IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 22, 2020, accepted August 12, 2020, date of publication August 19, 2020, date of current version September 1, 2020.

*Digital Object Identifier 10.1109/ACCESS.2020.3017891*

# BlockEdge: Blockchain-Edge Framework for Industrial IoT Networks

**TANESH KUMAR[1], (Student Member, IEEE), ERKKI HARJULA[1], (Member, IEEE), MUNEEB EJAZ[1], AHSAN MANZOOR[2], PAWANI PORAMBAGE[1], (Member, IEEE), IJAZ AHMAD[3], (Member, IEEE), MADHUSANKA LIYANAGE[1,4], (Senior Member, IEEE), AN BRAEKEN[5], AND MIKA YLIANTTILA[1], (Senior Member, IEEE)**

[1]Centre for Wireless Communication, University of Oulu, 90014 Oulu, Finland
[2]Rovio Entertainment Company, 02150 Espoo, Finland
[3]VTT Technical Research Centre of Finland, 02044 Espoo, Finland
[4]School of Computer Science, University College Dublin, Dublin 4, D04 V1W8 Ireland
[5]Industrial Sciences Department (INDI), Vrije Universiteit Brussel, 1050 Brussels, Belgium

Corresponding author: Tanesh Kumar (tanesh.kumar@oulu.fi)

This work was supported in part by the Academy of Finland through the projects Industrial Edge, SecureConnet, WiFiUS: Massive IoT, 6G Flagship Project under Grant 318927, in part by the European Union through the Resilient and Secure Multi-controller Communication Platform for 5G Networks (RESPONSE 5G) under Grant 789658, in part by the Technology Industries of Finland Centennial Foundation through the Edge Computing Enhanced by Artificial Intelligence (MEC-AI) project, and in part by the Jane and Aatos Erkko Foundation.

**ABSTRACT** Industry 4.0 encompasses a promise of a new industrial revolution in terms of providing secure, intelligent, autonomous and self-adaptive industrial IoT (IIoT) networks. Key industrial applications and systems will be significantly more complex due to the involvement of the vast number of different devices and diverse nature of various stakeholders and service providers. These complex industrial processes, services and applications also have strict requirements in terms of performance - latency in particular - and resource-efficiency, together with high standards for security and trust. In this context, Blockchain and Edge Computing emerge as prominent technologies to address the mentioned essential requirements and to further strengthen the rise of the new era of digitization. The Edge computing paradigm ensures low latency services for IIoT applications while optimizing the network usage, whereas Blockchain provides a decentralized way for ensuring data integrity, trust and security. In this paper, we propose a 'BlockEdge' framework that combines these two enabling technologies to address some of the critical issues faced by the current IIoT networks. We verify the feasibility of our approach by evaluating the performance and resource-efficiency of BlockEdge in terms of latency, power consumption and network usage, through simulations against non-Blockchain solution.

**INDEX TERMS** Blockchain, edge computing, fog computing, cloud computing, industrial IoT, industry 4.0, performance evaluation.

## I. INTRODUCTION

With the emergence of the Fifth generation mobile networks (5G) and the recent evolution of the enabling technologies related to Internet of Things (IoT), the current world is facing a significant digital transformation from almost every aspect of the daily life [1]. These enabling technologies may include Blockchain, Edge/Fog computing, Network virtualization and Softwarization technologies, among others. They play a vital role in enabling numerous critical application areas, such as industrial automation, healthcare, transportation, banking, and smart home, among others. In Industrial IoT (IIoT), sensor information is gathered from a rapidly growing number of novel advanced sensors, producing huge amounts of data to be processed, often with real-time requirements. For example, an industrial process in a chemical factory is highly delay-critical and therefore requires very timely actions to execute all necessary processes optimally, securely and safely. Furthermore, the processing and analysis of the gathered sensor data and intelligent decision-making based on it, typically requires high computational capacity in this kind of industrial scenario.

The traditional centralized cloud-based approaches are mostly suitable for IIoT applications that require high

The associate editor coordinating the review of this manuscript and approving it for publication was Alessandro Pozzebon.

computational capacity and are delay-tolerant. These applications include, e.g. globally accessible data storage and highly demanding computing tasks, big data analysis, processing and decision making with no real-time requirements. However, due to the increasing number of low-latency services, it would be sub-optimal to execute all processing and data management tasks in centralized clouds [2]. Therefore, IIoT applications, that comprise of massive numbers of sensors, actuators, devices, and machines that generate huge volumes of data, and at the same time, require low latency, high reliability and high security, would benefit from edge computing [3]. One of the similar and very relevant concept to edge is fog computing; however, fog networks can be considered as much richer in terms of resources/capabilities as compared with edge. Fog network can be seen as the vast umbrella of technologies and required resources that bring cloud computing capabilities closer to the edge/IoT networks [61]. In addition to current edge and fog computing solutions, data management policies, security and reliability requirements favor local edge computing solutions (called as local edge or extreme edge) [4].

Recently, Blockchain has become a hot topic due to its high applicability for various financial and banking domains, e.g. in crypto-currencies such as Bitcoin. However, Blockchain as a generic technology for providing trust with distributed and decentralized settings, can as well be utilized in several other promising applications, such as healthcare, supply chain management, and IIoT [5], [66]. Among all these, IIoT is one of the most prominent application areas, in which Blockchain can be considered as an enabler technology for many key highlighted applications. IIoT setups are growing massive and their complete deployment can raise various challenges related to, e.g. ensuring Confidentiality, Integrity and Availability (CIA), improving data availability and accountability, among many others. Blockchain can address these requirements and play a key role by providing secure and verifiable solutions for data storing and sharing. IIoT applications have requirements of a similar kind to ensure secure data integrity and trust among various involved stakeholders related to different parts of the logistic chain (e.g., acquiring raw materials, transportation, storage, factory processing and deployment to customers). In these applications, requirements such as monitoring of each process and maintaining history at each process are also crucial [6].

The main objective of this work is to incorporate these two potential technologies, i.e. Edge computing and Blockchain for IIoT networks to address the increasing/advanced requirements of current IoT based industrial applications [7], [8]. Edge computing can be utilized to gain low latency features, whereas Blockchain is vital to provide secure and trusted data sharing, accessibility and tracking/monitoring functionalities. Therefore, this article elaborates the importance of Blockchain-Edge co-existence using an IIoT use case, which is also under investigation in the Industrial Edge project [9]. In this paper, we further extend our previously proposed work (three-tier architecture) in [3], [4], [40], [41] by adding blockchain and other essential functionalities and propose the Blockchain-Edge based framework for the discussed scenario and analyzed the potential requirements and challenges related to this framework for IIoT applications.

### A. MOTIVATION

Industry 4.0 applications require edge-based distributed, secure and virtualized functions/resources to keep the overall system cost-efficient and manageable in the large geographical areas with varying quality of access networks, and at the same time, enable autonomous and real-time industrial process monitoring and management in industrial/factory premises. Such kind of industrial applications will utilize Multi-access Edge Computing (MEC) and 5G technology in the access network to provide a high-performance cloud platform for localized applications. MEC, for instance, provides a low-latency remote control functionality for remote operations of a number of critical industrial processes. The key measurable quantities in such industrial processes include the latency, data transfer rate and connection reliability.

In addition, it is crucial to define optimal methods for supply, factory process and product delivery, and assembly logistics management that would facilitate improved efficiency, scalability and adaptability while maintaining low supply chain maintenance and investment costs. In this research direction, Blockchain has emerged as a key technology enabler for decentralized quality verification of different processes such as the supply, production and end-product logistic chain. This information can be used for boosting the logistic chain and production efficiency, for more accurate monitoring of logistic chain quality, and for fault tracking and fair revenue sharing between stakeholders. The examples include the verification of supply material origins, conditions during transport and storage, storage time, mapping supply materials to end products, monitoring the factory process, end product, identification and electronic assembly guidance at the manufacturing site. Therefore, the integration of these two enabling technologies can provide various meaningful opportunities to manage the overall industrial processes value chain in an optimized, efficient and secure manner.

### B. OUR CONTRIBUTION

Our main contributions in this paper are as follows:

- We propose a conceptual blockchain-edge based framework for industrial IoT applications.
- We formulate the workflow of the proposed framework and identify the key technological requirements.
- We analyze the feasibility of our proposed framework by evaluating the performance and comparing the results with existing work.

### C. ORGANIZATION OF THE PAPER

The rest of the paper is organized as follows: Section II presents the state of the art related to the blockchain and edge computing for IIoT. Section III provides an overview of the

proposed BlockEdge framework together with an industrial use case and process workflow mechanism. We elaborate the key technological requirements for the proposed framework in Section IV. The performance evaluation of the proposed system is given in Section V for both cases, i.e. with and without blockchain. We provide a discussion and future directions in Section VI and conclude the paper in Section VII.

## II. BACKGROUND AND RELATED WORK

### A. BLOCKCHAIN FOR IIoT

Industrial Internet or Industrial Internet of Things (IIoT) is the latest paradigm shift of industrial and manufacturing companies by combing the digitization of industry with the proliferation of the Internet of Things (IoT) [10]. IIoT is widely using in several industrial sectors, including manufacturing, energy, transportation, logistics, healthcare and utilities. An IIoT system usually comprises many IoT devices which are spread across the whole industrial system [11]. These IoT devices collect the massive ambient data which can be used to identify performance bottlenecks in the systems, tackle the system faults efficiently and detect the abnormal operational behaviors of the systems [12]. Such IIoT framework can offer various benefits like efficient quality control, enhanced field service, better system monitoring, traceable supply chains, optimized production and operation cost [13]. For example, authors in [62] presented a blockchain based reputation model in the IoT environment that is capable of building groups of agents based on the values of their reputation capital. The addition of blockchain ensures reliable and certified information about devices/agents in distributed IoT environment.

However, IIoT systems are facing several challenges which need to be addressed before the formal adoption of IIoT across various industries. These challenges include improved resilience, high level of security and privacy, fast adaptability, higher scalability and efficiency on IIoT data collection, improved trust, lower maintenance costs and support for time-critical low latency IoT applications [12]–[15]. Different technologies such as 5G communication, blockchain, smart spaces, Machine Learning (ML), Artificial Intelligence (AI), edge computing can be utilized to address these challenges [16]–[19]. Among them, blockchain and smart contracts are identified as a viable solution to address some of these challenges. The key blockchain properties such as decentralization, immutability, auditability, and fault-tolerance can be used to augment a decentralized IIoT environment [20], [21]. Thus, blockchain and IIoT integration have gained the interest among both academic and industrial level researchers. Various industry solutions and platforms such as COSMOS,[1] Chronicled,[2] Dajie,[3] SmartAxiom,[4] Xage Security,[5] Multichain,[6] Ubirch,[7] Uniquid,[8] Riddle and Code,[9] Slock.it[10] have been developed to address security, privacy, trust and data management issues in IIoT syetems. Therefore, blockchains have been already employed across a wide range of IIoT applications such as smart grids, healthcare, manufacturing, supply chains, food industry, apparel and logistics among others.

IIoT blockchain integration is also facing few technical and operational challenges such as regulatory issues, lack of risk analysis, processing and storage limitations, additional security, privacy and trust issues, high operational cost and processing delays [22]–[24]. Further attention is required to resolve these challenges in order to optimize the IIoT blockchain integration.

### B. EDGE COMPUTING FOR IIoT

Due to increasing demand of low-latency based computations in the massive-scale IIoT networks, the traditional cloud computing-based solutions might not be very suitable for the industrial applications. Edge computing has emerged as a promising technological solution in this case that brings some of the computation, resources and services from the cloud to the edge of the network and closer to the source of the data/end users. This can provide key benefits in terms of ensuring minimum latency, high network efficiency and reliability of the system [42], [43]. Authors in [63] proposed a deep reinforcement Q-learning model based on autonomic computation offloading for mobile edge/fog devices that improves the overall performance in the computations offloading.

