Blockchain-Enabled Safety-as-a-Service for Industrial IoT Applications

Chandana Roy, Sudip Misra, and Saswati Pal

Abstract

The integration of Industrial Internet of Things (IIoT)-based technologies with the existing industrial manufacturing processes help to improve on-site safety of workers, reduce downtime of machines, improve productivity rate, and minimize near-miss incidents and casualties. However, a prior intimation of the various safety-related information may minimize the probability of accidents on the factory floor and casualty rates. Typically, the safety-as-a-service (Safe-aaS) infrastructure provides customized safety-related decisions to the registered end-users. However, there exist certain problems associated with the privacy of the information provided by the end-users during registration, decision parameters requested by the end-users, and data sensed by the sensor nodes. In this work, we provide an architecture of Blockchain integration into the Safe-aaS infrastructure. Additionally, we discuss the implementation and management of the Blockchain-enabled Safe-aaS architecture. Extensive analytical results demonstrate that the profit of the safety service provider (SSP) improves with the adoption of blockchain technology into the Safe-aaS architecture. On the other hand, the overall throughput in our proposed architecture follows an increasing trend, with the increase in the number of decisions successfully delivered. Additionally, the throughput decreases with the increase in the number of registered end-users.

Introduction

Industrial Internet of Thing (IIoT) technologies require safety as one of the essential considerations, across different industrial verticals. In the case of road transportation industries, IIoT provides safety-related information to the driver, to reduce accidents and improve traffic conditions on the road. Intelligent Transportation Systems (ITSs) and Advanced Driver Assistance Systems (ADASs) are some of the technologies developed with the primary aim of provisioning driver support systems and enabling V2X communication. Similarly, in the industrial scenario, different sensors, such as radio, video camera, Global Positioning System (GPS), accelerometer, temperature and humidity, pressure, and digital maps, are utilized to reduce the operational costs and increase the reliability of industrial assets. On the other hand, a prior intimation of safety-related information regarding the probability of accidents, risks associated with the process and working personnel, breakdown of machines, and control of machines from remote locations, may improve the workplace safety conditions.

Safe-aaS infrastructure is recently proposed to offer customized safety-related decisions as services to the end-users, as per their requirements [1]. The end-users provide basic information, register to the infrastructure, and select certain decision parameters through a Web portal, as illustrated in Fig. 1. On the other hand, the decision provided to the end-user may be generated from the combination of multiple sensor data. Moreover, the data sensed by the sensor nodes are primarily processed in the cloud/edge based on the time-criticality of the data. One of the major challenges in Safe-aaS is to provide security and privacy in a decentralized manner, considering the Quality of Service (QoS) and user-level agreement. Recently, blockchain technology is widely applied across various industries to provide trustworthiness, privacy, and security in a decentralized manner. Typically, blockchains are referred to as distributed ledger, which help to secure transactions in the network. Moreover, blockchains are characterized as decentralized, transparent, and peer-to-peer networks [2]. Motivated by these facts, we incorporate blockchain into the Safe-aaS infrastructure to secure the data sensed by the sensor nodes and the transactions among different Safety Service Providers (SSPs) and registered end-users.

Digital Object Identifier: 10.1109/IOTM.0001.1900080

Safe-aaS: The Safety-as-a-Service Architecture

A Safe-aaS [1] architecture is a unique, newly designed, Service-Oriented Architecture (SOA)-based, five-layered architecture, which provides customized safety-related decisions to the end-users, as per their request. The end-users register to the infrastructure, select the origin and destination points, and specify the decision parameters through the Web portal, as depicted in Fig. 1. In an industrial scenario, the decision parameters may be downtime of machines, proper safety measures to be taken by the workers, and the health of the machine. Further, the on-site working professionals, officers, and different government agencies are the end-users of Safe-aaS. Thereafter, the end-users make payments based on the number of decision parameters selected by them and their duration of service. However, the end-users are completely unaware of the back-end process of decision generation.

