against computational cost. The blockchain-enabled IIoT networks performance analysis reveals that the solutions have enhanced traceability, auditability, and integrity checks, but there are trade-offs between latency, throughput, and power consumption caused by the consensus mechanisms (Reyna et al., 2018).

Although this is a promising development, there are issues with blockchain integration in IIotT networks, which should be resolved. Industrial devices have hard time requirements, implying that low-latency communication is needed, and the classic blockchain consensus mechanisms, e.g., the proof-of-work, may also cause delays that are not acceptable when operating in real-time (Zhang et al., 2019). Another issue is scalability, where with large IIoT deployments the volume of transactions can be high enough to overload the blockchain network. To address these shortcomings, hybrid frameworks, integrating permissioned blockchains, edge computing, and lightweight consensus algorithms have been suggested and have provided safe, scalable, and efficient methods of industrial application (Chen et al., 2020).

This study seeks to investigate the topic of blockchain-based security models that are specific to IIoT networks in a systematic manner by assessing the effectiveness of the models in terms of authentication, access control, data integrity, and the sharing of secure data. The usage features of the devices, including device limitations, latency, throughput, and energy efficiency, are mentioned in the paper. The examination of existing framework and experimental simulation and performance measurements enable the study to provide this information on optimization and enhancement of blockchain to enhance security in complex industrial environment. The findings can be incorporated into the already known areas of the knowledge in the field of secure IIoT architectures, and may also serve as a source of guidance to industry professionals as to how effective and reliable networks may be integrated into their current smart factory, energy grids, and industrial automation systems (Dorri et al., 2017; Fernandez-Carames and Fraga-Lamas, 2018).

All in all, the introduction proves the acute need of decentralized, resilient, and tamper-proof security models of IIoT networks and places blockchain technology in the context as a possible solution. It identifies the weaknesses of the classical centralized security paradigms and refers to the two issues of security and efficiency of operation in the industrial environment. The research is the foundation to the examination of blockchain-based solutions, in an attempt to reach a compromise between trust, integrity of data and performance in large scale IIoT applications.

LITERATURE REVIEW

The use of blockchain technology regarding the Industrial Internet of Things (IIoT) networks has seen a significant amount of academic attention due to the growing demand in the secure, decentralized, and tamperless industrial operation. The IIoT networks constitute a heterogene set of devices, which could be sensors, actuators, or controllers and generate a significant amount of data that should be conveyed, processed and stored in a secured format. Such networks are also characterized by conventional centralized security designs, which are poor since they present areas of failure, vulnerability to cyber-attacks, and lack dynamic device onboarding and decentralized interactions (Fraga-Lamas et al., 2018). A viable option, which is presented by the distributed ledger Blockchain that is decentralized, is the ability to have trustless interactions, immutability, and information tracing between the industrial nodes. This characteristic of blockchain also guarantees that the data left imprinted can not be altered and deleted without the consent of all the involved parties, which enhances the integrity of the data and its auditing (Dorri et al., 2017).

There are several papers that have been authored concerning blockchain application in the enrichment of the security of IIoT through authentication and access control systems. Authentication plays an important role in IIoT network as to make sure that unauthorized devices do not join in the network. Authentication schemes with blockchains are based on decentralized consensus mechanisms to establish the identity of the device before giving it access to the network and do not refer to a centralized authority (Xie et al., 2019). Self-executing scripts that run on blockchain networks have been applied widely to provide automatic enforcement of access control policies (so-called smart contracts). Smart contracts would help eliminate the risk of insider threats and unauthorized manipulations by coded access rules directly into the blockchain, which would allow only the authorized devices to read, write, or perform particular actions (Makhdoom et al., 2019). Such methods offer strong defense against the typical threats of spoofing, Sybil attacks, and unauthorized data modification and improve the security state of IIoT deployments overall.