Furthermore, authors in [40] presented architectural comparison of various available IoT models which are shown in Fig. 1. The first one in Fig 1 (A) is the traditional cloud based IoT model, where the centralized cloud is responsible for all of the data processing, computation and decision making of various tasks. On the other hand, Fig 1 (B) highlights the edge-IoT model that allows some data processing/computation to be performed at the nearest edge in order to fulfill the low-latency requirements which is essential for some of the delay-critical tasks/processes in the application. The third IoT model given in Fig 1 (C), which introduces the concept of local IoT edge (mist or extreme edge) and allows some of the processing and decision making at the local networks itself (locally on site). This is highly important in various IoT applications to address potential connectivity problems and to restrict the propagation of highly sensitive data outside that particular network. The research in [4] further elaborated these three IoT models in the context of the

[1] https://cosmos.network/
[2] https://www.chronicled.com/
[3] https://www.f6s.com/dajie
[4] https://www.smartaxiom.com/
[5] https://xage.com/
[6] https://www.multichain.com/
[7] https://ubirch.de/en/
[8] https://uniquid.com/
[9] https://www.riddleandcode.com/
[10] https://slock.it/

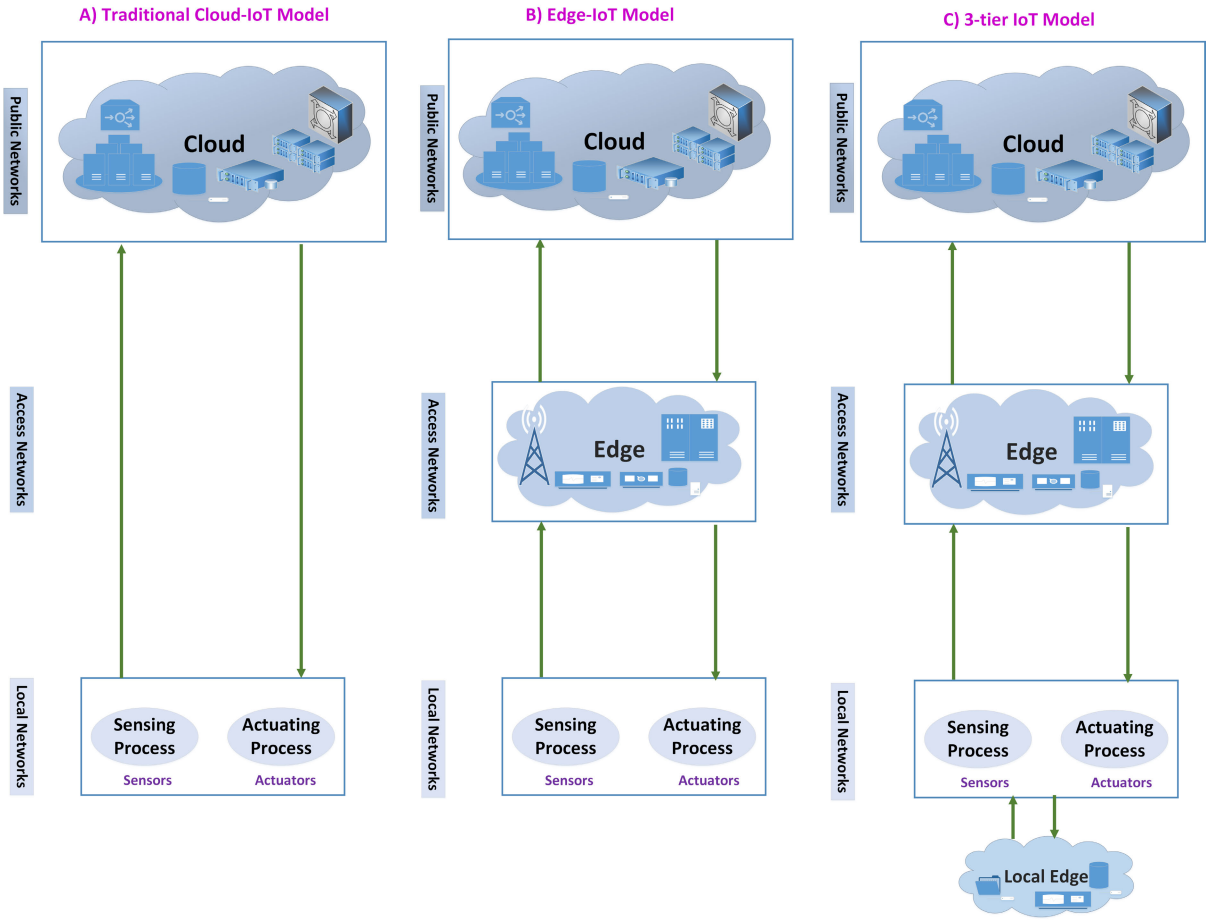


**FIGURE 1.** Various IoT models: (A) Traditional Cloud-IoT model, (B) Edge-IoT model, (C) Three-tier Edge-IoT model.

IIoT application and compared the performance evaluation of the overall system.

The efficient utilization of edge paradigms in various IIoT computing environments has been already addressed in the literature in the following papers: Multiple challenges are appearing in the Industrial IoT in 5G environment towards cyber physical manufacturing systems to achieve high data rate, high reliability, high coverage, low latency [25]. Edge computing has been used to solve the challenges in the aspects of data processing, secure data storage, efficient data retrieval and dynamic data collection in IIoT [26]. In [27], the authors used predictive edge computing for time series of industrial IoT and large-scale critical infrastructure based on open-source software analytic of big data. Moreover, in [28], real-time distributed computing is exploited at network edges for massive-scale IIoT networks. The proposed edge computing gateway for IIoT in [29] uses multiple collaborative microcontrollers (MCUs). Their multi-MCU edge gateways can efficiently perform network management, embedded data collection, and networking communication, thereby considerably reducing the real-time power consumption and improving scalability. The work presented in [30] describe an enhanced, trusted execution environment for industrial IoT edge devices.

### C. BLOCKCHAIN-EDGE INTEGRATION FOR IIoT

Integrating blockchain and edge computing enables several opportunities for the Industry 4.0 applications and addresses the existing shortcomings in the IIoT systems such as better quality of service and experience (QoS/QoE), ensuring distributed trust, enhancing security and privacy, processing/ monitoring/tracking, efficient resource utilization, easier policy/rules applicability and prediction/maintenance, among others. Recently, there are some studies carried out in this direction that highlight the importance and need for the combination of the two technologies. For example, authors in [31], presented a detailed and comprehensive survey about the research opportunities and challenges for the integrated Blockchain-Edge is presented. Furthermore [44] incorporated blockchain with edge computing to provide a secure storage management mechanism for IoT networks.

Authors in [32] described a blockchain based framework to enhance the IoT data quality and reliability through the edge computing environment. Another research in [33]

proposed a blockchain based lightweight framework, 'Fog-Bus', that incorporates various enabling technologies, such as blockchain, edge, fog and cloud. However, most of these existing works are mainly dedicated to find optimal solutions or defining architectural frameworks at the access networks or cloud network. Moreover, since industrial IoT applications require relatively more computations and processing capabilities at the local/device level, it is therefore important to efficiently utilize each of these three networks (i.e. local, access, and cloud) in large-scale IIoT applications. In addition, this paper also discusses the efficient utilization of blockchain technology at various networks in order to take the maximum benefits from its features. In addition, our work provides a comparative performance analysis for both the cases, i.e. when blockchain is incorporated with the IIoT network and without the addition of the blockchain.

## III. PROPOSED BLOCKCHAIN-EDGE FRAMEWORK

Considering the above-discussed need of the blockchain-edge integrated IIoT networks, we have proposed a conceptual Blockchain-Edge framework (BlockEdge) in this section. The framework comprises three key parts, i.e. IoT-Edge networks (local network), Fog networks and Cloud (Global) networks along with the blockchain serving each of the networks. Before describing the actual framework, we took an industrial IoT use case in order to highlight various processes and requirements.

### A. IIoT USECASE: SMART BUILDING CONSTRUCTION

To understand the potential of Blockchain-Edge integration in IIoT, we draw an industrial use case "Smart House Construction", as shown in Figure 2. The building of a smart house requires the frequent involvement of various contractors/sub-contractors that need to work collaboratively to execute different tasks assigned. We assume that the 'owner' of the smart house makes a contract/agreement with the construction company, i.e. the 'Builder'. Moreover, the builder further allocates the various tasks to the number of relevant contractors. These contractors may include: Raw-material provider, interior-design contractor, log-house contractors and IoT/ICT companies, among others. Each of these contractors may further assign the sub-tasks to the different sub-contractors. For example, the log-house contractor will assign sub-tasks to the sub-contractors such as wood harvesting company, transportation contractor and log manufacturing factory, among others.

For the sake of simplicity and ease of the understanding, we only choose one contractor and its associated sub-contractors, i.e. 'Log-House' contractor, as shown in Fig. 2. The logistic and production chain of a log-house construction industry runs into various phases, starting from refining and processing of the trees from a forest until delivery and fitting of manufactured wood-logs at the construction site. This use case portrays a scenario of a system with high requirements for monitoring the quality of raw materials and end-products, and managing the efficiency and reliability of the supply chain, manufacturing and assembly. In the following paragraphs, we discuss the key sub-tasks required in this process.

#### 1) HARVESTING

Harvesting of trees in the forest is done by the harvesting company. The key responsibilities are to guarantee a securely and safely execution of the harvesting process along with monitoring of the forest and weather conditions. Various sensors, actuators, devices deployed locally can monitor and analyze various essential parameters and should take the necessary actions. The information gathered at this phase is required to securely share with other sub-contractors in the process.

#### 2) COLLECTION AND TRANSPORTATION

The goods transportation company will be assigned the task to collect the harvested raw material/trees from the site of the forest and deliver it to the manufacturing factory (to make wood logs). Each of the details, from collection

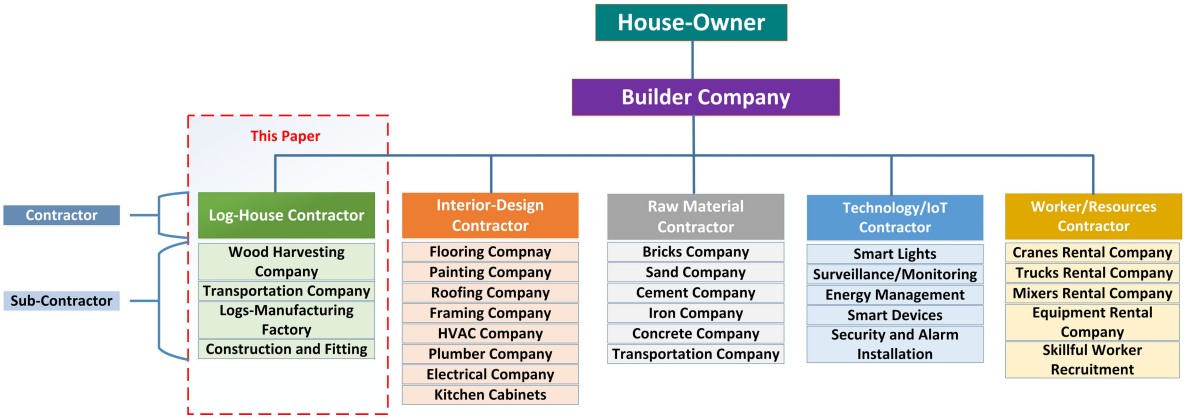


**FIGURE 2.** Smart building construction use case.

to delivery, is traced/monitored by the transportation contractor and shared with the other sub-contractor in the network.

#### 3) MANUFACTURING

The smart manufacturing factory produces the wood-logs from the harvested raw material. Various sensors, devices and machines are required to work collaboratively in this task. This phase requires low-latency based resources/services together with monitoring of each of the operation to ensure the security, safety and efficiency of the overall process. The manufacturing information in this phase will also be shared with the relevant sub-contractors.

#### 4) STORAGE

The manufacturing contractor will store the manufactured wood-logs in the warehouse and provide monitoring features such as appropriate storing conditions. This sub-task must ensure that the wood logs are stored properly until the transportation contractor collects and delivers the manufactured goods from the warehouse to the actual construction site.

#### 5) CONSTRUCTION

This sub-task is performed by the construction company, which will do the required fitting and other necessary work from the manufactured wood-logs. The construction company and the house owner can trace/monitor all the phases through the shared ledger. In case of quality problems, the Blockchain is vital to find the faulty processes that may have caused the problem and appoint the stakeholders responsible for these processes.

### B. REQUIREMENTS OF THE USE CASE

In this section, we highlight some key requirements of the use case that the proposed framework is required to address.