The five layers of the Safe-aaS infrastructure are *device*, *edge*, *decision*, *decision virtualization*, and *application*. Fig. 2 illustrates the block diagrammatic representation of the infrastructure. There are heterogeneous types of static and mobile sensor nodes present in the device layer. Static sensor nodes such as scalar and camera sensor nodes are deployed at a particular geographical location. On the other hand, the mobile sensor nodes are the sensor nodes placed into mobile entities such as humans, vehicles, and robots. These sensor nodes sense and transmit the sensed data to the edge layer/cloud for primarily processing the data. Typically, the sensed data which are time-critical in nature, are processed at the edge nodes. Further, the processed data are transmitted to the decision layer for the extraction of meaningful information from the data and generate a decision. Thereafter, the logical mapping between the decision parameters requested by the end-users and the decisions to be delivered to them is done in the decision virtualization layer. Practically, the decision parameters requested by the different end-users may be of similar type. Therefore, the decision generated for each of the registered end-users may comprise overlapping decision parameters. Using the concept of decision virtualization, the same decision is delivered to multiple end-users simultaneously by the safety service provider (SSP). The application layer acts as the interface between the end-users and the Safe-aaS infrastructure. In order to receive a safety-related decision(s), the end-users register to the infrastructure through the Web portal.

There are different actors present in the Safe-aaS architecture, i.e., sensor owners, vehicle owners, SSP, and end-users. The sensor owners deploy their sensor nodes at different geographical

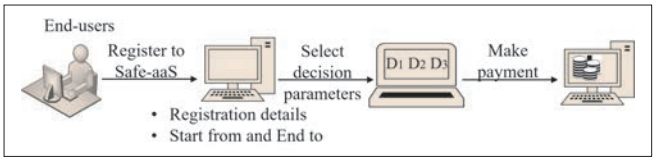

FIGURE 1. Registration of end-users in Safe-aaS

locations. Moreover, the sensor nodes are externally placed into humans and robots. In the practical scenario, various types of semi-automatic/fully automatic transfer vehicles are used inside the different operational units in industries for lifting, dumping, and transferring heavy raw materials, machines, and finished products. These vehicles may possess built-in sensor nodes, or the sensor nodes are externally placed into them. The owners of these vehicles are known as vehicle owners. These sensor and vehicle owners give their sensor nodes on rent to the SSP. On the other hand, the SSP is a centralized entity that manages the entire Safe-aaS architecture. Therefore, business transactions occur among the different actors in Safe-aaS. The trust of the data sensed by the sensor nodes, security, and privacy are some of the essential matters of concern to provide Safe-aaS services to the end-users. In order to improve the transparency of the decisions delivered to the registered end-users, security, and storage of the decisions generated, the integration of blockchain technology with the Safe-aaS architecture has the potential to resolve these issues.

Need for Blockchain in Safe-aaS

An SOA-based IIoT platform assures new opportunities as well as challenges pertaining to privacy and security for advanced business models, and service-level applications. Typically, the end-users register to the Safe-aaS platform and request certain decision parameters. Based on the decision parameters selected by them, the end-users receive customized decisions. Further, multiple end-users may request similar decision parameters. Before the decisions are virtualized, the decision parameters requested by the end-users are mapped with the decisions to be delivered to them. Therefore, the management of the appropriate decision parameters during the process of decision virtualization is a critical task. Moreover, there is a necessity of addressing the privacy and data management aspects into the Safe-aaS platform. The following attributes characterize the Blockchain-enabled Safe-aaS architecture:

- *Extends complete privacy*: The concept of decision virtualization enables the sharing of the same decision among multiple end-users simultaneously. Therefore, it is indispensable to retain the end-users' details, decision parameters requested by them, and restrain unauthorized access to the sensed data. The integration of blockchain technology with the Safe-aaS architecture empowers the Safety Service Provider (SSP) to achieve absolute privacy, without permitting any third party to have access to the raw sensor data or processed decisions.
- *Facilitates secure user-level agreement*: The decision parameters requested by multiple end-users may overlap. Therefore, the decision generated is shared with multiple registered end-users. The sensor nodes deployed at different geographical locations in the device layer sense and transmit data to the edge layer/cloud. These data are processed to generate decisions. Further, these generated decisions are utilized in accordance with the decision virtualization to accomplish the user level agreement. Therefore, the implementation of the blockchain approach caters to the necessary security aspects of the Safe-aaS architecture.
- *Improves service level quality*: In order to validate the agreement both at the user level and the service level, the blockchain technology facilitates the traceability of the appropriate utilization of resources.
- *Enforces light-weight blockchain platform*: The Safe-aaS architecture comprises five layers, where the blockchain platform is easily implementable to enforce secure and smart agreements. This provides a secure and light-weight platform for the generation of customized decisions to be delivered to the end-users.

