Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 191 (2021) 176–183

Procedia Computer Science

www.elsevier.com/locate/procedia

The 18th International Conference on Mobile Systems and Pervasive Computing (MobiSPC)
August 9-12, 2021, Leuven, Belgium

Privacy, Security and Policies: A Review of Problems and Solutions with Blockchain-Based Internet of Things Applications in Manufacturing Industry

Kamalendu Pal[a,*]

[a]*City, University of London, Northampton Square, London EC1V 0HB*

Abstract

Internet of Things (IoT) aims to simplify the collection of the distributed data in a global manufacturing business, sharing and processing of information and knowledge across many collaborating partners using appropriate information system architecture. As with the IoT, convergence with blockchain technology that processes data, privacy and security-related issues, and data policies (e.g., regulatory compliance) may apply to data and software artefacts. Besides, blockchain technology could contribute to the more intelligent and flexible handling of transactional data through appropriate convergence with IoT technology in supporting data integration and processing. This paper examines this hybrid architecture's privacy, security, and policy-related issues to appreciate the convergence and understand the integration of IoT and blockchain technology. This paper primarily identifies common trends focusing on relevant topics in blockchain-based IoT technology research and by highlighting the need to explore security issues further – for example, data privacy challenges in the manufacturing industry.

Keywords: Internet of Things; Global Manufacturing; Blockchain Technology; Security; Data Privacy; Policy Issues

* Corresponding author. Tel.: +44-208-399-7430; fax: +0-000-000-0000 .
E-mail address: k.pal@city.ac.uk

10.1016/j.procs.2021.07.022

1. Introduction

The modern manufacturing industry and its supply chain represent a leap forward from more traditional automation to fully connected and flexible manufacturing operations. This flexible system can use a constant stream of data from connected operations and production systems to learn and adapt to new demands. It becomes a trend impacting business and economic growth; many networked machines are used increasingly to carry out manufacturing operations. These machines may carry out the same or different functions or tasks, and some machines rely heavily on the output from other machines (known as a '*pipelined product line'*). The connection between networked machines may also be configured dynamically to increase flexibility and adaptation to customized tasks. As a result, the smart synergy of networked machines is critical to improving the performance of modern manufacturing systems [10] [12].

One critical enabling technology for modern manufacturing is the Internet of Things (IoT), which is forming a worldwide information network composed of large numbers of interconnected '*Things*'. Here, manufacturing '*Things*' may include materials, material handling equipment, robots, machines, products, human operators, sensors, actuators, controllers, to name but a few. The internet-based IoT infrastructure ushers an enormous opportunity to connect manufacturing '*Things*', applications, services to achieve effective digital connectivity of the entire manufacturing enterprise. This integration can be extended from enterprise resource planning (ERP) to supply chain management (SCM) to manufacturing execution system (MES) to process control systems (PCS). However, the rapid growth of large-scale IoT sensing leads to the manifestation of big data stored locally or in data repositories distributed over the cloud (i.e., Service-Oriented Computing - SOC) [14]. Appreciating the full potential of big data for modern manufacturing requires fundamentally new methodologies for large-scale IoT data management, information processing, and manufacturing process control architecture [9].

Moreover, global manufacturing networks are becoming complicated due to a growing need for inter-organizational and intra-organizational connectedness that enabled by advances in modern technologies (e.g., Radio Frequency Identification (RFID), IoT, Blockchain, SOC, Big Data Analytics) [13] and tightly coupled business processes. The manufacturing business networks use information systems to monitor operational activities in a nearly real-time situation. Therefore, digitalization of business activities attracts attention from manufacturing network management purpose, improves communication, collaborates, and enhances trust within business partners due to real-time information sharing and better business process integration. However, the above new technologies come with different types of disruptions to operations and ultimate productivity. For example, some operational disruptions are due to privacy, security-related threats that hinder the safety of goods, services, and customers' trust to do business with the affected manufacturing enterprises.