- **Low latency services:** One of the primary requirements of the selected IIoT use case is to ensure the delivery of low-latency services/resources to the required entities in the network.
- **Trusted data sharing:** Since the IIoT use case comprises of several network entities (sensors/devices and stakeholders), one of the crucial requirements of the proposed framework is to ensure the trusted data sharing/exchange among various network entities.
- **Optimized scalability:** Since the IIoT networks comprise of a huge number of sensors/devices, it is required to have better solution of the scalability. In addition, when the blockchain is incorporated in the IIoT networks, the scalability requirements are even more vital.
- **Secure process monitoring/tracking:** The log-house use case will have various tasks and sub-tasks (e.g. Weather monitoring during harvesting, tracking details during transportation of goods and monitoring while manufacturing in the smart factory ) that are required to be monitored and traced in order to ensure the processes are executed safely and securely.
- **Secure offloading:** Since some of the processes in the use case require high computation and data processing capabilities near to the IoT sensors/devices (local level), it is necessary to guarantee that the collected data/resources can be securely offloaded to the assigned high computational node (Fog in our case).
- **Authentication and access control:** The industrial use case will contain heterogeneous sensors/devices that would require secure access to various available resources, thus the lightweight authentication and access control are critical requirements to consider in the system.

### C. KEY NETWORK ELEMENTS

Before discussing the actual proposed BlockEdge framework, we explain very briefly the key network entities along with its role in this section.

#### 1) IoT NODES

This includes a different variety of IoT nodes (i.e. sensors, actuators, RFID tags, devices, camera, location tracking devices, manufacturing equipment/devices) available at the local device level. Usually, these nodes are resource-constrained and perform functionalities such as data sensing and transmitting to the upper level/networks. However, there are some IoT nodes having higher resource capabilities (such as camera, mobile device) that can locally process some of the data, e.g. gateway nodes between the IoT devices and edge nodes.

#### 2) IoT CLUSTERS

By one IoT cluster, we mean that a sub-contractor, i.e. for example, wood harvesting company is a sub-contractor that provides services according to the agreement with the contractor 'Log-house contractor', as shown in Fig. 2. Thus, an IoT cluster represents a sub-contractor that possesses the number of IoT nodes/devices that are required to work collaboratively to execute different assigned tasks/sub-tasks securely.

#### 3) EDGE NODES

Edge nodes/devices possess more resources than the nodes/sensors in the IoT clusters and are available near the vicinity of the IoT devices. The data gathered from an IoT cluster (i.e. sub-contractor) is sent to the respective edge node for further data processing and to ensure the execution of the required low-latency based operations.

#### 4) LOCAL/PRIVATE BLOCKCHAIN

The local blockchain can be seen as the private/permissioned blockchain serving the IoT clusters. Since it requires high computational and processing capabilities to run the local blockchain, we propose to deploy the blockchain at the respective edge nodes for a particular IoT cluster. This can be considered as lightweight blockchain that adds some of

the key features such as trusted data sharing, authentication and access control among others.

#### 5) FOG NODES

These nodes are richer in terms of resources and processing capabilities as compared with the edge nodes. One fog network corresponds to a contractor (e.g. Log-house contractor) in the framework. The fog nodes/devices provide the necessary resources (computation, storage) to the number of associated IoT clusters/edge nodes.

#### 6) FOG/PUBLIC BLOCKCHAIN

This can be considered as the public blockchain running on the fog nodes and share the necessary information about the processes/phases to the other contractors in the use case.

#### 7) CENTRALIZED CLOUD

Centralized/Public cloud are highly resourceful servers/nodes that are able to process higher computational tasks and provide immense storage and processing capabilities.

### D. FRAMEWORK OVERVIEW

#### 1) LOCAL NETWORK

This can also be termed as the "IoT-Edge networks" as it comprises various IoT clusters and each of them is connected to the respective edge nodes, as highlighted in Fig. 3. As mentioned already, the IoT clusters are mainly resource constrained, thus we combine these IoT clusters with corresponding edge nodes ('IoT-Edge' networks) via some high-capable nodes/devices or gateway. Thus, it allows to do some data pre-processing, analysis and decision making locally and fulfill the low latency requirements for local delay-critical operations/phases. For example, the manufacturing sub-contractor in the log-house construction phase requires faster services/resources and decision making/responses to process the harvested raw-material in the smart factory.

We assume lightweight private/permissioned blockchain at the IoT-edge networks which will allow secure and trusted sharing of the required information among different IoT-edge clusters (i.e. among other sub-contractors under the log-house contractor). For example, in the log-house use case, each of the sub-contractors is required to share certain information with every other sub-contractor to keep everyone in this phase aware and updated about the current status of the different processes/sub-processes. Since the IoT cluster is limited in terms of resources to run the local blockchain, associated edge nodes provide the needed resources for deployment of the local blockchain at the local network. As mentioned earlier, the local blockchain deployments will be private/permissioned and thus heavy computational consensus mechanisms such as Proof-of-Work are not essential.

At the local networks, blockchain is a useful tool for supply and product chain monitoring and management. With smart contracts, a sub-contractor is able to verify the supply sources and other stakeholders in the chain, optimize the routes, and, monitor the quality of supplies and end-products throughout the whole value chain. The private blockchain maintains the transaction of each of the processes and help enforcing any new policy for different network entities at

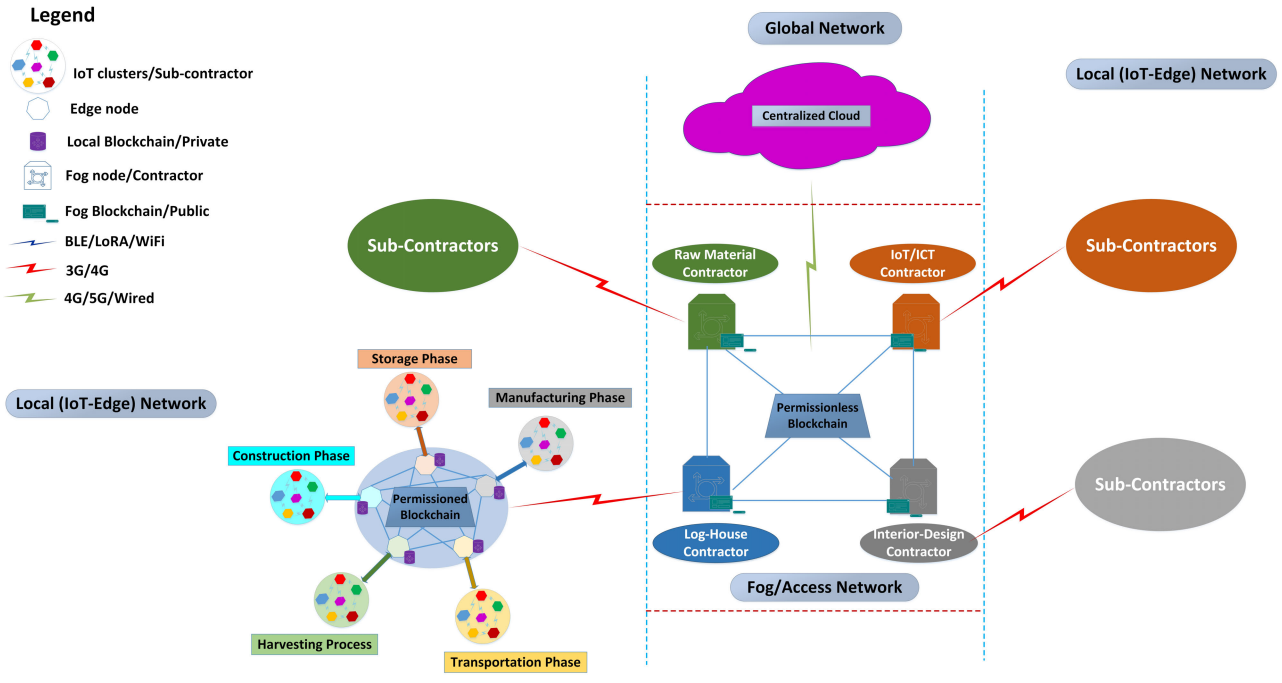


**FIGURE 3.** Blockchain-Edge Framework for Industrial IoT Applications.

the local networks. The local blockchain also ensures the authentication and access control mechanism at the local network, i.e. lightweight authentication of valid sensors/devices, adding/removing a node in the IoT cluster, or providing access rights to authorized nodes once the conditions are fulfilled as agreed in the smart-contract.

In case, the required service/resource is not available at the local networks, the request is forwarded to the fog networks for further data processing and to execute the higher-resource intensive operations. Also, in the case, the required request for any particular service/resources is not latency critical, the edge node will also forward that request to assigned fog networks. On the one hand, industrial environments are typically heavily burdened by radio interference and harsh physical conditions such as extreme temperatures, humidity, etc. On the other hand, remote areas where supply materials, such as harvested logs in our use case, are collected might have weak radio network coverage. Thus, it is important that the local network can, at least for a limited time, autonomously adapt itself to operate without a connection to the public network or even the closest access network base station.

#### 2) FOG NETWORK

The fog network is relatively highly resourceful in terms of computation, storage and processing capabilities compared with local networks (IoT-Edge). By a single fog node, we mean that a contractor, such as log-house contractor or a raw-material contractor which is responsible for monitoring/supervising the corresponding IoT cluster (all relevant sub-contractors) and facilities them with the essential or requested resources/services and functionalities. The fog network is vital in providing elastic resources and services with low-latency access for smart and connected industrial environments. In comparison with the IoT-Edge, fog nodes provide advanced and highly computational functionalities such as AI based data analytics and decision making, predictive security measures and continuous monitoring, etc. Another key functionality at the fog networks is the orchestration/dynamic allocation of various resources that are needed at the various IoT clusters (local networks).

Various fog nodes (contractors) will need to share the necessary information of on-going processes with each other. At the fog network, we assume permission-less or public blockchain and share the limited information in the network. Blockchain on the Fog networks can provide a market platform where the provider can sell resources such as data and computing power, generating revenue for the user. The blockchain at the fog node also maintains the record of all transactions that are carried out by its assigned edge nodes.

#### 3) GLOBAL NETWORK

The global/centralized network can provide the highest resource capabilities as compared with the above two networks. It follows the traditional centralized cloud computing approaches that provide a globally available service platform for applications requiring high storage and computational capacity. The Blockchain here is given the role of supervision of the overall construction processes at the global layer. Transactions occurring between multiple networks and organizations are stored on the Blockchain as permanent records, meaning they could be tracked from any point in the whole supply chain. Blockchain also provides a platform for the trade of physical assert in the form of a transaction or to make a payment when certain conditions are fulfilled. Blockchain recording in the global layer can oversee all the nodes and makes it easier to identify a weak link if something fails or breaks down. Hence, it increases the overall reliability of the system.

In order to efficient and secure execution of various phases in the log-house use case, it is important that all the levels/networks (i.e. local, fog and global) should work collaboratively at each phase of the value chain. For example, the local networks with the resource constrained capabilities can do the limited data processing/computations and decision making for parts of the tasks that requires low latency. Fog node assists the corresponding IoT-edge nodes by providing needed resources and services. For example, it can offer essential high-computational security services/resources to the IoT edge nodes to ensure that enough security measures are available at the local networks to execute various tasks. On top of the fog, global network with higher resources capabilities ensures overall management and supervision of the network. Further steps of the process workflow of the proposed framework are as follows:

The workflow of the proposed framework starts from the local (IoT-edge) networks and continues until the global networks, as shown in Fig. 4. For the ease of explaining the workflow, we only took a single sub-contractor at the IoT-Edge/local networks and one contractor at the Fog networks. The process initiates from the local networks where various IoT sensors/devices available in the IoT cluster generate the data and send it to the closest/assigned gateway node. This node possesses relatively higher capabilities and can do the basic pre-processing and analysis, and is also responsible for forwarding the data/information to the corresponding edge node. The request handler at the edge node further processes the information, stores it at the local database and necessary data is sent to the local blockchain that ensures trustworthy data sharing with the other sub-contractors.

When a service/resource is requested by the IoT cluster from the respective edge node, the request handler will send the request to the appropriate/relevant service module/unit for further processing. After that, it will check whether the requested service or resource is available at the local storage. If the search is successful, then the access rights are verified through the smart contract and the required resource is sent to the edge request handler. In case, the requested resource is not available at the edge (or the available resources at the edge node cannot fulfill the requirements of the requested resources), then the request is forwarded to the fog networks via the fog offloading node.