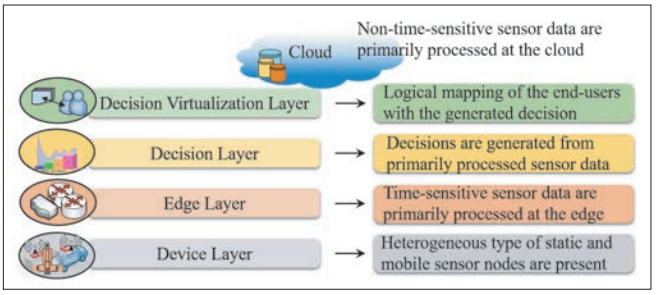

FIGURE 2. Safety-as-a-Service: block diagram

Blockchain-Enabled Safe-aaS

In Safe-aaS implementation, the end-users in the device layer share their personal information with the SSP during registration. Additionally, the end-users may possess vehicles with built-in or externally-placed sensor nodes. These end-users may act as vehicle owners and rent their sensor nodes to the Safe-aaS infrastructure. Therefore, there is a requirement of the management of the resources as well as information of end-users. Considering these issues, we present the blockchain-enabled Safe-aaS architecture to harness the benefits of blockchain. The integration of blockchain improves the privacy aspects for the identity management of the end-users and provides secure decisions to the end-users in Safe-aaS. This idea puts forth the re-architecting of a distributed blockchain-enabled decision virtualization layer, wherein the decisions are processed. The proposed distributed network at the decision virtualization layer of Safe-aaS, as illustrated in Fig. 3, is based on the concept of the blockchain framework. Consequently, secure on-demand customized decisions are provided to the end-users via digitally signed smart contracts. Blockchain-enabled Safe-aaS ensures the security and trust among the various actors in the network, with the help of a digital signature. The digital signature comprises the complete transaction details as well as the cryptographic key. On the other hand, the end-users make payment based on the decision parameters selected by them during registration. We consider that the Safe-aaS infrastructure comprises distributed SSPs and decision virtualization administrators with high computation capability. Thus, these resource-filled nodes act as *miners* and maintain the records of the service transactions.[1] These miners carry out complex algorithms [3] to produce blocks for every transaction. The logical interpretation and mapping of the generated decisions with the decision parameters requested by the end-users is done at the decision virtualization layer and is passed onto the miners. The algorithm executed by the miners includes the arrangement of the transaction details (services and payment) in a block. Thereafter, the transaction is sealed with an encrypted key, and the digital signature is created. The miners broadcast this block in the distributed network across the layers to achieve the transaction details verified by the nodes. The nodes in the network work on the cryptographic key to validate the transaction details. After the block is successfully validated, the block is placed in the network, and the blockchain is updated. Further, any form of alteration in the transaction information is not feasible. Since the end-users, as well as the sensor nodes, are highly resource-constrained in nature, we ensure that the copy of the blockchain is retained only with the SSPs and the decision virtualization administrators. Each of the miners in the blockchain may have different computation power and storage capacity. Thus, we consider that these miners receive incentives in terms of resources. When an end-user registers to the Safe-aaS platform and requests safety-related decisions, a transaction is recorded at the miner. As the miners receive incentives against each of the blocks cre-