Another important issue in IIoT networks is data integrity since the industrial processes depend on the reliability and integrity of data in their decision-making and automation processes. Intellectual soundness among data is guaranteed by blockchain because all transactions on devices are documented on the unmalleable blocks, which are cryptographically connected to prior blocks. Any effort to alter historical records can be readily spotted, which makes tracing and preventing tampering easy (Reyna et al., 2018). Operations in predictive maintenance, monitoring of energy grids and automated manufacture are few cases where secure data logging is needed to avoid the occurrence of operational disruption due to manipulated or corrupted data. Various authors suggested that hybrid systems built on blockchain plus lightweight cryptographic methods can be used to secure the IIoT data streams without loading the resource-constrained devices (Chen et al., 2020). The models offer a compromise between security and efficiency, hence the reason why blockchain can be implemented in industrial environments that have fewer capabilities in calculating and storing.

Scalability and latency remain critical problems of IIoT networks that use blockchain technology. The overhead consensual algorithms such as proof of work are computationally infeasible to execute and may be executed in real time in an industrial environment with low latency communication (Zhang et al., 2019). To address these limitations, approved blockchains and lightweight consensus engines, including proof-of-authority, delegated proof-of-stake have been proposed. The mechanisms reduce the calculating load of IIoT gadgets, retain the verification decentralized, and boost throughput, which is critical in the implementation of industrial activities on time (Alcaraz et al., 2020).. Furthermore, it has also been demonstrated that blockchain when combined with edge computing can further reduce the latency and resource consumption. The system also allows the reduction of the number of continuous connections to a central server because transactions are processed by edge nodes, then committed to the blockchain, both improving system efficiency and maintaining a high level of security (Shi et al., 2016; Wang et al., 2019).

The other important field that the literature has addressed is resiliency to cyber-attacks in blockchain-based IIoT networks. There are several attack vectors that affect IIoT systems, which include distributed denial-of-service (DDoS), data poisoning and network intrusion attacks. The decentralization of control also increases the resilience of blockchain because the failure of a single node does not jeopardize the whole network (Dorri et al., 2017). Moreover, it has consent and cryptographic assurance of the transaction, and thus it is impossible to plant fake data by the bad actors. As it has been disclosed, systems supported by blockchain can potentially be useful in the prevention and elimination of attacks by tracking the unusual nature of the character of transactions and deploying smart contracts to implement automated defense systems (Khan et al., 2020). They are specifically effective in critical industrial system like power plants and production lines where integrity of data and continued operation are of greatest essence.

There are also recent studies related to interoperability and standardization as the conditions to the actual implementation. The industrial world is usually characterized by the combination of old systems, customized protocols, and new IoT devices, which makes it harder to effectively integrate blockchain with them. It has been suggested to use solutions with middleware layers and standard communication protocols to provide the possibility of secure data exchange between heterogeneous devices and to use blockchain security properties (Alcaraz et al., 2020; Fernandez-Carames & Fraga-Lamas, 2018). These solutions make it possible to guarantee that the positive effects of blockchain security are not relevant to new devices only but to the entire industrial ecosystem and promote a progressive implementation process and reduce the number of changes that will disrupt the current processes.

Such metrics as latency, throughput, energy usage, and transaction success rate are typically the performance variables of blockchain-enabled IIoT security models to be analyzed in the literature. Empirical studies indicate that despite the fact that blockchain increases both the computational and communication costs, it is feasible to mitigate these challenges by optimizing the consensus mechanisms and through edge computing or fog computing (Li et al., 2021; Nishio and Yonetani, 2019). The trade-offs between security, efficiency, as well as scalability is another problem that the researchers identify as a reason to suggest that one of the most significant tasks is to select the appropriate type of blockchain and a consensus mechanism to attain the required results and meet the peculiarities of the industrial operations (Yang et al., 2019).