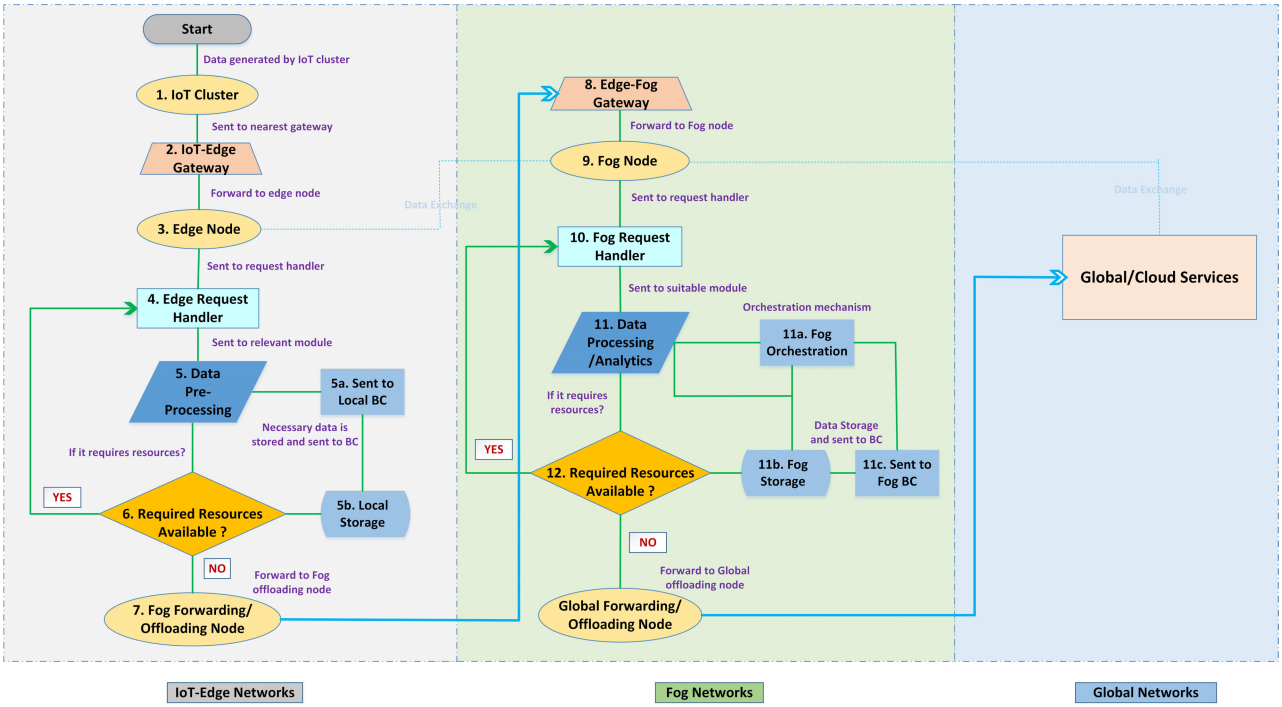


**FIGURE 4.** High-level workflow of the proposed framework.

Based on the nature of the requested resources, the fog request handler forwards the request to the appropriate unit for processing/analytics. It verifies whether the required resource is available there through the fog database. On the successful resource matching, the smart contract at the fog networks verifies the access control rights for a particular edge node. If the requested service is not available, then it forwards the request to the global networks via global offloading/forwarding node. Since global network is the richest in terms of resources, it provides the requested resources to the fog node.

## IV. TECHNOLOGICAL REQUIREMENTS FOR PROPOSED FRAMEWORK

We have identified some of the major technological requirements for a successful deployment of the proposed conceptual Blockchain-Edge framework in the context of the selected use case. Following, we elaborate them briefly.

### A. REQUIREMENTS FOR LOCAL NETWORKS

One of the obvious requirements for the industrial operations at local network is to ensure low-latency-based delivery of the requested resources/services/computations [45]. The inclusion of the edge node with each of the local IoT cluster would address this very requirement by processing the latency-sensitive request near the IoT cluster itself. Another crucial requirement at this network includes a lightweight authentication and access control mechanism for the various low resource sensors/nodes together with establishing the distributed trust among the different nodes and involved stakeholders [46], [47], [64]. These characteristics can be accomplished through the local blockchain in the network. In addition, the access control rights can also be granted through the local blockchain via the smart contract. Secure node bootstrapping would be important at the local networks to ensure secure adding/removing of nodes and to add new features/functions or services at the local layer [3].

As the IoT nodes/devices at the local network are usually resource constrained, one of the important requirements to ensure enough resources to run the local blockchain and provide the needed scalability functionalities [48]. For this purpose, our proposed framework combines IoT nodes/devices (cluster) with the associated edge node to address these scalability issues. The local network consists of low power sensors/nodes and actuators connected together to offer various industrial services, such as sensing and collection of raw data and pre-processing of the data. One of the key requirements of the local networks is to provide uninterrupted and secure connectivity among various nodes and devices. There are several short-range radio communications technologies available such as Bluetooth Low Energy (BLE), ZigBee, Z-Wave, Near Field Communication (NFC), etc. The use of a particular technology depends on the requirements in that specific industrial process or phase [49], [50]. Table 1 summarizes the impact of the key requirements in the different networks.

Since the local network is very restricted in terms of processing, computation and storage, the role of virtualization technologies become vital for successful execution of various processes/phases. The requirements of various local IoT clusters such as gathering raw data and addition/removal of nodes,

**TABLE 1.** Key technological requirements in Blockchain-Edge systems.

| Requirements | Description | Local Networks | Fog Networks | Global Networks |
|---|---|---|---|---|
| Latency Requirements [4], [31], [40], [45] | Fulfill the latency requirements at each network | Low Latency | Low/Medium Latency | High Latency |
| Security and Privacy [1], [3], [22], [41], [67] | Ensure secure communication at each layer in the industrial process | Lightweight Authentication, Secure Bootstrapping | Intrusion Detection/Prevention Systems (IDS/IPS), AI Based Security | End-to-end (E2E) security, Secure Tunneling |
| Trust Management [30], [31], [46], [47], [64] | Ensure distributed trust for various network elements | Distributed Trust among Nodes/Devices, Secure Bootstrapping | Distributed trust among various stakeholders | Business trust models |
| Virtualization [40], [51], [58] | Availability of virtual functionalities/services in the required phases | Lightweight Virtualization, Unikernels, Containers | Hypervisors, Containers | Virtualized Network Functions |
| Standardization efforts | Drafting the standards and regulations of enabling technologies | IEEE 802.15.4, ISO 18000-7 | IEEE P1935, ETSI MEC ISG | IEEE P2301, IEEE P2302, IEEE P2303 |
| Interoperability [13], [24], [59], [65] | Ensure compatibility between different devices/platforms at various phases | Devices/Syntactic Interoperability | Between Fog and Local Networks | Semantic and Platform Interoperability, |
| Scalability [24], [31], [48] | Adopt the scaling of devices/nodes at different phases | Secure Bootstrapping mechanism | Cloudlets Activation Schemes | Horizontal and Hierarchical Scaling, Three-Axis Scaling, Data Centricity |
| Offloading [29], [31], [48] | Offloading of functions/computations and data at various layers | Local offloading to edge nodes | Fog offloading | Data/Resource offloading using key enabling technologies |
| Storage [14], [23], [44] | Storage capabilities needed at different phases | Local Devices Storage (gateway nodes and edges) | Fog nodes/servers | High Data Centres/Public Clouds |
| Resources Computations [19], [40], [57] | Resource/Computational capabilities needed at different phases | Restricted/Limited Capabilities | Higher capabilities | Fully Cloud resources |
| AI Utilization [34], [53], [54], [55], [56] | Intelligent automation of various processes at each layer | Lightweight Edge Intelligence | Fog training models | Overall network intelligence |

among others, are dynamic and are likely to change over time. Thus, one of the key requirements at the local networks is to deploy/implement a microservices framework for dynamically changing a population of sensors/nodes and to allocate the available resources in an improved and optimized manner. Docker Swarm, Google Kubernetes and Apache Mesos are some of the well-known and frequently used technologies for the deployment of microservices [51].

Another important requirement is the implementation of smart contracts in the Blockchain to automate various processes in the framework. For example, it should notify certain events to relevant stakeholders, e.g., status of the transported goods and manufactured products, and start and end of the delivery of a manufactured product [52]. In addition, automatic verification of the final product description with respect to initial logs related to data and origin of the product should be stored and notified in case suspicious security related actions occur to an auditing entity. The functions in the smart contracts can be activated when certain conditions are met, for instance, the release of the payment when goods are transferred. As the framework includes IoT devices that need to share information, we need the Blockchain to have higher throughput and lower latency, i.e. create new blocks in less time without compromising the security. Table 1 summarizes some of the probable ways to tackle with various requirements at the different layers.

### B. REQUIREMENTS FOR FOG NETWORKS

The fog node manages the assigned set of IoT-edge networks and is responsible for providing the necessary services/resources. Since the fog network will provide the resource orchestration mechanism along with the intelligent monitoring functionalities for the local IoT clusters, it is therefore, important to deploy AI/ML based approaches at the fog node [53]. For example, to ensure predictive security measures, ML based security model training and validation is crucial at the fog networks. Most traditional ML based

algorithms are mainly based on centralized training models and are not suitable for edge/fog [34]. Some of the popular training approaches in this direction that may be useful for fog nodes can be transfer learning and knowledge distillation [54], [55]. In addition, to ensure the privacy protection and single point of failure at the fog networks, federated learning emerges as one of the promising solutions for the fog based IIoT networks [56].

The fog network provides optimized resources to the involved local participants and, therefore, it should offer dynamic resource allocation, scheduling and offloading functionalities [57]. The fog network would also utilize the virtualization technologies to provide efficient allocation, provisioning and sharing of resources/services [58]. Furthermore, mobility management and local awareness at the fog network is essential because of delivery of the required services/resources to the moving users and to the resource constrained local nodes/devices. The other important requirement at the fog network includes the interoperability due to the availability of highly heterogeneous environment which contain a diverse set of service providers/entities with different devices/nodes requiring a different set of communication and networking requirements [59], [65]. Since we have proposed a public blockchain at the fog, it is therefore, crucial to define what kind of restricted/limited data can be shared with the other fog-nodes (contractors).

### C. REQUIREMENTS FOR GLOBAL NETWORKS

As the global layer deals with providing powerful services and capabilities, it, therefore, demands a higher set of resources for computation, storage and processing. Considering our log-house construction use case scenario, the main goals of the global layer are to handle, manage, and supervise the overall industrial process, manage and assist the required storage and other resources to execute the defined process, and provide secure availability and accessibility of intensive resources. One of the key requirements is to have secure connectivity of the global layer with the other levels in the system (i.e. local and fog). The global layer also requires monitoring the overall transaction activities for various industrial processes using Blockchain and should be able to store detailed records at the cloud platform. Moreover, this layer would need strong authentication, authorization and access control mechanisms to assure the secure accessibility of various services/information by the different stakeholders in the network.

What is more, the global layer can be categorized as a giant logistics platform for data and a big number of transactions occurs in the form of processing and sharing of the data. Data from the local and fog network enters into the cloud (global networks) and can be further processed, computed and accessed by other authorized stakeholders. At last, the data will either be returned to the network or stored at the global networks to re-use it at a later date. The current trend of moving most of the network services will also fuel the idea of moving mission critical processes to the cloud (global layer). However, the global layer has to support features such as accountability, reliability, compliance, security, verifiability, auditability and acceptance of liability for these mission critical processes. In other words, these processes need secure supply chain mechanisms. Every step in such a supply-chain has to be verified in real-time. If something goes wrong, it should be possible to identify what went wrong and who is accountable. Blockchain can be used as an ideal platform to satisfy these requirements because it can store everything that happens to data and share the information with relevant systems or persons.

## V. PERFORMANCE EVALUATION

In this section, we evaluate the performance and efficiency of our proposed IIoT framework and compared it with the existing IIoT models without a blockchain [11]. To realize the full potential of IoT edge computing and fog for real-time analytics together with a centralized cloud, we considered three key network performance factors, i.e. latency, energy consumption and network utilization. We have also analyzed how the addition of the blockchain in the IIoT model (proposed) affects the overall performance of the IIoT network.

### A. PERFORMANCE METRICS

We measure the performance and resource efficiency of each of the three IIoT networks (i.e. local/IoT-edge network, fog network and global network) presented in [11], [40]. The key performance factors, which are considered vital while analysing the performance of the overall application, are listed below.

- **Latency:** Latency refers to the degree of end-to-end delay between the time a transfer of a data stream is requested and the actual time when the requester starts to receive data.
- **Power consumption:** The power consumption due to the effects of data forwarding, computation, and data storage at each network layer. The power consumption of the overall network can be expressed as:

$$P_T = P_L + P_F + P_G, \tag{1}$$

  where $P_C$, $P_E$ and $P_L$ correspond to the total power consumption at local, fog and global layers, respectively. It includes both processing and communication power between the nodes.
- **Network Usage:** The network usage can be referred to as the utilization of each of three network layers in the IIoT application. It can also measured as the number of packets (KB) that are transmitted across the communication network. The network usage increases with the increase of the number of the data processing and network devices.