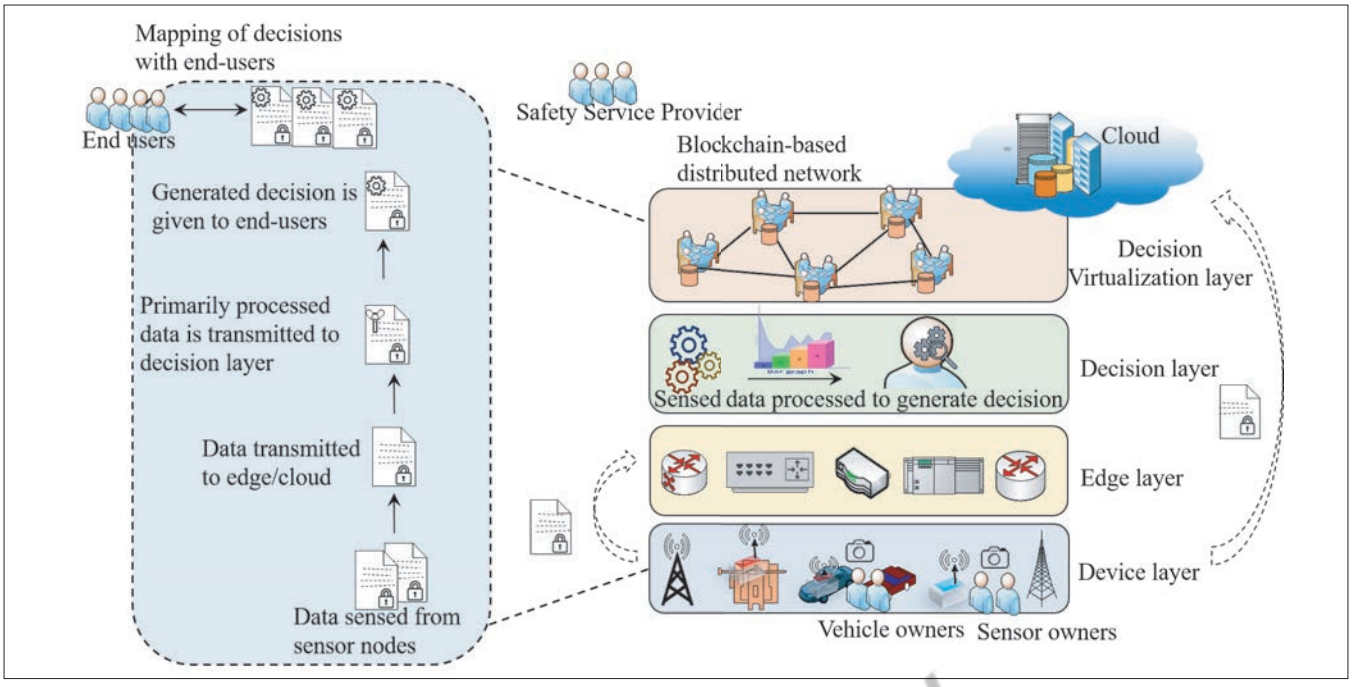

FIGURE 3. Blockchain-enabled Safe-aaS.

Property	Blockchain-enabled Safe-aaS
Type	Consortium
Access	Permissioned
User information	Pseudonymity
Device authentication	Mandatory
Consensus mechanism	PBFT, gossip learning-enabled PoW
Consensus determination	Selected set of nodes
Read permission	Restricted
Immutability	Could not be tampered
Scalability	Highly scalable
Robustness	Highly robust
Confidentiality	Distributed

TABLE 1. Characteristics of blockchain-enabled Safe-aaS.

ated for the recorded transactions, competition exists among them for the creation of the blocks. Moreover, the blockchain records are chronologically ordered, depending on the transactions scattered over the network. Thus, transparency in the requested decision parameters and their corresponding price charged from the end-users is maintained. The reputation of the miners (SSPs) is improved in terms of their reliability and quality of service (QoS). Therefore, blockchain-enabled Safe-aaS infrastructure helps to generate transparent decisions, provide these decisions to multiple end-users, and improves the integrity of the infrastructure. The various characteristics of blockchain-enabled Safe-aaS are represented in Table 1.

Blockchain: Implementation and Management

Blockchain Partakers: We consider a large geographical area, which is uniformly divided into several regions, with multiple SSPs distributed over the network for blockchain consortium. Heterogeneous types of static and mobile sensor nodes are deployed in each of these regions. Additionally, sensor/vehicle owners, end-users, and SSPs are also present. Depending upon the area of the region, multiple SSPs may be present in the region. The key participants in the scenario are the *SSPs*, *decision virtualization administrators*, and *end-users*. The end-users register to the Safe-aaS architecture for safety-related decisions through the Web portal. On the other hand, the sensor/vehicle owners rent their sensor nodes to the Safe-aaS infrastructure. The general information regarding the sensor node such as sensor type, the unique id of a sensor node, and other related attributes are maintained by the SSPs for management purposes.

The decision virtualization layer comprises decision virtualization administrators, who are responsible for the mapping of the end-users' requested decision parameters and the decisions generated. Thereafter, the transactions between the end-users and decision virtualization administrators are recorded with the SSPs over the network. The SSPs compete among them to convert these transactions into a block. These blocks are added to the chain and broadcasted to the entire network.