As a global network context, the IoT system integrates different heterogeneous objects and sensors, which surround manufacturing operations and facilitates the information exchange within the business stakeholders (also known as nodes in networking term). However, with the rapid enlargement of the data communication network scale and the smart evolution of hardware technologies, typical standalone IoT-based applications may no longer satisfy the advanced need for efficiency and security in the high degree of heterogeneity of hardware devices and their complex data formats. Firstly, burdensome connectivity and maintenance costs brought by centralized architecture result in its low scalability. Secondly, centralized systems are more vulnerable to adversaries' targeted attacks under network expansion [9].

Intuitively, a decentralized approach based on blockchain technology may solve the above problems in a typical centralized IoT-based information system. Mainly, the above justification is for three reasons. Firstly, an autonomous decentralized information system is feasible for trusted business partners to join the network, improving the business task-processing ability independently. Secondly, multiparty coordination enhances nodes' state consistency that information system crashes are avoidable due to single-point failure. Thirdly, nodes could synchronize the whole information system state only by coping with the blockchain ledger to minimize the

computation related activities and improve storage load. Besides, blockchain-based IoT architecture for manufacturing information systems attracted researchers' attention [10] [12].

Despite the potential of blockchain-based technology, severe security issues have been articulated in its integration with IoT to form an architecture for manufacturing business applications. This paper describes different types of security-related problems for information system design purpose. Below, this paper highlights an overview of the digitization of manufacturing business processes. Next, it explains the different security-related problems in IoT based information system, and then IoT with blockchain-based system architecture and related research works. Finally, the paper presents concluding remarks and the scope of future research.

2. Digitization of manufacturing business process

The manufacturing industry (e.g., apparel, automotive) inclines to worldwide business operations due to the financial benefits of the globalization of product design and development. In this way, a typical manufacturing network consists of organizations' sequence, facilities, functions, and activities to produce and develop an ultimate product or related services. This activity starts with raw materials purchase from selective suppliers and products produced at one or more production facilities [9]. Next, these products are moved to intermediate collection points (e.g., warehouse, distribution centers) to store temporarily to move to the next stage of the manufacturing network and finally deliver the products to intermediate storages or retailers or customers [11]. The connecting path from supplier to the customer can include several intermediaries, such as warehouse, wholesalers, and retailers, depending on the ultimate products and markets. Manufacturing enterprise connectedness is enabled by advances in modern information technologies and tightly coupled business processes [9], as shown in Fig. 1.

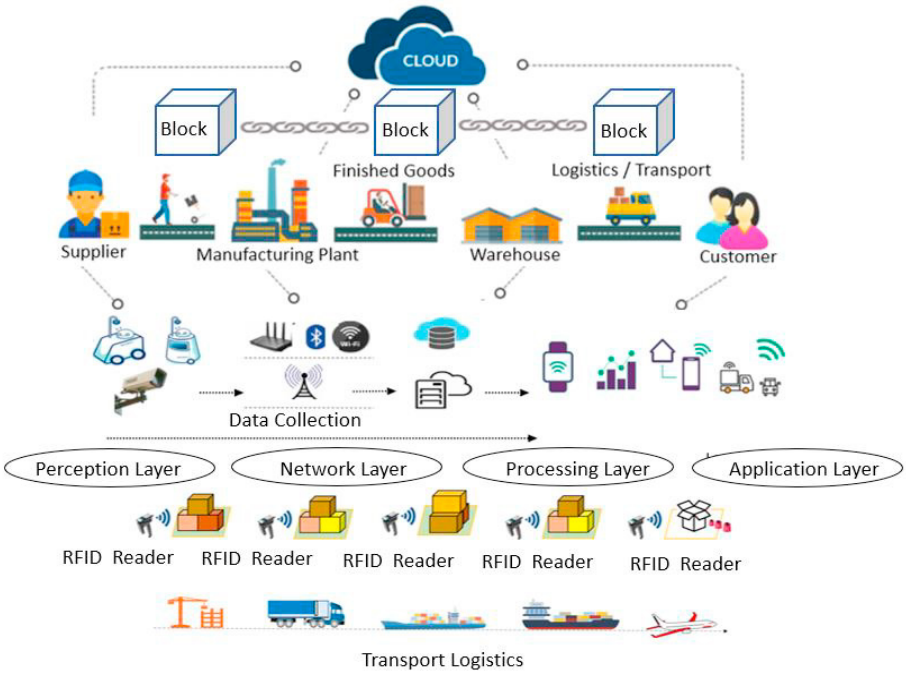

Fig. 1 RFID tagging level at different stages in manufacturing business processes