### B. SIMULATION ENVIRONMENT

There are a number of simulation tools available in the literature to measure the performance at the cloud, but in the case

**TABLE 2.** Simulation parameters for the Blockchain-Edge framework.

| Parameters | Global Networks | Fog Networks | Edge Networks | IoT Node |
|---|---|---|---|---|
| Upstream bandwidth (MBps) | 150 | 75 | 30 | 12.5 |
| Downstream bandwidth (MBps) | 80 | 37.5 | 18 | 6 |
| Storage capabilities / RAM (GB) | 16 | 8 | 4 | 1 |
| Processing capabilities / CPU (MIPS) | 13000-20000 | 8000-11000 | 4000-8000 | 500-1500 |
| Communication latency (ms) | 145 | 45 | 5 | 1 |
| Blockchain Instructions (M) | 20 | 11 | 5 | - |
| Blockchain Processing Power (Idle-Max)W | 20-80 | 12-40 | 1.4-20 | - |

of fog and edge, only a few of them are available. In [35], Fogbed is introduced, which is an extension of the emulator Mininet and allows to simulate fog and cloud testbeds. However, in terms of fog computing aspects, there are some limitations such as scalability, mobility, etc. EdgeCloudSim is proposed in [38] for edge computing environment related IoT applications. With EdgeCloudSim, both computational, network resources and simulation modelling can be measured. One of the main advantages of EdgeCloudSim is the evaluation of performance during the mobility of the nodes but, however, it does not support scalability.

Gupta *et al.* [39] introduced iFogSim simulation tool where resource management modelling and scheduling techniques can be implemented for different IoT based applications. It is based on Java as a tool for the simulation of fog, edge and local networks. iFogSim uses Distributed data flow (DDF) models. The key reason to choose iFogSim for simulation is that it offers a hierarchical structure, which helps to place the application at different layers in the network. Furthermore, it is also the extension of CloudSim simulator along with various additional features such as offering the placement of the application at fog/edge layer or even on the local level. iFogSim allows to simulate real-time IoT based applications, processing in Fog/Edge environment and measure resource and network management metrics such as latency, cost, networking congestion, energy consumption.

We have evaluated the performance using iFogSim for the selected log-house construction use case for the proposed BlockEdge framework and analyzed various performance metrics for the three IoT models presented in [40] for both cases, i.e. when the blockchain is included in the network and when it is not added into the network. Moreover, we compared the obtained results with the existing IIoT models presented in [4] (i.e. research in [4] contains performance analysis of these three IoT models in the context of an industrial use case and they did not consider blockchain in their models).

In Table 2, we mentioned all the relevant simulation parameters taken during the performance evaluation of the proposed framework. With the thorough study of various relevant research papers, we have analyzed that the configuration of each device is application specific and vary according to the requirements of a particular IoT application [68]–[71]. The latency parameters between the devices have been set for the simulation using Traceroute [70]. As we move toward the root of the topology, i.e from Local to the Cloud, the power consumption of the devices gradually increases. Moreover, this research is part of our recent project "Industrial Edge Project [9]" and considering the requirements defined in the selected use case, various parameters are set accordingly. However, in order to draw the comparison, we kept the same values in both the cases when the blockchain is included in the network and when it is not.

Figure 5 shows the high-level design of BlockEdge framework implemented in the iFogSim simulation environment. The simulation of the proposed BlockEdge framework is mainly divided into three key phases. The first phase in the iFogSim allows the deployment of resource constrained nodes and respective edge nodes together with the addition of lightweight blockchain. The data sensed and gathered at the nodes are sent to edge nodes for local processing and decision making. Table 2 presents the key parameters used during the implementation of the BlockEdge framework in the iFogSim. After that, local blockchain provides trusted data sharing with other edge nodes (i.e. sub-contractors). The next phase allows the deployment of Fog nodes which have higher computational capabilities. A single fog node (contractor) is connected with multiple IoT-edge nodes (sub-contractor) and provides necessary resources (processing/storage) and supervision of the local networks. The final phase is the deployment of the cloud that is the highest in resources and responsible for management overall applications. Thus, the implementation design approach of BlockEdge framework is bottom-up, i.e. from local networks to global networks.

### C. RESULTS

We compared the three key performance metrics, i.e. latency, power consumption, and network usage, from both

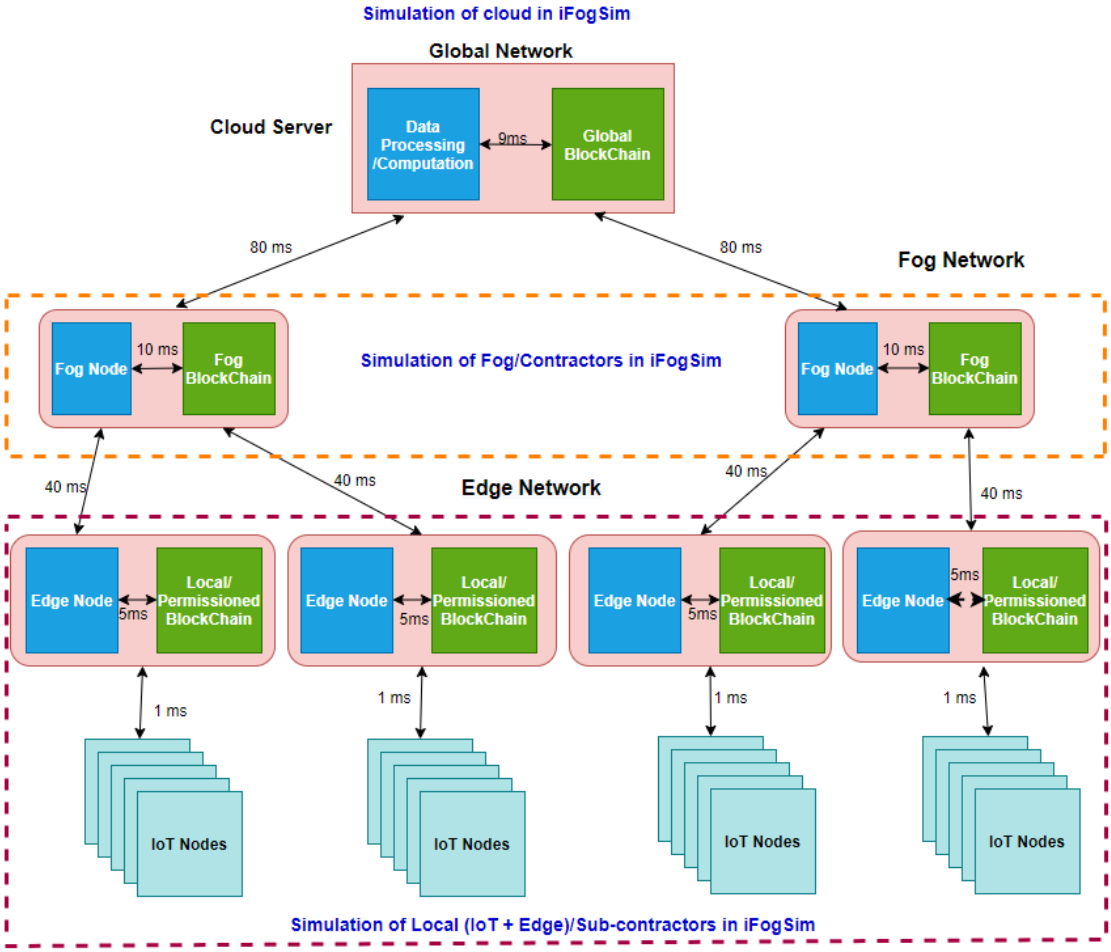


**FIGURE 5.** High level design of BlockEdge framework in iFogSim.

perspectives, i.e when the blockchain is not integrated into the IIoT models and when it is included.

For the sake of the simplicity, we only took one sub-contractor/IoT-edge network (in our case wood harvesting company) and one contractor/access network (log-house contractor). As an example service, we use real-time video-based automated remote controlling of a wood harvester [4]. Various video cameras are deployed at various sides of the harvester record and stream the video to the node which runs the control algorithm based on the video feed and intelligent video recognition. The key factors in this scenario are the latency, for example, there should be minimum delay for the video stream and control messages.

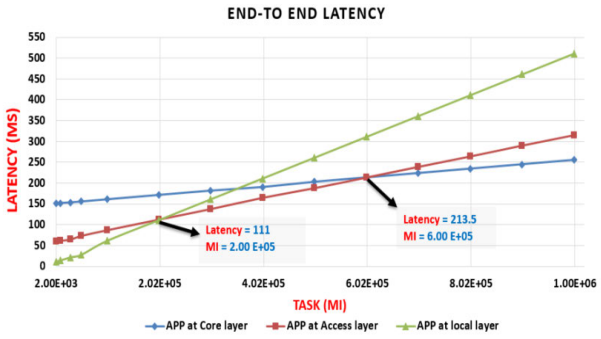


**FIGURE 6.** Latency: Without BlockChain.

### 1) LATENCY

#### *a: WITHOUT BLOCKCHAIN*

Figure 6 illustrates the end-to-end latency (millisecond, ms) vs. complexity of the algorithm (million instructions per task, MI) for different cases, where the control algorithm is placed at each level of the IIoT architecture, when blockchain pre-processing is not used. Local processing shows best results in terms of end-to-end latency with less complex tasks when complexity is below 200000 MI. This is shown in Figure 6, where the green and red curves intersect. If the complexity is roughly between 200000 MI and 600000 MI, the most optimal location for the control algorithm is in the fog server. Respectively, the cloud server is the most optimal location for the control algorithm when the complexity is above 600000 MI.

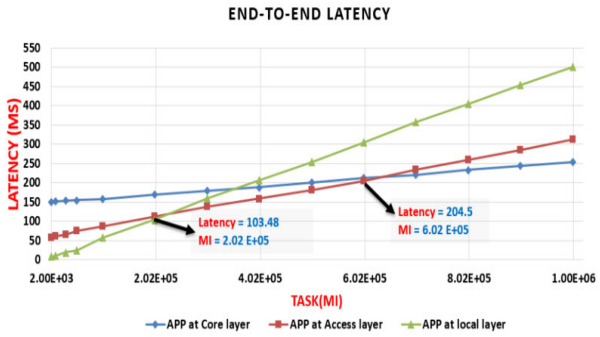


**FIGURE 7.** Latency: With BlockChain.

### *b: WITH BLOCKCHAIN*

Figure 7 illustrates the end-to-end latency (millisecond, ms) vs. complexity of the algorithm (million instructions per task, MI) for different cases, where the control algorithm is placed at each level of the IIoT framework in case blockchain pre-processing is used. Local processing shows best results in terms of end-to-end latency with less complex tasks when complexity is below 250000 MI. This is shown in Figure 7, where green and red curves intersect. When the complexity is roughly between 250000 MI and 625000 MI, the most optimal location for the control algorithm is the fog server. The cloud server is the most optimal location for the control algorithm when the complexity is above 625000 MI. As the blockchain is introduced for pre-processing at each layer, the overall end-to-end latency is reduced, and therefore also the boundaries between the ideal location of running the algorithm are different, as compared to the results in Figure 6.

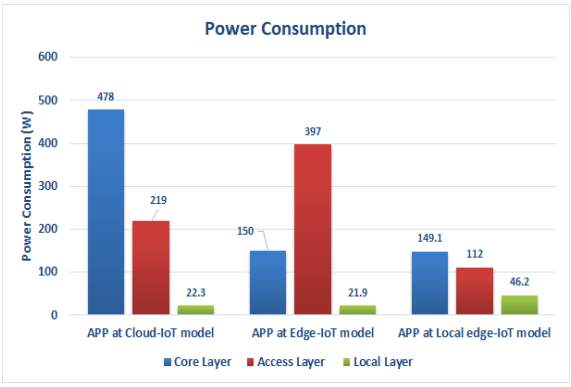


**FIGURE 8.** Power Consumption: Without BlockChain.

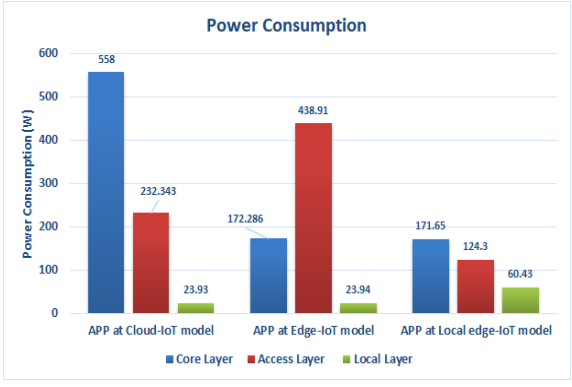


**FIGURE 9.** Power Consumption: With BlockChain.

### 2) POWER CONSUMPTION

### *a: WITHOUT BLOCKCHAIN*

The power consumption on each network of the IIoT models is evaluated with varying the location of the control algorithm, and when blockchain pre-processing is not used, is shown in Figure 8.