Blockchain Framework: The Safe-aaS blockchain framework is designed to operate as permissioned blockchains featuring the concept of consortium access. The primary motivation behind permissioned blockchain is to authorize the SSPs to act as miners and concurrently restrict the access of blockchain data only to the registered end-users. Practically, the Safe-aaS architecture is distributed over a large geographical area. Thus, with the increase in the number of registered end-users, scalability issues arise. As the number of nodes acting as miners is restricted, the permissioned consensus process in the blockchain-enabled Safe-aaS caters to the needs for scaling the miners' resources. Therefore, miners gain incentives. Further, the amount of resources required increases with the increase in the number of transactions. On the other hand, the Safe-aaS consortium permits cooperation and modification of rules related to the transactions and creation of blocks in Safe-aaS. To enhance the modularity in our architecture, we consider the presence of region-based multiple blockchains in the entire Safe-aaS infrastructure. The SSPs and decision virtualization administrators of several regions form the backbone of blockchain. These SSPs and administrators are logically interconnected among them across the overall network. Therefore, each regional segment has its own distributed blockchain, service level agreement, consensus rules, control policies, and payment regulations. The variation in profit of SSPs with time is depicted in Fig. 4. We observe that the profit of SSP increases

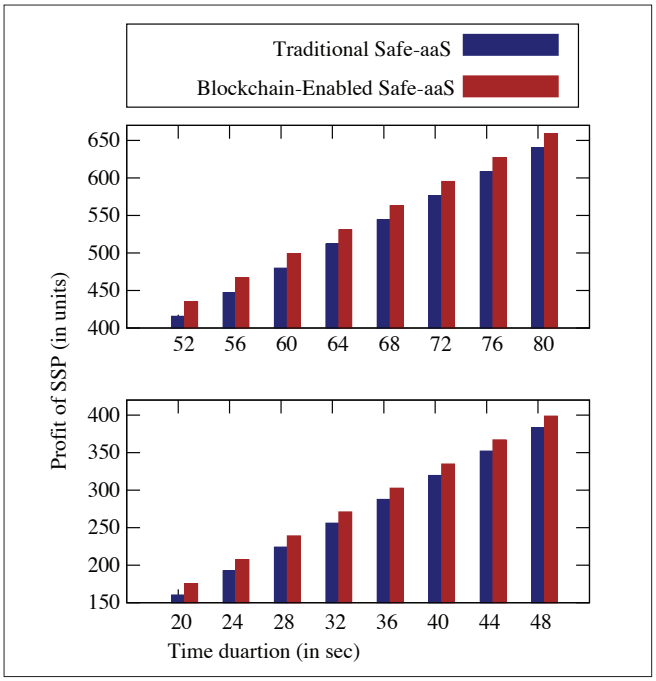

FIGURE 4. Profit of SSP.

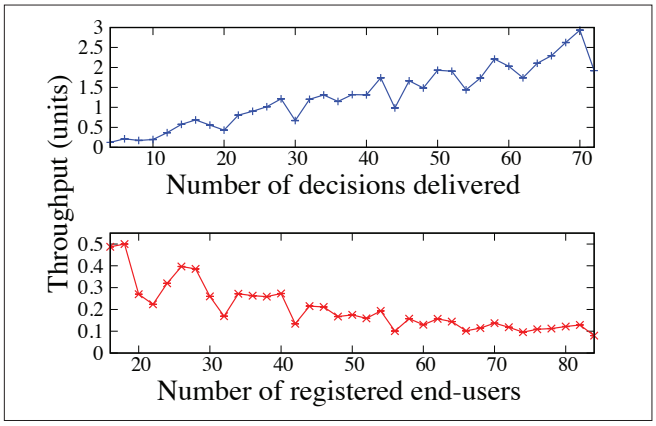

FIGURE 5. Throughput.

in the blockchain-enabled Safe-aaS compared to that of the traditional Safe-aaS. Therefore, we conclude that security is one of the important factors affecting the revenue of service providers.