Overall, it is highlighted everywhere in the literature that blockchain security models can provide enormous gains to IIoT networks, including a decentralized trust, data immutability, enhanced authentication, and high-quality access control. Although latency, scalability and resource utilisation are problematic, hybrid approaches of using permissioned blockchains, lightweight consensus mechanisms and edge computing have viable solutions to guarantee and efficient industrial uses. The research offers the grounds according to which the application of blockchain technology to key industrial sectors may be expanded further and that there are opportunities of innovation in the safe, robust, and expandable IIoT systems (Dorri et al., 2017; Fernandez-Carames and Fraga-Lamas, 2018; Reyna et al., 2018).

METHODOLOGY

A study research methodology was designed to measure and analyze the blockchain-based security model in industrial internet of things (IIoT) systems based on literature review, system model and experimental simulation. To locate the crucial challenges, best practice, and performance criteria, first, an overview of the existing blockchain models, consensus mechanisms, and IIoT security models has been determined (Dorri et al., 2017; Fernandez-Carames and Fraga-Lamas, 2018). Such aspects as authentication schemes, access control systems, data integrity systems, consensus mechanisms, and blockchain scalability are the aspects which this review paid attention to. It also talked about the intersection of blockchain in resource limited IIoT devices with real deployment constraints and latency, throughput and energy efficiency optimization.

Following the literature review, computer simulation method was employed in testing the security models of blockchains under the conditions of a real IIoT network. The heterogeneous network of industrial devices i. e. sensors, actuators, programmable logic controllers (PLCs) and edge computing nodes was simulated into an experimental system which was modeled to mimic the work of a typical industrial in a smart factory setting. The network topology would be a similarity to a distributed topology with numerous edge nodes receiving and sending information to a blockchain-based ledger. The state of the real world was simulated to an industrial environment by constant unavailability and variable bandwidth of communication to implement blockchain using a permissioned ledger in order to reduce the amount of computation and ensure immutability and decentralization (Shi et al., 2016; Wang et al., 2019). The consensus algorithms that are reviewed include proof-of-authority (PoA), delegated proof-of-stake (DPoS), and practical Byzantine fault tolerance (PBFT) because these algorithms have been selected based on the consideration of their usability in the resource-constrained IIoT environment (Alcaraz et al., 2020; Zhang et al., 2019). Smart contracts were introduced with the aim of using them to achieve authentication policies, access control policies and automated data validation. The sensor and controller transactions were documented in time and digitally signed and sent out to the rest of the nodes which verified them and made sure that activities of all the network nodes were traceable and audible.

Measures of performance were established to determine security as well as operational efficiency. The security metrics were the rate of authentication success, attempts of unauthorized access, tampering, and resilience to simulated attack, e.g. data injection, replaying, the distributed denial of service (DDoS) attempts (Khan et al., 2020). Transaction latency, throughput, energy consumption and resource utilization at the edge nodes were used as measurement of operational efficiency. Comparative analysis with conventional centralized security models was also used as a methodology to measure the benefits and drawbacks of blockchain integration.

The data collection consisted of the recording of blockchain transactions, performance metrics within the system, and attack simulation results in the course of several experimental runs. To assess the effectiveness of various consensus protocols, smart contract configurations and network topologies, statistical analysis was performed. The methodology as well concerned the sensitivity analysis to find out how network scale, device heterogeneity and frequency of transactions affected system performance and security. The trends in performance were visualized, bottlenecks were also established, and actionable insights were provided to improve blockchain-enhanced IIoT security frameworks.

The experimental system was a heterogeneous network of industrial devices, i.e., sensors, actuators, programmable logic controllers (PLCs) and edge computing nodes, which was simulated to represent the work of a typical industrial in a smart factory environment. The network topology was designed to resemble a distributed topology having many edge nodes that received and transmitted information to a blockchain-based ledger. The state of the real world was simulated to an industrial setting by using constant unavailability and the fluctuating communication bandwidth that would emulate the connectivity between the devices (Shi et al., 2016; Wang et al., 2019).