The total power consumption of the control algorithm placed on cloud, fog, and Local layers are 719.6 W, 568.9 W and 307.3 W. When the control algorithm is run at local layer, the power consumption is 57 percent lower compared to the case where the algorithm is running at cloud level.

When the processing takes place at cloud, the network activity and computational load imposes 478 W power consumption at the core layer, including both the network and communication activity at the core layer. On the access layer, the imposed power consumption is 219.3 W, which consists of only the network load on the edge layer. On the local layer, the imposed consumption is 22.3 W, which consists of only the network load on local layer. The results exclude the power consumption of the capturing the video as the capturing node is the same node in all scenarios. When the processing takes place at fog, the access layer consumes 397 W (including network load and edge server computation load) power. On the local layer, the consumption is 21.9 W (including local network load). On the core layer, the cloud server remains idle with 149.1 W power consumption. When the processing is placed at local device, it consumes 46.2 W (including network and processing load). In idle mode, core and edge layers it consumes 150 W and 112 W.

From the results in Figure 8, the impact of running the algorithm on different IoT models can be seen clearly. The basic principle appears to be: The further away the video feed is analyzed from the capturing node, the more power is used. This is emphasized due to the scenario's data-intensive design, where the raw video feed needs to be sent to the processing node and the longer the path, the more power is consumed. Comparing with the local capacity-constrained nodes and networks, high capacity nodes and network devices are more power-hungry.

### *b: WITH BLOCKCHAIN*

The power consumption on each level of the proposed framework is evaluated with the varying location of the control algorithm, and when blockchain pre-processing is used, is shown in Figure 9.

The total power consumption of the control algorithm placed on cloud, fog and Local layers are 814.2 W, 635.1 W and 356.3 W. When the control algorithm is run at local layer,

the power consumption is 56.2 percent lower compared to the case where the algorithm is running at the cloud level.

When the processing takes place at the cloud, the network activity and computational load imposes 558 W power consumption at the core layer, which is 80W more than in Figure 8. On the access layer, the imposed power consumption is 232.34 W, and on the local layer, the imposed consumption is 23.9 W.

When the processing takes place at fog, the access layer consumes 438 W, which is 41 W more than in Figure 8, where Blockchain is not in use. The local layer consumes 23.9 W and the core layer consumes 172.2 W.

When the processing is placed at the local device, it consumes 60.4 W (14.2 W more than in Figure 8) and in idle mode, core and edge layers consume 171.65W and 124 W.

From the results in Figure 9, it can be seen that the addition of blockchain pre-processing at each level of the network increases the power consumption and hence the total power utilized in this scenario is higher as compared when the blockchain was not included in the system. This is emphasized due to the data-intensive design scenarios.

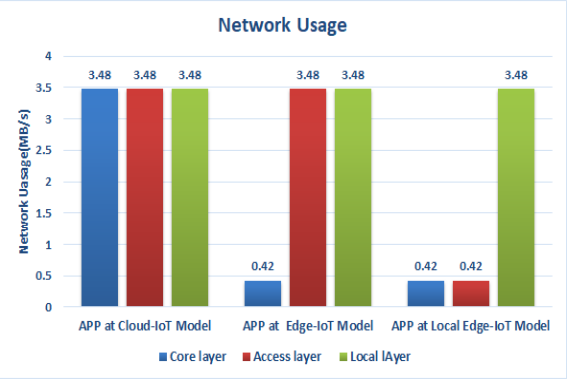


**FIGURE 10.** Network Usage: Without BlockChain.

### 3) NETWORK USAGE

#### *a: WITHOUT BLOCKCHAIN*

The network usage for different IIoT models is shown in the Figure 10, where the number of transferred bytes per send is evaluated in the case when blockchain pre-processing is not considered. In our scenarios, we used a constant bit-rate 1080p video, H.264 compression and 40 FPS causing, together with necessary control traffic, roughly 3.47 MB/s network usage through networking components on the route.

When the processing takes place at cloud, the network utilization taken by each of the three layer is the maximum (i.e. 3.4 MB/s). On the other hand, when the processing takes place at fog server, the network load inflicts to both local and access layers. This is because, in this case, most of the tasks are executing either at the local or access layers, and thus the cloud layer has relatively less network utilization.

When the processing takes place at local network, it utilizes the network mainly on the local layer (i.e. 3.4 MB/s) and rest of two layers are least used, as highlighted in Fig. 10. Local networks process the data locally, so the video feed remains between capturing node and processing node results, only control traffic is used by core/cloud and access layers.

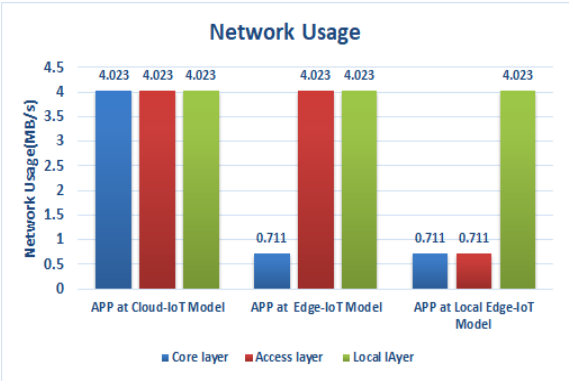


**FIGURE 11.** Network Usage: With BlockChain.

#### *b: WITH BLOCKCHAIN*

Figure 11 describes the network usage when the number of transferred bytes per send is evaluated, and blockchain pre-processing is considered.

In Figure 11, likewise in the previous case, the local layer here takes also less network usage compared with the cloud and access layer. However, due to the addition of the blockchain, the overall network utilization is higher than the in previous case. When the processing takes place at access layer, the local and fog network utilize most of the network (i.e. both 4.023 MB/s).

In the case of local network processing, the local layer is the one which utilizes most of the network because of data is processed at the local network (0.71 MB/s), because the network is utilized on other processing node results, only control traffic is used by core and access layers, as shown in the Fig. 11.

### *D. RESULT ANALYSIS*

In the above section, we compared/evaluated various performance metrics for the three-tier IIoT model from both perspectives (i.e. with and without inclusion of blockchain). We have analyzed that with the inclusion of Blockchain in three-tier IIoT framework and the latency values are slightly better than the case when without blockchain. Since our architecture combines IoT clusters and edge nodes together (i.e. local networks) and most of the latency-critical processing is done at the local networks. The tasks that require high resource capabilities or are not highly latency-sensitive can be directed to the Fog networks for the required processing. This makes the local network more efficient to process/execute the delay-critical operations for the industrial processes.

On the other hand, the power consumption taken by our proposed framework is little higher than the one without a blockchain. The main reason for the increase in the power

consumption is the addition of blockchain at local and access networks and thus the proposed framework requires high data processing and computation capabilities as compared when the architecture without blockchain. However, this slight increment of power consumption can be acceptable in the massive scale IIoT application because the inclusion of blockchain provides several other promising features for the application such as establishing distributed trust, authentication and access control mechanism, and process monitoring among others. Similarly, with the inclusion of blockchain, we get higher network utilization as compared with the IIoT framework without a blockchain.

## VI. DISCUSSION AND FUTURE DIRECTIONS

Industry 4.0 is expected to transform the existing/traditional ways of handling and managing the industrial and manufacturing processes by making it fully digitized, autonomous and adaptive according to the dynamic requirements. This evolution is going to change the current dimensions of industrial processes which is mainly based on the real/physical world. This will provide meaningful integration of real/physical world into the virtual world which is vital for the vision of industry 4.0 applications to ensure secure, optimized and cost-efficient solutions to various industrial processes. However, this transition will heavily be dependent on the advancements and maturity of the various enabling technologies and supporting communication protocols. In this direction, Edge computing and Blockchain are considered as viable technologies for the vision of Industry 4.0 and are capable to address various shortcomings in the current industrial applications.

This article formulates a framework that combines these two enabling technologies to address some of the critical industrial IoT requirements. Although, for the sake of simplicity, we limit this paper to the log-house use case only, but in general, the proposed framework provides immense opportunities due to its applicability in the various important industrial manufacturing and automation use cases such as supply chain management, smart factories and smart construction etc. In addition, this article emphasizes the need of blockchain technology in the existing IIoT frameworks to gain several vital features such as trust, decentralization and secure data processing. The local and fog networks in our framework fulfill the essential latency criteria required for the securely execution of the various industrial/construction processes.

Furthermore, the performance of the proposed framework is evaluated and compared with the existing available IIoT models without inclusion of blockchain. The evaluation results obtained in this paper can clearly provide useful analysis and insights into how these both technologies (blockchain and edge) can efficiently be incorporated without compromising the overall network performance in the whole value chain. This work can be used as a foundation for the future research, while including/considering various other enabling technologies in IIoT applications. For example, one of the potential future work for this research will be to integrate the SDN into this BlockEdge framework and a similar evaluation method can be acquired to analyze the impact on the overall network performance.

The successful deployment/implementation of the BlockEdge vision depends on strong solutions for various key requirements discussed in this article. From a business perspective, the challenging task would be to draft the regulations/rules and standards which are acceptable by all involved stakeholders such as the service providers, network operators, developers, manufacturers, and customers. Healthy debate will also arise regarding whether it is a safe approach to automating the industries fully. Strong regulations will also be required for the utilization of blockchain in the industry 4.0 application. Following, we discuss some of the potential future directions in the context of this paper.

### A. INTEGRATION OF ARTIFICIAL INTELLIGENCE

The utilization of Artificial Intelligence (AI) for the future IIoT applications will be vital for industrial automation and context-aware real-time decision making. The intelligence at the edge/fog would take a relatively more decisive role in data processing and analytics, allocation of resources and computation as compared to the traditional approaches in the case of the centralized cloud. Various resources, services or functions can be dynamically allocated to a particular node/device/entity based on sensing the particular context. One of the important future research directions will be to define and adjust the level of intelligence needed for various phases/processes, stakeholders and at different networks. In addition, further research is required to explore and analyze whether the existing AI approaches/algorithms used in various fields can completely be mapped for providing intelligence in communication networks. If this is not the case, then we need to find out what modifications are required in current AI algorithms to cope with modern networks requirements. Recently, the concept of federated learning is getting huge attention and can be integrated into the Blockchain-Edge framework to provide intelligent privacy preserving solutions for the IIoT applications containing a huge volume of the data. Another open issue while incorporating AI with Blockchain-Edge based IIoT networks is the training of the AI models. For example, in the case when the IIoT application is running at the centralized cloud, the training of the models can easily be implemented/deployed at the cloud where all the required data and resources are available. However, in the case of the edge/fog, information is distributed over various nodes with limited storage and processing capabilities, which makes it challenging to train the models at the respective edge/fog networks.

### B. INTEGRATION OF RELEVANT ENABLING TECHNOLOGIES

Industry 4.0 applications are expected to benefit from the recent technological advancements. For example, Industry 4.0 combines various enabling technologies such as Blockchain, Edge Computing, VR/AR, 3D printing, SDN,

and NFV, among others, to address mission-critical requirements of the current and future industrial applications. The integration of any particular technology may vary from application to application and according to the requirements or use scenario. The modes and quality of industrial processes and services can be enhanced by efficient utilization of such enabling technologies.

For example, digital twin is one of emerging technology that provides the interaction platform by integrating the physical/real world with the virtual world. The developments in AR/VR further complement and support the growth of digital twin and its relevant use cases. In addition, the network virtualization/softwarization technologies (i.e. containers and virtual machines) play a huge role in the optimization/allocation of various available resources. Therefore, there is a huge future research scope to analyze the integration of these enabling technologies into IIoT to resolve various complex challenges in the industrial phases and to ensure a secure and connected industrial ecosystem.