Secure Services: An SSP maintains registration and provides services considering secure identification and service authorization. Further, the SSP implements smart contracts to execute identification and authentication, enables the payment settlements, and provides customized services. Typically, the SSP manages the two vital functionalities, user assertion and service provisioning. During registration, the end-user provides their personal details, starting and destination point, and decision parameters, through the Web portal. The SSP keeps track of the user identities and assigns them a pseudonym for further reference. This promotes a pseudonymous blockchain identity (BID), which comprises an alphanumeric string. Consequently, the SSP refers to the BID in order to transmit the user details to the other layers. Similarly, the data sensed by the sensor nodes are transmitted securely to the cloud/edge layer for further processing and generating a user-oriented composite and customized decision, as depicted in Fig. 3. The entire information pertaining to the users, their requests, and sensed data is maintained through a blockchain service agreement (smart contract) to enable secure and smooth services. On the other hand, the throughput[2] of a Blockchain-enabled Safe-aaS exhibits an increasing trend with the increase in the number of decisions successfully delivered to the end-users, as demonstrated in Fig. 5. However, we observed that the throughput shows a decreasing trend with the increase in the number of registered end-users in the scenario. One of the possible reasons behind such a trend is that with the increase in the number of end-user requests, congestion may occur in the network, which is effectively handled with the existing queuing models. However, the proposed blockchain-enabled infrastructure provides a secure domain without compromising the overall network performance.

Smart Contracts: We consider smart contracts are able to convert blockchain-enabled Safe-aaS into a high computing platform [4] and fulfill the requirements of the resource-intensive SSPs. The different pay-off terms corresponding to the decision parameters requested by the end-users are encoded into the smart contracts. The contract regulates the interactions between an end-user with the SSP and the other layers of Safe-aaS with the help of the virtual administrator. Safe-aaS incorporates two smart contracts to enable smooth functioning of the blockchain framework, a service provisioning smart contract (SPSC), and a decision virtualization smart contract (DVSC). In order to approve the access of the end-users to the details filled by them during registration, the SPSC is utilized by the SSP. Further, the SPSC enables the establishment of a secure and automatic agreement with the end-user. Additionally, the SPSC dictates the financial details associated with each of the end-users, when they register themselves to the Safe-aaS platform. On the other hand, the decision virtualization administrator applies DVSC to bridge the interaction gap with the other layers of Safe-aaS. The DVSC integrates information from the decision layer with the BID and the corresponding decision parameters requested by the end-users and renders the user-oriented compact decisions. Therefore, DVSC protects the decision parameters requested by the end-users and their personal details.

Consensus Algorithm: Smart contracts handle the transactions for service provisioning. On the other hand, the consensus algorithm [3] converts these transactions into blocks. To apply conventional consensus algorithms such as Proof-of-Work (PoW) [4], the resource overhead required is quite high. Further, the application of the algorithm becomes challenging in a distributed environment. Therefore, the implementation of the consensus algorithm in the Safe-aaS infrastructure is difficult. We consider a hybrid structure of gossip learning-empowered PoW (Proof of Work) and PBFT (Practical Byzantine Fault Tolerance) for a permission-based Safe-aaS blockchain consortium. The combination of gossip learning [5] and PBFT improves scalability and robustness in terms of communication among the multiple distributed SSPs in the Safe-aaS platform. The PBFT protocol inducts a voting mechanism to select the appropriate miner/SSP among the available different SSPs or decision virtualization administrators in the network. The selected miners follow a gossip learning-based algorithm to train the data collected from distributed nodes at the devices/edge nodes/cloud and provide the logically shared response for the decision parameters requested by end-users. The fusion of these two techniques is blended into the proposed framework to provide secure mining of transactions into blocks.

Related Work

In the past few years, different researchers explored various research issues related to safety and security in various industries such as manufacturing, road transportation, logistics, and supply chain. The edge devices in the IIoT edge gateway are utilized to connect the physical systems with the cyber world. However, these devices are prone to various forms of threats such as targeted ransomware. Considering the likelihood of such attacks and threats, Hawawreh *et al.* [6] designed the first version of a ransomware security testbed for an IIoT edge gateway. The authors also suggested some countermeasures to deal with these attacks. Further, in order to integrate advanced technologies, advanced control, data analysis, and improve security, the introduction of an intelligent manufacturing system is necessary.

Urbina *et al.* [7] proposed the architecture of smart sensors, which possess the characteristics of real-time data analysis, and wired/wireless connectivity. Additionally, the authors implemented the architecture of smart sensors using hardware available in the market and implemented two test environments. Recently, Roy *et al.* [1] proposed a unique SOA-based infrastructure, Safe-aaS, which provides safety-related customized decisions to the end-users. The authors introduced the concept of decision virtualization, by which safety-related decisions are simultaneously delivered to multiple end-users. However, the provision of safety services in the industrial scenario, security and privacy aspects of the data generated from the sensor nodes, and the information of end-users are not addressed.