IoT technology aims to connect different things over the data communication networks. As a crucial technology in integrating heterogeneous systems or devices, SOA is often used to support the accumulated data processing from IoT system. SOA has been successfully deployed in research areas such as cloud computing, wireless sensor networks (WSNs), and vehicular network, as shown in Fig 1. Many multi-layered SOA architectures for IoT based

technology are proposed by academics and practitioners [11]. From the perspective of functionalities, a four-layered SOA based architecture is considered in this paper. A brief overview of this architecture is described in Table 1. Table 2 shows design considerations for industrial IoT applications. The evolution creates a seamless integration of multiple advanced information techniques across all operations of the manufacturing system. However, it results in many difficulties when building systems for achieving the intelligence, traceability, security, and flexibility of smart manufacturing.

Table 1. A layered architecture for IoT

Layers	Description
Perception layer	This layer is integrated with existing hardware (RFID, sensors, actuators) to sense/control the physical world acquire data.
Network layer	This layer provides essential working support and data transfer over a wireless or wired network.
Processing layer	This layer creates and manages services. It provides services to satisfy user needs.
Application layer	This layer provides interaction methods to users and other applications.

Table 2. Design considerations for industrial IoT

Design goals	Description
Energy	The duration an IoT device can operate with a limited power supply.
Latency	Time required for message propagation and processing.
Throughput	Maximum data can be transported through the network.
Scalability	The number of devices can be supported.

At the same time, with the huge growth of IoT applications and devices, security attacks pose a more serious threat for the manufacturing industry [13]. For example, Stuxnet [13], a malicious computer worm that targeted industrial computer systems were responsible for causing a substantial problem to Iran's nuclear program. The ransomware attack, WannaCry was a worldwide cyberattack in May 2017, which targeted computer systems worldwide. A new variant of WannaCry forced Taiwan Semiconductor Manufacturing Company (TSMC) to temporarily shut down several of its chip fabrication factories in August 2018 [14]. The virus spread to 10,000 machines in TSMC's most advanced manufacturing facilities. The centralized-controlled manufacturing system also may suffer from device spoofing and false authentication in information sharing [13].

Modern IoT systems are ushering their path for a revolutionized manufacturing industry in which many of the needed objects of use will be interconnected. These objects will link and communicate with each other and their surroundings to automate most regular tasks. This interconnection of IoT nodes requires security, seamless authentication, robustness, and accessible maintenance services. Blockchain comes out as a viable solution. The decentralized nature of the blockchain has resolved many securities, authentication, and maintenance issues regarding IoT-based information systems.

3. Related work on IoT Security and Privacy

Leveraging the advantages of integrating Blockchain in IoT, academics and practitioners have investigated how to handle critical issues, such as IoT device-level security, managing enormous volumes of data, maintaining user privacy, and keeping confidentiality and trust [14] [4]. In research work, a group of researchers [6] have proposed a blockchain-based IoT system architecture to prevent IoT devices' hacking problems.

A group of researchers [3] have introduced a blockchain integrated, IoT based information system for supply chain management. It provides an example of a reliable, transparent, and secured system. Another group of researchers [7] has reported a blockchain-based food supply chain that uses a proof-of-object (PoO) based authentication method. In this research, RFID tags are attached to the individual food products that are used for tracking purpose throughout their lifecycle within the supply chain network. All the real-time tracking and monitoring data produced are stored in a blockchain-based information system, which monitors food quality.

Francesco Longo and colleagues [16] have proposed that an information system consists of blockchain technology for supply chain management. The system allows the supply chain business partners to share their information among peers with appropriate authentication and integrity.