### C. ADAPTIVE SECURITY, PRIVACY AND TRUST MECHANISM

The future industrial IoT frameworks are going to be complex due to the high demanding services/resources and the integration of various enabling technologies. However, these technological evolutions provide a much wider scope to the adversaries to launch various attacks. Such industry 4.0 applications require a dynamic, predictive and adaptive security management framework that is able to detect and mitigate potential security threats at each of the networks (i.e. local, fog and global). One of the interesting future research area in this direction is to propose a security orchestration mechanism that is able to monitor the security requirements for various available nodes/devices and dynamically fulfills those requirements.

In addition to the adaptive security management mechanisms, the novel distributed and collaborative trust models are required to cope-up with the future complex industry 4.0 applications with a huge number of network entities and various stakeholder's/service providers. With the increasing number of participants in industrial IoT networks, traditional IoT trust models may not be feasible in satisfying/fulfilling trust requirements to all the network entities. Moreover, future research work in this area must also consider the GDPR regulation to ensure proper consideration of the privacy/anonymity and protection of the personal data. For example, the main factors for such risks can be because of decentralization and autonomous nature of industry 4.0 that comprises the huge volume of data acquisition, aggregation, storage and processing.

## VII. CONCLUSION

The current trend in terms of advancements in various promising technologies provides a solid foundation towards achieving the vision of the Industry 4.0. In this context, this paper integrates two of such emerging technologies (i.e. Blockchain and Edge) for IIoT applications to fulfill the essential requirements. Some of these IIoT requirements include; low latency services, distributed trust, security and process tracking/monitoring, among others. We proposed a blockchain and edge based framework in this paper and elaborated it with a relevant IIoT use case. In order to analyze performance of our proposed framework, we performed simulations on iFogSim and compared our results with the IIoT architecture without blockchain capabilities. According to the results, BlockEdge has demonstrated the feasibility of decentralized trust and security management in IIoT environment, which does not compromise the system performance and resource-efficiency.

## REFERENCES

[1] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5G security challenges and solutions," *IEEE Commun. Standards Mag.*, vol. 2, no. 1, pp. 36–43, Mar. 2018.
[2] Y. Sahni, J. Cao, S. Zhang, and L. Yang, "Edge mesh: A new paradigm to enable distributed intelligence in Internet of Things," *IEEE Access*, vol. 5, pp. 16441–16458, 2017.
[3] T. Kumar, P. Porambage, I. Ahmad, M. Liyanage, E. Harjula, and M. Ylianttila, "Securing gadget-free digital services," *Computer*, vol. 51, no. 11, pp. 66–77, Nov. 2018.
[4] M. Ejaz, T. Kumar, M. Ylianttila, and E. Harjula, "Performance and efficiency optimization of multi-layer IoT edge architecture," in *Proc. 2nd 6G Wireless Summit (6G SUMMIT)*, Mar. 2020, pp. 1–5.
[5] R. Beck, "Beyond bitcoin: The rise of blockchain world," *Computer*, vol. 51, no. 2, pp. 54–58, Feb. 2018.
[6] A. Bahga and V. K. Madisetti, "Blockchain platform for industrial Internet of Things," *J. Softw. Eng. Appl.*, vol. 9, no. 10, p. 533, 2016.
[7] A. Stanciu, "Blockchain based distributed control system for edge computing," in *Proc. 21st Int. Conf. Control Syst. Comput. Sci. (CSCS)*, May 2017, pp. 667–671.
[8] M. Isaja, J. Soldatos, and V. Gezer, "Combining edge computing and blockchains for flexibility and performance in industrial automation," in *Proc. Int. Conf. Mobile Ubiquitous Comput., Syst., Services Technol. (UBICOMM)*, 2017, pp. 1–7.
[9] *Industrial Edge: Adaptive, Efficient and Reliable Edge Computing for Industrial Applications (2018-19)*. Accessed: Jul. 4, 2020. [Online]. Available: https://www.oulu.fi/cwc/industrialedge
[10] A. Gilchrist, *Industry 4.0: The Industrial Internet of Things*. Cham, Switzerland: Springer, 2016.
[11] J.-Q. Li, F. R. Yu, G. Deng, C. Luo, Z. Ming, and Q. Yan, "Industrial Internet: A survey on the enabling technologies, applications, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1504–1526, 3rd Quart., 2017.
[12] A. Gurtov, M. Liyanage, and D. Korzun, "Secure communication and data processing challenges in the industrial Internet," *Baltic J. Mod. Comput.*, vol. 4, no. 4, pp. 1058–1073, Dec. 2016.
[13] H. Xu, W. Yu, D. Griffith, and N. Golmie, "A survey on industrial Internet of Things: A cyber-physical systems perspective," *IEEE Access*, vol. 6, pp. 78238–78259, 2018.
[14] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial Internet of Things: Challenges, opportunities, and directions," *IEEE Trans. Ind. Informat.*, vol. 14, no. 11, pp. 4724–4734, Nov. 2018.
[15] M. Liyanage, A. H. Sodhro, P. Kumar, A. D. Jurcut, and A. Gurtov, "Securing the communication of industrial Internet," in *Guide to Disaster-Resilient Communication Networks*. Springer, 2020.
[16] P. Matthyssens, "Reconceptualizing value innovation for industry 4.0 and the industrial Internet of Things," *J. Bus. Ind. Marketing*, vol. 34, no. 6, pp. 1203–1209, Jul. 2019.
[17] Y. Siriwardhana, P. Porambage, M. Liyanage, J. S. Walia, M. Matinmikko-Blue, and M. Ylianttila, "Micro-operator driven local 5G network architecture for industrial Internet," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2019, pp. 1–8.
[18] M. Li, D. Hu, C. Lal, M. Conti, and Z. Zhang, "Blockchain-enabled secure energy trading with verifiable fairness in industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 16, no. 10, pp. 6564–6574, Oct. 2020.

[19] M. Younan, E. H. Houssein, M. Elhoseny, and A. A. Ali, "Challenges and recommended technologies for the industrial Internet of Things: A comprehensive review," *Measurement*, vol. 151, Feb. 2020, Art. no. 107198.

[20] S. Zhao, S. Li, and Y. Yao, "Blockchain enabled industrial Internet of Things technology," *IEEE Trans. Comput. Social Syst.*, vol. 6, no. 6, pp. 1442–1453, Dec. 2019.

[21] K. Zhang, Y. Zhu, S. Maharjan, and Y. Zhang, "Edge intelligence and blockchain empowered 5G beyond for the industrial Internet of Things," *IEEE Netw.*, vol. 33, no. 5, pp. 12–19, Sep. 2019.

[22] J. Sengupta, S. Ruj, and S. Das Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *J. Netw. Comput. Appl.*, vol. 149, Jan. 2020, Art. no. 102481.

[23] X. Wang, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, and K. Zheng, "Survey on blockchain for Internet of Things," *Comput. Commun.*, vol. 136, pp. 10–29, Feb. 2019.

[24] A. Panarello, N. Tapas, G. Merlino, F. Longo, and A. Puliafito, "Blockchain and IoT integration: A systematic survey," *Sensors*, vol. 18, no. 8, p. 2575, Aug. 2018.

[25] J. Cheng, W. Chen, F. Tao, and C.-L. Lin, "Industrial IoT in 5G environment towards smart manufacturing," *J. Ind. Inf. Integr.*, vol. 10, pp. 10–19, Jun. 2018.

[26] J.-S. Fu, Y. Liu, H.-C. Chao, B. K. Bhargava, and Z.-J. Zhang, "Secure data storage and searching for industrial IoT by integrating fog computing and cloud computing," *IEEE Trans. Ind. Informat.*, vol. 14, no. 10, pp. 4519–4528, Oct. 2018.

[27] E. Oyekanlu, "Predictive edge computing for time series of industrial IoT and large scale critical infrastructure based on open-source software analytic of big data," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2017, pp. 1663–1669.

[28] E. Oyekanlu and K. Scoles, "Real-time distributed computing at network edges for large scale industrial IoT networks," in *Proc. IEEE World Congr. Services (SERVICES)*, Jul. 2018, pp. 63–64.

[29] C.-H. Chen, M.-Y. Lin, and C.-C. Liu, "Edge computing gateway of the industrial Internet of Things using multiple collaborative microcontrollers," *IEEE Netw.*, vol. 32, no. 1, pp. 24–32, Jan. 2018.

[30] S. Pinto, T. Gomes, J. Pereira, J. Cabral, and A. Tavares, "IIoTEED: An enhanced, trusted execution environment for industrial IoT edge devices," *IEEE Internet Comput.*, vol. 21, no. 1, pp. 40–47, Jan. 2017.

[31] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated blockchain and edge computing systems: A survey, some research issues and challenges," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1508–1532, 2nd Quart., 2019.

[32] R. Casado-Vara, F. de la Prieta, J. Prieto, and J. M. Corchado, "Blockchain framework for IoT data quality via edge computing," in *Proc. 1st Workshop Blockchain-Enabled Networked Sensor Syst.-BlockSys*, 2018, pp. 19–24.

[33] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When mobile blockchain meets edge computing," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 33–39, Aug. 2018.

[34] I. Ahmad, S. Shahabuddin, T. Kumar, E. Harjula, M. Meisel, M. Juntti, T. Sauter, and M. Ylianttila, "Challenges of AI in wireless networks for IoT," in *Proc. IEEE Ind. Electron. Mag.*, Nov. 2017, pp. 1–12.

[35] A. Coutinho, F. Greve, C. Prazeres, and J. Cardoso, "Fogbed: A rapid-prototyping emulation environment for fog computing," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–7.

[36] M. Etemad, M. Aazam, and M. St-Hilaire, "Using DEVS for modeling and simulating a fog computing environment," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Jan. 2017, pp. 849–854.

[37] A. Khakimov, A. Muthanna, and M. Saleh Ali Muthanna, "Study of fog computing structure," in *Proc. IEEE Conf. Russian Young Researchers Electr. Electron. Eng. (EIConRus)*, Feb. 2018, pp. 51–54.

[38] C. Sonmez, A. Ozgovde, and C. Ersoy, "EdgeCloudSim: An environment for performance evaluation of edge computing systems," in *Proc. 2nd Int. Conf. Fog Mobile Edge Comput. (FMEC)*, May 2017, pp. 39–44.

[39] H. Gupta, A. Vahid Dastjerdi, S. K. Ghosh, and R. Buyya, "IFogSim: A toolkit for modeling and simulation of resource management techniques in the Internet of Things, edge and fog computing environments," *Softw., Pract. Exper.*, vol. 47, no. 9, pp. 1275–1296, Sep. 2017.

[40] E. Harjula, P. Karhula, J. Islam, T. Leppanen, A. Manzoor, M. Liyanage, J. Chauhan, T. Kumar, I. Ahmad, and M. Ylianttila, "Decentralized IoT edge nanoservice architecture for future gadget-free computing," *IEEE Access*, vol. 7, pp. 119856–119872, 2019, doi: 10.1109/ACCESS.2019.2936714.

[41] T. Kumar, A. Braeken, V. Ramani, I. Ahmad, E. Harjula, and M. Ylianttila, "SEC-BlockEdge: Security threats in blockchain-edge based industrial IoT networks," in *Proc. 11th Int. Workshop Resilient Netw. Design Model. (RNDM)*, Nicosia, Cyprus, Oct. 2019, pp. 1–7.

[42] S. Stankovski, G. Ostojic, I. Baranovski, M. Babic, and M. Stanojevic, "The impact of edge computing on industrial automation," in *Proc. 19th Int. Symp. INFOTEH-JAHORINA (INFOTEH)*, East Sarajevo, Bosnia and Herzegovina, Mar. 2020, pp. 1–4.

[43] P. Porambage, J. Okwuibe, M. Liyanage, M. Ylianttila, and T. Taleb, "Survey on multi-access edge computing for Internet of Things realization," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2961–2991, 4th Quart., 2018.

[44] B. W. Nyamtiga, J. C. S. Sicato, S. Rathore, Y. Sung, and H. Y. Park, "Blockchain-based secure storage management with edge computing for IoT," *Electronics*, vol. 8, no. 8, p. 828, Jul. 2019, doi: 10.3390/electronics8080828.

[45] J. Hiller, M. Henze, M. Serror, E. Wagner, J. N. Richter, and K. Wehrle, "Secure low latency communication for constrained industrial IoT scenarios," in *Proc. IEEE 43rd Conf. Local Comput. Netw. (LCN)*, Chicago, IL, USA, Oct. 2018, pp. 614–622.

[46] C. Lin, D. He, X. Huang, K.-K.-R. Choo, and A. V. Vasilakos, "BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0," *J. Netw. Comput. Appl.*, vol. 116, pp. 42–52, Aug. 2018.