One of the essential aspects of implementing IoT architecture is maintaining data security, confidentiality, and integrity [8], as IoT is applicable in different scenarios such as the UAV framework [9] and industrial applications [10], which often face security breaches. In recent years, IoT and IIoT have witnessed an enormous dependency on blockchain technology owing to the no single-point-of-failure nature. Several works have proposed the concept of Blockchain-as-a-Service by blending the blockchain technique with the cloud as well as fog architecture [11, 12]. The consequent modified services provide transparency, distributed security, and advanced performance. The existing literature focuses on blockchain, which serves as the underlying secure platform for several architectures and services in the IIoT application. On the other hand, decentralization, security, and scalability are the important features of the blockchain platform. In order to address the security and efficiency of a blockchain-enabled platform, Liu *et al.* [13] proposed a deep reinforcement learning-based framework for blockchain-enabled IIoT systems. Fernandez-Carames and Fraga-Lamas [3] provided a comprehensive review of blockchain-based industrial communications architecture and service-oriented architectures for Industry 4.0 applications. They provided an outline for determining the benefits of embedding blockchain with industrial applications to enhance cybersecurity. Alahmadi and Lin [14] proposed the utilization of smart contracts for supply chain management in IIoT. The authors introduced the concept of fairness in IIoT by imposing penalties to prevent the malicious nature of the participants. Several works related to blockchain-based smart grid frameworks are presented by Musleh *et al.* [15], which show the efficacy of blockchain in handling cyber-physical security threats.

Conclusion

In this work, we focused on the decision access mechanism for end-users in the Safe-aaS architecture. We highlighted the necessity of distributed security and confidentiality mechanisms for the Safe-aaS architecture in the context of IIoT. We envisioned a consortium blockchain-enabled Safe-aaS architecture to provide reliable data sharing and secure services among several actors. Further, we proposed the fusion of blockchain and gossip learning as a promising way to achieve privacy-aware registration, built-in security, and smart information sharing in the blockchain-enabled Safe-aaS architecture. We discussed the framework for blockchain-based safety service providers and the value of efficient resource usage.

In the future, we plan to implement the blockchain-enabled Safe-aaS architecture as well as assess the challenges faced while integrating gossip learning into the consensus mechanism of permissioned blockchain. Subsequently, we plan to address the solution techniques to achieve a hybrid blockchain.

References

[1] C. Roy *et al.*, "Safe-aaS: Decision Virtualization for Effecting Safety-as-a-Service," *IEEE Internet of Things J.*, vol. 5, no. 3, June 2018, pp. 1690–97.

[2] A. Bahga and V. K. Madisetti, "Blockchain Platform for Industrial Internet of Things," *J. Software Engineering and Applications*, vol. 9, no. 10, 2016, p. 533.

[3] T. M. Fernández-Caramés and P. Fraga-Lamas, "A Review on the Application of Blockchain to the Next Generation of Cybersecure Industry 4.0 Smart Factories," *IEEE Access*, vol. 7, 2019, pp. 45,201–218.

[4] F. Daniel and L. Guida, "A Service-Oriented Perspective on Blockchain Smart Contracts," *IEEE Internet Computing*, vol. 23, no. 1, Jan 2019, pp. 46–53.

[5] I. Hegedüs, G. Danner, and M. Jelasity, "Gossip Learning as a Decentralized Alternative to Federated Learning," *IFIP Int'l. Conf. Distributed Applications and Interoperable Systems*, Springer, 2019, pp. 74–90.

[6] M. Al-Hawawreh, F. D. Hartog, and E. Sitnikova, "Targeted Ransomware: A New Cyber Threat to Edge System of Brownfield Industrial Internet of Things," *IEEE Internet of Things J.*, vol. 6, no. 4, Aug. 2019, pp. 7137–51.

[7] M. Urbina *et al.*, "Smart Sensor: SoC Architecture for the Industrial Internet of Things," *IEEE Internet of Things J.*, vol. 6, no. 4, Aug. 2019, pp. 6567–77.