Practitioners and academics [9] advocated three primary aspects of modern manufacturing: (i) integration of heterogeneous data along with the global operations, (ii) data collection, and (iii) analysis of collected data. Within heterogeneous data integration, SOC plays a dominating role, given that intelligent perception and collection from the various computer networks of physical manufacturing resources and abilities.

Standard IoT systems are built on a centralized computing environment, which requires all devices to be connected and authenticated through the central server. This framework would not be able to provide the needs to outspread the IoT system in globalized operation. Therefore, moving the IoT system into the decentralized path may be the right decision. One of the popular decentralization platforms is blockchain technology.

Blockchain technology provides an appropriate solution to the security related issues mentioned above challenges posed by a distributed IoT ecosystem. Blockchain technology offers an approach to storing information, executing transactions, performing functions, and establishing trust in secure computing without centralized authority in a networked environment. A blockchain is a chain of timestamped blocks connected by special mathematical techniques (i.e., cryptographic hashes) and behaves like a distributed ledger whose data are shared among a network of users. This paper emphasizes the convergence of blockchain technology with IoT for a better manufacturing industry solution.

4. Categorization of security attacks

The security attacks in IoT-based information system can be categorized into four areas: (i) perception layer attacks, (ii) network layer attacks, (iii) processing layer attacks, and (iv) application-layer attacks. This section presents an overview of some of the security attacks and relevant literature reviews on the countermeasures to manage them. This security information and related references are itemized in Table 3, Table 4, and Table 5.

Table 3. Perception layer attacks

Type of attack	Description
Tampering	Physical damage is caused to the device (e.g., RFID tag, Tag reader) or communication network [1] security.
Malicious Code Injection	The attacker physically introduces malicious code onto an IoT system by compromising its operation. The attacker can control the IoT system and launch attacks [2].
Radio Frequency Signal Interference (Jamming)	The predator sends a particular type of radiofrequency signal to hinder communication in the IoT system, and it creates a denial of service (DoS) from the information system [2].
Fake Node Injection:	The intruder creates an artificial node and the IoT-based system network and access the information from the network illegally or control data flow [2].
Sleep Denial Attack	The attacker aims to keep the battery-powered devices awake by sending them with inappropriate inputs, which causes exhaustion of battery power, leading to the shutting down of nodes [2].
Side-Channel Attack	In this attack, the intruder gets hold of the encryption keys by applying malicious techniques on the devices of the IoT-based information system [1], and by using these keys, the attacker can encrypt or decrypt confidential information from the IoT network.

Table 4. Network layer attacks

Type of attack	Description
Traffic Analysis Attack	Confidential data flowing to and from the devices are sniffed by the attacker, even without going close to the network to get network traffic information and attacking purpose [1].
RFID Spoofing	The intruder first spoofs an RFID signal to access the information imprinted on the RFID tag [2]. The intruder can then send its manipulated data using the original tag ID, posing it as valid. In this way, the intruder can create a problem for the business operation.
Routing Information Attacks	These are direct attacks where the attacker spoofs or alters routing information and makes a nuisance by creating routing loops and sending error messages [1].
Sybil Attack	A single malicious node claims multiple identities (known as Sybil nodes) and locates itself at different networks [1]. This leads to colossal resource allocation unfairly.
Man in the Middle Attack (MiTM):	Here, an attacker manages to eavesdrop or monitor the communication between two IoT devices and access their private data [1].
Replay Attack	An attacker may capture a signed packet and resend the packet multiple times to the destination [15]. This keeps the network busy, leading to a DoS attack.

Table 5. Processing layer attacks

Type of attack	Description
Virus, Worms, Trojan Horses, Spyware and Adware	Using this malicious software, an adversary can infect the system to tampering with data or stealing information or even launching DoS [1].
Malware	Data present in IoT devices may be affected by malware, contaminating the cloud or data centres [15].