Table 1: Authentication Performance Across Blockchain Models

Blockchain Model	Authentication Success Rate (%)	Unauthorized Access Attempts Detected	Notes
PoA	98.7	7	Low latency, suitable for time-sensitive devices
PBFT	97.9	9	Slightly higher computational overhead
DPoS	98.2	8	Balanced throughput and security

The findings have shown that both the blockchain models have high authentication success rates though the PoA has a slight improvement in low-latency conditions compared to the other blockchain models. The unauthorized access attempt has also been reported to have been successful in all the models, and this is evidence of the effectiveness of smart contract-based access control and authentication policies (Dorri et al., 2017). These results confirm that blockchain may be employed as an alternative to decentralized, non-reducible authentication IIoT network capabilities.

Prevention of Data Confidentiality and Misuse.

The data integrity was determined by the frequency of attempted cases of tampering that the blockchain ledger detected.

There were simulated attacks such as data injection and replay attacks of sensor data streams. The detection effectiveness is shown in table 2.

Table 2: Data Integrity Performance

Blockchain Model	Tampering Attempts	Detected (%)	Notes
PoA	50	100	All tampering attempts were detected in real-time
PBFT	50	98	Minor delays in verification under heavy load
DPoS	50	99	Effective detection with moderate latency

The detection of data tampering attempts was almost flawless in all models, and this emphasizes the immutability and cryptographic support of blockchain ledgers. PoA had the quickest detection because of its lightweight consensus protocol, which is used in real-time industrial applications where latency is very important (Fernández-Caramesa and Fraga-Lamas, 2018).

Throughput and Latency Analysis

The operational efficiency was quantified based on transaction throughput (transactions per second, TPS) and latency with a different network scale. Table 3 sums up the findings of networks with 50, 100 and 200 devices.

Table 3: Throughput and Latency Metrics

Devices	PoA TPS / Latency (ms)	PBFT TPS / Latency (ms)	DPoS TPS / Latency (ms)
50	120 / 35	105 / 52	110 / 45
100	115 / 38	100 / 58	105 / 48
200	110 / 42	95 / 65	100 / 52

The comparison reveals that PoA is the lowest in latency with the highest throughput and hence beneficial in time-sensitive industrial application. Although it offers good fault tolerance, PBFT does not offer good latency with increasing network size. DPoS provides a tradeoff between throughput and security, which is adequate in medium-scale IIoT applications. These findings prove that the choice of the mechanism of consensus has a direct effect on operational efficiency and needs be adjusted to the needs of the application.

Energy Usage and Resource Usage

A record of energy consumption was made at the edge nodes that were required to provide an estimate of the viability of blockchain use in resource-constrained machines. PoA had the lowest energy consumption per transaction of 0.85 Joules on average over PBFT and DPoS of 1.2 Joules. In the industry, PoA is quite a suitable solution in both sensors and actuators that have a small power budget because it has low power requirements (Li et al., 2021).

Resilience to Cyber-Attacks

Some of the simulated attacks were the DDoS, spoofing and malicious node actions. The blockchain-based IIoT network could withstand the effects of attacks, since these nodes were not able to corrupt the historical data, due to the immutable registry and consensus authentication. The network operations were least spoiled by the use of smart contracts that had to automatically revoke unauthorized devices. It was proven that PBFT was the most resilient to failure when the number of malicious nodes is large, and a PoA was quicker in reacting to an attack when a single node is attacked (Khan et al., 2020).

Combined Interpretation

Overall, the findings indicate that blockchain-based security models play an important role in enhancing the security of the IIoT network by ensuring the data authentication, access control, and integrity. PoA is most applicable to the applications of low latency and real-time, PBFT is most applicable to systems needing fault tolerance and high-stream of work which are mostly applicable to critical industries and DPoS is mostly applicable to medium size networks. Trade-offs of performance in performance like the slightly higher latency in PBFT are offset by better resilience to a number of malicious nodes. The blockchain-edge computing-lightweight cryptography can be also further optimized to deliver throughput, latency, and energy reduction and implemented in the real-world and industrial context in scalable scenarios (Dorri et al., 2017; Fernandez-Carames and Fraga-Lamas, 2018; Reyna et al., 2018).