[8] P. Sarigiannidis, E. Karapistoli, and A. A. Economides, "Modeling the Internet of Things Under Attack: A G-Network Approach," *IEEE Internet of Things J.*, vol. 4, no. 6, 2017, pp. 1964–977.

[9] T. Lagkas *et al.*, "UAV IoT Framework Views and Challenges: Towards Protecting Drones?" *Sensors*, vol. 18, no. 11, 2018, p. 4015.

[10] A. Triantafyllou, P. Sarigiannidis, and T. D. Lagkas, "Network Protocols, Schemes, and Mechanisms for Internet of Things (IoT): Features, Open Challenges, and Trends," *Wireless Commun. and Mobile Computing*, vol. 2018, Sept. 2018.

[11] M. Samaniego and R. Deters, "Blockchain as a Service for IoT," *IEEE Int'l. Conf. Internet of Things (iThings), IEEE Green Computing and Communications (GreenCom), IEEE Cyber, Physical and Social Computing (CPSCom),* and *IEEE Smart Data (SmartData)*, 2016, pp. 433–36.

[12] J. Singh and J. D. Michels, "Blockchain as a Service (BaaS): Providers and Trust," *IEEE European Symp. Security and Privacy Wksps. (EuroS&PW)*, 2018, pp. 67–74.

[13] M. Liu *et al.*, "Performance Optimization for Blockchain-Enabled Industrial Internet of Things (IIoT) Systems: A Deep Reinforcement Learning Approach," *IEEE Trans. Industrial Informatics*, vol. 15, no. 6, June 2019.

[14] A. Alahmadi and X. Lin, "Towards Secure and Fair IIoT-Enabled Supply Chain Management via Blockchain-Based Smart Contracts," *IEEE Int'l. Conf. Commun. (ICC)*, 2019, pp. 1–7.

[15] A. S. Musleh, G. Yao, and S. Muyeen, "Blockchain Applications in Smart Grid–Review and Frameworks," *IEEE Access*, vol. 7, 2019, pp. 86,746–757.

Biographies

Chandana Roy (chandanaroy@iitkgp.ac.in) is an Institute Scholar and is pursuing her Ph.D. in the Department of Industrial and Systems Engineering, Indian Institute of Technology Kharagpur, India. She received her M.Tech. degree from National Institute of Technology Durgapur, India in 2012. Prior to that, she completed the B.Tech. degree in electrical engineering from the West Bengal University of Technology, India in 2010. Her current research interests include Internet of Things (IoT), Industrial Internet of Things (IIoT), Wireless Body Area Networks (WBANs), Blockchain, and cloud computing. She is student member of the IEEE and ACM..

Sudip Misra (sudipm@iitkgp.ac.in) is a professor at the Indian Institute of Technology Kharagpur. He received his Ph.D. degree from Carleton University, Ottawa, Canada. He is the author of over 300 scholarly research papers and 10 books. He is a fellow of different scientific and technical societies such as FNASc (India), FIETE (India), FIET (UK), and FRSPH (UK). Currently, he is an associate editor of *IEEE Transactions Mobile Computing*, *IEEE Systems Journal*, and *IEEE Transactions on Sustainable Computing*. He is an editor of *IEEE Transactions on Vehicular Computing*. He has been a recipient of nine research paper awards in different conferences. He was awarded the IEEE ComSoc Asia Pacific Outstanding Young Researcher Award at IEEE GLOBECOM 2012. He was also awarded the Canadian Government's prestigious NSERC Post Doctoral Fellowship and the Humboldt Research Fellowship in Germany.

Saswati Pal (saswatipal@iitkgp.ac.in) is an Institute Research Scholar and pursuing her Ph.D. from the School of Nano-Science and Technology, Indian Institute of Technology Kharagpur, India. Prior to that, she was working as a senior research fellow with the Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur, India. She received her M.Tech. degree in electronics and communication from the National Institute of Technology Jalandhar, India in 2016. Her current research interests include molecular communication, Internet of Things, Blockchain, and wireless body area networks.

Footnotes

[1] Transactions of the end-users with the Safe-aaS architecture refer to the decision parameters requested by the end-users, payment done by them, and decision generated.

[2] The throughput of a Blockchain-enabled Safe-aaS infrastructure with respect to a SSP is the probability of that SSP to be selected as a miner and number of decisions delivered per registered end-users by that SSP.