4. 1 *Application Layer attacks and solutions*

Blockchain has the potential to efficiently revolutionize the functioning of many IoT applications by providing a decentralized, trusted, and secure data sharing service in which information can easily be traced and backtracked. With the booming growth of IoT, the number of connected IoT devices and the data generated by them has become a massive bottleneck in meeting Quality-of-Service (QoS) [5]. In this way, blockchain comes into the picture by supporting a decentralized way of storing data and trustful and anonymous transactions. Blockchain technology can therefore be used for tracking and coordinating the billions of connected devices. It can also help the processing of transactions to allow significant savings for IoT industry manufacturers. Furthermore, the blockchains cryptographic algorithms would also help make consumer data privacy more robust [8].

A blockchain is a distributed immutable, verifiable ledger. A typical design of a blockchain consists of a series of transactions that are put into one block. These blocks are then linked so that if a transaction is altered in one block, it must be updated in all the subsequent blocks [8]. Since the ledger is maintained with many peers, it is challenging to alter a transaction [5]. Therefore, all the blockchain peers need to agree or validate each transaction to get added to a block [9]. Once validated, the block gets updated in the blockchain. This agreement is achieved with the help of consensus algorithms like Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof-of-Stake (DPoS), Proof-of-Authority (PoA) and so on. Blockchain technology is radically reshaping not only the modern IoT world but also the industries. Researchers of late have focused on integrating blockchain into the IoT ecosystem to include distributed architecture and security features.

5. IoT based information service and policy

The gathering, storing, and interpretation of personal data from IoT devices raises enormous privacy concern [17]. Besides, these data are often stored in the cloud computing environment, which compound the challenges introduced to the industry [19] and big data analysis [18] and have urged IoT-based technology a critical priority for privacy and data protection regulators [20]. The IoT technology-supported data gathering is also of interest to competition authorities and consumer protection and safety governing agencies.

In addition, transparency and accountability lie at centre of data protection regulatory obligations. Both need evidence (e.g., appropriate audit) of where data has flowed as an essential first step. Currently, such a capability is not considered or even provided at an appropriately deployed IoT-based information system in global manufacturing. It needs to cover diverse research areas (e.g., evidence of data flows within business processes, appropriate policy aligns with law and regulation, assistance to users in expressing their wishes in the automated system). All these policy-related issues need to consider building an effective IoT-based information system in the manufacturing industry.

6. Conclusion

The IoT-based system is a smart, more comprehensive network of interconnected objects, which through unique address schemes (e.g., EPC-based address), can cooperate and interact with their neighbours to collect data, process data, and convert it to daily business-related decisions. The data obtained from the IoT applications along manufacturing business processes can make operational decision-making much more comfortable. However, standalone IoT application systems face different security problems ranging from attacks on IoT devices to attacks on transit data. Furthermore, the tight integration of the digital world with the physical world using automated information systems has further created IoT systems' vulnerabilities.

IoT device data often stored in the service-oriented computing storage in the cloud, but they are not protected against compromised integrity devices or tampering at the source. In contrast, the blockchain is an evolving technology that can help with IoT systems resiliency. However, the extensive use of IoT technologies and blockchain-based linked data results in new security, privacy, and policy-related issues; at the same time, they can also be part of the solution. For example, more accurate models for figuring out security issues can be built using the data's contextual semantic interpretation. Besides, the purposeful interpretation of personal data exchanged among business partners could improve the ability of IoT-based manufacturing network users to control interactions and better manage their online privacy. The machine-processable and machine-readable representation of data-related policies can also provide different benefits to manufacturers by automation of policy-management tasks. There is a clear role for technical assistance in aligning privacy policy enforcement mechanisms with data protection regulations. The architecture proposed in this paper lays the groundwork for further research in data protection area, providing security and privacy-related issues that retains the most benefits of blockchain technology.

References

[1] Andrea, I., Chrysostomou, C., Hadjichristofi, G.., (2015). Internet of things: security vulnerabilities and challenges, In IEEE Symposium on Computers and Communication (ISCC), 180-187.

[2] Ahemd, M.M., Shah, M.A., Wahid, A., 2017. IoT security: a layered approach for attacks and defences. In: 2017 International Conference on Communication Technologies (ComTech), 104–110.

[3] Azzi, R., Chamoun, R.K., Sokhn, M., 2019. The power of a blockchain-based supply chain. Comput. Ind. Eng. 135, 582–592.