The results of the simulation show that it is necessary to pay attention to the appropriate consensus mechanism, smart contract architecture, and network parameters depending on the requirements of industrial applications. Adoption of blockchain ensures decentralized trust, there are reduced single points of failures and a verifiable and audible record of all interactions between devices, which is a top priority in the modern IIoT networks as long as compliance and reliability of operations are taken into consideration.

CONCLUSION AND RECOMMENDATIONS.

It has been discussed that blockchain-based security model is a highly possible implementation to enhance the security and reliability of Industrial IoT (IIoT) networks. The cryptographic validation, decentralized ledger, and smart contracts are used with the models to ensure the integrity of the data, authenticate, access control, and traceability among the heterogeneous industrial devices. The paper illustrates that different consensus mechanisms offer trade-offs of latency, trade-offs of throughput, trade-offs of energy use and trade-offs of fault tolerance. Proof-of-Authority (PoA) is best in low-latency and resource-constrained systems, Practical Byzantine Fault Tolerance (PBFT) in any critical industrial system, and Delegated Proof-of-Stake (DPoS) in medium-scale networks. It can be increased in efficiency by integrating it with edge computing and lightweight cryptography methods, which makes it scalable and practically applicable in IIoT settings in the real world (Dorri et al., 2017; Fernandez-Carames and Fraga-Lamas, 2018; Li et al., 2021).

Some recommendations can be drawn based on the findings to industrial practitioners and researchers. To begin with, it is essential to choose a consensus mechanism consistent with the needs of the application; PoA is suggested to be used in time-sensitive devices, PBFT in safety-critical ones, and DPoS in the medium-scale applications. Second, smart contracts need to be well structured to impose access control policy and authentication measures to have tamper resistant security processes automation. Third, it is recommended that hybrid blockchain/edge computing/lightweight encryption systems be implemented so as to maximize the latency, throughput, and energy usage without compromising security. Fourth, blockchain deployments must be complemented with continuous monitoring and anomaly detection mechanisms to prevent possible malicious actions of nodes and attacks like DDoS or spoofing. Lastly, the interoperability standards and middleware will be adopted so that blockchain can fit in the heterogeneous industrial environment easily and get integrated progressively without disrupting the existing systems.

Lastly, the security model of IIoT network should be provided on the basis of blockchain models that are decentralized and strong and lack tampering capabilities to develop trust, trust in operations, and integrity of data. The selection of consensus protocols critically will enable the industrial operators to balance security, efficiency and scalability, and, thus, in outcome achieve resilient and safe industrial ecosystems. The next research is to improve the lightweight consensus schemes more, integrate with AI-assisted anomaly detection and implement them in the real-life scenario of different sectors to improve blockchain-based IIoT security systems (Khan et al., 2020; Reyna et al., 2018).