[4] Dorri, A., Kanhere, S.S., Jurdak, R., Gauravaram, P., 2019. LSB: A Lightweight Scalable Blockchain for IoT Security and Privacy. CoRR abs/1712.02969. http://arxiv.org/ abs/1712.02969. Ericsson, The connected future.

[5] Ferrag, M.A., Derdour, M., Mukherjee, M., Dahab, A., Maglaras, L., Janicke, H., 2019. Blockchain technologies for the internet of things: research issues and challenges. IEEE Internet Things J. Forbes, How blockchain can help increase the security of

smart grids.

[6] Kim, S.-K., Kim, U.-M., Huh, H.J., 2017. A study on improvement of blockchain application to overcome vulnerability of IoT multiplatform security. Energies 12 (402).

[7] Mondal, S., Wijewardena, K.P., Karuppuswami, S., Kriti, N., Kumar, D., Chahal, P., 2019. Blockchain inspired RFID-based information architecture for food supply chain. IEEE Internet Things J. 6 (3), 5803–5813.

[8] Makhdoom, I., Abolhasan, M., Abbas, H., Ni, W., 2019. Blockchain's adoption in IoT: the challenges, and a way forward., J. Netw. Computer Application, 125, 251–279.

[9] Pal, K. & Yasar, A. (2020). Internet of Things and blockchain technology in apparel manufacturing supply chain data management, Procedia of Computer Science, 170, 450-457.

[10] Pal, K. (2020). Information sharing for manufacturing supply chain management based on blockchain technology, in cross-Industry Use of Blockchain Technology and Opportunities for the Future, I. Williams, Ed. Hershey, PA, USA: IGI Global, 1-17.

[11] Pal, K. (2020). A Review of the IoT-Based Pervasive Computing Architecture for Microservices in Manufacturing Supply Chain Management, in Advanced Concepts, Methods, and Applications in Semantic Computing, O Daramola, and T. Moser (Ed.), Chapter 6,113-126, Hershey, PA, USA: IGI Global, USA.

[12] Pal, K. (2021). Applications of Secured Blockchain Technology in the Manufacturing Industry, Blockchain and AI Technology in the Industrial Internet of Things, S Pani, S Lau, and X Liu (Ed), Chapter 10,144-162, Hershey, PA, USA: IGI Global, USA.

[13] Pal, K. (2021). Securing the Internet of Things Applications Using Blockchain Technology in the Manufacturing Industry, IoT Protocols and Applications for Improving Industry, Environment, and Society, C González García and V García-Díaz (Ed), Chapter 11, 234-273, Hershey, PA, USA: IGI Global, USA.

[14] Pal, K. (2021). Blockchain Technology With the Internet of Things in Manufacturing Data Processing Architecture, Enabling Blockchain Technology for Secure Networking and Communications, Adel Ben Mnaouer and Lamia Chaari Fourati (Ed.), Chapter 10, 229-247, Hershey, PA, USA: IGI Global, USA.

[15] Varga, P., Plosz, S., Soos, G., Hegedus, C., 2017. Security threats and issues in automation iot. In: 2017 IEEE 13th International Workshop on Factory Communication Systems (WFCS), 1–6.

[16] Longo, F., Nicoletti, L., Padovano, A., d'Atri, G., Forte, M., 2019. Blockchain-enabled supply chain: an experimental study. Comput. Ind. Eng. 136, 57–69.

[17] Weber, R. H. (2010). Internet of things-new security and privacy challenges, Computer Law & Security Review, 26(1), 23-30.

[18] Smith, M., Szongott, C., Henne, B., von Voigt, G. (2012). Big data privacy issues in public social media, in 6th IEEE International Conference on Digital Ecosystems and Technologies (DEST), 1-6. - 60

[19] Takabi, H., Joshi, J., Ahn, G. (2010). Security and privacy challenges in cloud computing environments, IEEE Security & Privacy, 8(6). - 62

[20] Kohnstamm, J., Madhub, D. (2014). Mauritius declaration on the Internet of things, in International Conference of Data Protection and Privacy Commissioners.