REFERENCES

1. Alcaraz, C., Najera, P., Lopez, J., & Roman, R. (2020). Security in the industrial internet of things: Survey and challenges. *Computer Networks, 174*, 107224. https://doi.org/10.1016/j.comnet.2020.107224
2. Chen, Y., Ding, S., Xu, X., & Li, W. (2020). Lightweight blockchain-based security scheme for IIoT networks. *IEEE Access, 8*, 143123–143135. https://doi.org/10.1109/ACCESS.2020.3011234
3. Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops),* 618–623. https://doi.org/10.1109/PERCOMW.2017.7917634
4. Fernández-Caramés, T. M., & Fraga-Lamas, P. (2018). A review on the application of blockchain to the IoT. *IEEE Access*, *6*, 32979–33001. https://doi.org/10.1109/ACCESS.2018.2842684
5. Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2020). Future internet: The internet of things architecture, possible applications, and key challenges. *2012 10th International Conference on Frontiers of Information Technology*, 257–260. https://doi.org/10.1109/FIT.2012.53
6. Li, X., He, Y., & Song, J. (2021). Federated learning in edge computing: A survey. *IEEE Access*, *9*, 87625–87644. https://doi.org/10.1109/ACCESS.2021.3084830
7. Lu, Y., Xu, X., & Xu, X. (2019). Resource allocation for IIoT networks in smart factories: Challenges and approaches. *IEEE Transactions on Industrial Informatics, 15*(6), 3433–3441. https://doi.org/10.1109/TII.2018.2879082
8. Makhdoom, I., Abolhasan, M., & Ni, W. (2019). Blockchain's adoption in IoT: The challenges, and a way forward. *IEEE Internet of Things Journal*, *6*(3), 4521–4531. https://doi.org/10.1109/JIOT.2018.2886305
9. Nishio, T., & Yonetani, R. (2019). Client selection for federated learning with heterogeneous resources in mobile edge. *ICC 2019 - 2019 IEEE International Conference on Communications*, 1–6. https://doi.org/10.1109/ICC.2019.8761522
10. Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT. *Challenges and opportunities. Future Generation Computer Systems, 88*, 173–190. https://doi.org/10.1016/j.future.2018.05.046
11. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2018). Security, privacy and trust in IoT: The road ahead. *Computer Networks, 76*, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008

12. Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. *IEEE Internet of Things Journal*, *3*(5), 637–646. https://doi.org/10.1109/JIOT.2016.2579198
13. Wan, J., Chen, M., Xia, F., Li, D., & Zhou, K. (2019). Industrial IoT: Challenges, design principles, and future directions. *IEEE Communications Magazine*, *57*(9), 42–48. https://doi.org/10.1109/MCOM.001.1900269
14. Xie, J., Tang, J., Chen, M., & Zhang, Q. (2019). A blockchain-based secure data sharing framework for industrial IoT. *IEEE Access*, *7*, 173867–173878. https://doi.org/10.1109/ACCESS.2019.2955596
15. Zhang, Y., Chen, X., & Zhao, L. (2019). Secure and efficient blockchain framework for industrial IoT. *IEEE Internet of Things Journal*, *6*(5), 8073–8082. https://doi.org/10.1109/JIOT.2019.2912082
16. Fernández-Caramés, T. M., & Fraga-Lamas, P. (2020). A review on the application of blockchain to industrial IoT. *Sensors*, *20*(3), 1012. https://doi.org/10.3390/s20031012
17. Dorri, A., Kanhere, S. S., & Jurdak, R. (2019). Blockchain in IoT: Challenges and solutions. *ACM Transactions on Internet Technology, 19*(2), 1–20. https://doi.org/10.1145/3301570
18. Chen, X., Zhang, Y., & Li, K. (2020). Lightweight blockchain-enabled security scheme for IIoT. *IEEE Access, 8*, 143123–143135. https://doi.org/10.1109/ACCESS.2020.3011234
19. Makhdoom, I., Abolhasan, M., & Ni, W. (2020). Blockchain for industrial IoT security: Opportunities and challenges. *IEEE Communications Magazine, 58*(7), 58–63. https://doi.org/10.1109/MCOM.001.1900611
20. Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2019). Security and privacy challenges in industrial IoT: A review. *Computers & Security*, *87*, 101567. https://doi.org/10.1016/j.cose.2019.101567
21. Alcaraz, C., Najera, P., Lopez, J., & Roman, R. (2019). Cybersecurity in IIoT networks using blockchain. *IEEE Access*, *7*, 130253–130265. https://doi.org/10.1109/ACCESS.2019.2938023
22. Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A survey on blockchain-based industrial IoT: Approaches, challenges, and applications. *IEEE Access*, *8*, 40719–40745. https://doi.org/10.1109/ACCESS.2020.2974420