[47] T. Wang, H. Luo, W. Jia, A. Liu, and M. Xie, "MTES: An intelligent trust evaluation scheme in sensor-cloud-enabled industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 16, no. 3, pp. 2054–2062, Mar. 2020.

[48] J. Xie, F. R. Yu, T. Huang, R. Xie, J. Liu, and Y. Liu, "A survey on the scalability of blockchain systems," *IEEE Netw.*, vol. 33, no. 5, pp. 166–173, Sep. 2019.

[49] A. Evesti, J. Suomalainen, and R. Savola, "Security aspects of short-range wireless communication-risk analysis for the healthcare application," *Int. J. Intell. Comput. Res*, vol. 5, nos. 3–4, pp. 438–449, 2014.

[50] R. Rondón, M. Gidlund, and K. Landernäs, "Evaluating Bluetooth low energy suitability for time-critical industrial IoT applications," *Int. J. Wireless Inf. Netw.*, vol. 24, no. 3, pp. 278–290, Sep. 2017.

[51] R. Pérez de Prado, S. García-Galán, J. E. Muñoz-Expósito, A. Marchewka, and N. Ruiz-Reyes, "Smart containers schedulers for microservices provision in cloud-fog-IoT networks. Challenges and opportunities," *Sensors*, vol. 20, no. 6, p. 1714, 2020.

[52] R. Azzi, R. K. Chamoun, and M. Sokhn, "The power of a blockchain-based supply chain," *Comput. Ind. Eng.*, vol. 135, pp. 582–592, Sep. 2019.

[53] J. An, W. Li, F. L. Gall, E. Kovac, J. Kim, T. Taleb, and J. Song, "EiF: Toward an elastic IoT fog framework for AI services," *IEEE Commun. Mag.*, vol. 57, no. 5, pp. 28–33, May 2019.

[54] G. Hinton, O. Vinyals, and J. Dean, "Distilling the knowledge in a neural network," 2015, *arXiv:1503.02531*. [Online]. Available: http://arxiv.org/abs/1503.02531

[55] S. Jialin Pan and Q. Yang, "A survey on transfer learning," *IEEE Trans. Knowl. Data Eng.*, vol. 22, no. 10, pp. 1345–1359, Oct. 2010.

[56] Y. Qu, L. Gao, T. H. Luan, Y. Xiang, S. Yu, B. Li, and G. Zheng, "Decentralized privacy using blockchain-enabled federated learning in fog computing," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 5171–5183, Jun. 2020.

[57] X. Gao, X. Huang, S. Bian, Z. Shao, and Y. Yang, "PORA: Predictive offloading and resource allocation in dynamic fog computing systems," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 72–87, Jan. 2020.

[58] J. Luo, L. Yin, J. Hu, C. Wang, X. Liu, X. Fan, and H. Luo, "Container-based fog computing architecture and energy-balancing scheduling algorithm for energy IoT," *Future Gener. Comput. Syst.*, vol. 97, pp. 50–60, Aug. 2019.

[59] P. Bellavista, J. Berrocal, A. Corradi, S. K. Das, L. Foschini, and A. Zanni, "A survey on fog computing for the Internet of Things," *Pervas. Mobile Comput.*, vol. 52, pp. 71–99, Jan. 2019.

[60] T. Qayyum, A. W. Malik, M. A. K. Khattak, O. Khalid, and S. U. Khan, "FogNetSim++: A toolkit for modeling and simulation of distributed fog environment," *IEEE Access*, vol. 6, pp. 63570–63583, 2018.

[61] Z. Zou, Y. Jin, P. Nevalainen, Y. Huan, J. Heikkonen, and T. Westerlund, "Edge and fog computing enabled AI for IoT—An overview," in *Proc. IEEE Int. Conf. Artif. Intell. Circuits Syst. (AICAS)*, Hsinchu, Taiwan, Mar. 2019, pp. 51–56.

[62] G. Fortino, F. Messina, D. Rosaci, and G. M. L. Sarne, "Using blockchain in a reputation-based model for grouping agents in the Internet of Things," *IEEE Trans. Eng. Manag.*, early access, Jun. 14, 2019, doi: 10.1109/TEM.2019.2918162.
[63] M. G. R. Alam, M. M. Hassan, M. Z. Uddin, A. Almogren, and G. Fortino, "Autonomic computation offloading in mobile edge for IoT applications," *Future Gener. Comput. Syst.*, vol. 90, pp. 149–157, Jan. 2019.
[64] G. Fortino, F. Messina, D. Rosaci, G. M. L. Sarne, and C. Savaglio, "A trust-based team formation framework for mobile intelligence in smart factories," *IEEE Trans. Ind. Informat.*, vol. 16, no. 9, pp. 6133–6142, Sep. 2020.
[65] G. Fortino, C. Savaglio, C. E. Palau, J. S. de Puga, M. Ganzha, M. Paprzycki, M. Montesinos, A. Liotta, and M. Llop, "Towards multi-layer interoperability of heterogeneous IoT platforms: The INTER-IoT approach," in *Integration, Interconnection, and Interoperability of IoT Systems*. Springer, Jul. 2018, pp. 199–232.
[66] T. Kumar, V. Ramani, I. Ahmad, A. Braeken, E. Harjula, and M. Ylianttila, "Blockchain utilization in healthcare: Key requirements and challenges," in *Proc. IEEE 20th Int. Conf. e-Health Netw., Appl. Services (Healthcom)*, Ostrava, Czech Republic, Sep. 2018, pp. 1–7.
[67] T. Kumar, A. Braeken, A. D. Jurcut, M. Liyanage, and M. Ylianttila, "AGE: Authentication in gadget-free healthcare environments," *Inf. Technol. Manage.*, vol. 21, no. 2, pp. 95–114, Jun. 2020.
[68] M. I. Bala and M. A. Chishti, "Offloading in cloud and fog hybrid infrastructure using iFogSim," in *Proc. 10th Int. Conf. Cloud Comput., Data Sci. Eng. (Confluence)*, Noida, India, Jan. 2020, pp. 421–426.
[69] I. Sarkar and S. Kumar, "Fog computing based intelligent security surveillance using PTZ controller camera," in *Proc. 10th Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Kanpur, India, Jul. 2019, pp. 1–5.
[70] M. M. E. Mahmoud, J. J. P. C. Rodrigues, K. Saleem, J. Al-Muhtadi, N. Kumar, and V. Korotaev, "Towards energy-aware fog-enabled cloud of Things for healthcare," *Comput. Electr. Eng.*, vol. 67, pp. 58–69, Apr. 2018.
[71] K. S. Awaisi, A. Abbas, M. Zareei, H. A. Khattak, M. U. S. Khan, M. Ali, I. Ud Din, and S. Shah, "Towards a fog enabled efficient car parking architecture," *IEEE Access*, vol. 7, pp. 159100–159111, 2019.
[72] *Traceroute-Print the Route Packets Trace to Network Host*. Accessed: Jul. 20, 2020. [Online]. Available: https://linux.die.net/man/8/traceroute

**TANESH KUMAR** (Student Member, IEEE) received the B.E. degree in computer engineering from the National University of Sciences and Technology (E&ME), Pakistan, in 2012, and the M.Sc. degree in computer science from South Asian University, New Delhi, India, in 2014. He is currently pursuing the Ph.D. degree with the Centre for Wireless Communications Research Group, University of Oulu, Finland. He is also a Research Scientist with the University of Oulu. He has coauthored over 40 peer-reviewed scientific articles. His current research interests include security, privacy and trust in the IoT, edge computing, blockchain, and Industry 4.0.

**ERKKI HARJULA** (Member, IEEE) received the M.Sc. degree in computer engineering and the D.Sc. degree in communications engineering from the University of Oulu, Finland, in 2007 and 2016, respectively. From 2000 to 2014, he was with the MediaTeam Research Group, University of Oulu. From 2008 to 2009, he was a Researcher with Columbia University, New York, NY, USA. From 2013 to 2015, he was with the Center for Internet Excellence, University of Oulu. He is currently a Postdoctoral Researcher and a Project Manager with the Centre for Wireless Communications Research Group, University of Oulu. He is a coauthor of over 50 international peer-reviewed scientific articles on the mobile and IoT systems, edge computing, distributed systems, and energy efficiency.

**MUNEEB EJAZ** received the B.Sc. degree in telecommunication from COMSATS University, Pakistan, in 2009, and the M.Sc. degree from the University of Oulu, Finland, in 2020, where he is currently pursuing the Ph.D. degree with the Center for Wireless Communication. His current research interests include the Internet of Things, cloud, edge, local/extreme edge computing, and blockchain.

**AHSAN MANZOOR** received the B.Sc. degree in computer software engineering from the Ghulam Ishaq Khan Institute, Pakistan, in 2014, and the M.Sc. degree from the University of Oulu, Finland, in 2017, where he is currently pursuing the Ph.D. degree. He is also working as a Blockchain Research Developer with Rovio Entertainment Company. He was a Research Assistant with the Centre for Wireless Communications, University of Oulu. His research interests include blockchain, the Internet of Things, and ubiquitous computing.

**PAWANI PORAMBAGE** (Member, IEEE) received the B.Sc. degree from the University of Nice Sophia-Anipolis, France, in 2010, the M.Sc. degree from the University of Moratuwa, Sri Lanka, in 2012, and the Ph.D. degree in communications engineering from the University of Oulu, Finland, in 2018. She is currently a Postdoctoral Researcher with the Centre for Wireless Communications, University of Oulu. She has coauthored over 40 peer-reviewed scientific articles. Her main research interests include lightweight security protocols, blockchain, security and privacy on IoT and MEC, network slicing, and wireless sensor networks.

**IJAZ AHMAD** (Member, IEEE) received the M.Sc. and Ph.D. degrees in wireless communications from the University of Oulu, Finland, in 2012 and 2018, respectively. He was a Visiting Scientist with Aalto University, Finland, in 2018. From 2018 to 2019, he was a Postdoctoral Fellow with the Centre for Wireless Communications, Oulu, Finland. He visited TU Vienna, Austria, to work with Prof. Thilo Sauter as a Visiting Scientist, in 2019. Since 2019, he has been working as a Research Scientist with the VTT Technical Research Centre of Finland. His research interests include 5G, 6G, 5G security, the IoT, and the application of machine learning in wireless networks. He was a recipient of several awards, including the Nokia Foundation, the Tauno Tönning and Jorma Ollila Grant Awards, and two IEEE Best Paper Awards.

**MADHUSANKA LIYANAGE** (Senior Member, IEEE) is currently working as an Ad Astra Fellow/Assistant Professor with the School of Computer Science, University College Dublin, Ireland. He is also an Adjunct Professor with the University of Oulu, Finland. His research interests include SDN, the IoT, block chain, and mobile and virtual network security.

**AN BRAEKEN** received the M.Sc. degree in mathematics from the University of Gent, in 2002, and the Ph.D. degree in engineering sciences from the Research Group Computer Security and Industrial Cryptography (COSIC), KULeuven, in 2006. She was a Professor with the Erasmushogeschool Brussel, in 2007. Since 2013, she has been with the Industrial Sciences Department, Vrije Universiteit Brussel. She has cooperated and coordinated more than 12 national and international projects. From 2014 to 2017, she has been a STSM Manager with the COST AAPELE project. From 2016 to 2019, she was with the Management Committee of the COST RECODIS project. Her current interests include security and privacy protocols for IoT, cloud and fog, blockchain, and 5G security. She is the (co)author of over 120 publications. She has been member of the program committee for numerous conferences and workshops. She has been a member of the Editorial Board of *Security and Communications* magazine. She has also been member of the organizing committee for different conferences and workshops. Since 2015, she has been a Reviewer for several EU proposals and ongoing projects, submitted under the programs of H2020, Marie Curie, and ITN.

**MIKA YLIANTTILA** (Senior Member, IEEE) received the Ph.D. degree in communications engineering from the University of Oulu, Finland, in 2005. From 2005 to 2010, he was a Professor (pro tem) of computer science and engineering and the Director of the Information Networks Study Program. From 2009 to 2011, he was the Vice Director of the MediaTeam Oulu Research Group. From 2012 to 2015, he was the Director of the Center for Internet Excellence. He is currently a full-time Associate Professor (tenure track) with the Centre for Wireless Communications (CWC), Faculty of Information Technology and Electrical Engineering (ITEE), University of Oulu. He is leading a Research Team and the Director of the Communications Engineering Doctoral Degree Program. He has coauthored more than 150 international peer-reviewed articles. His research interests include edge computing, network security, network virtualization, and software-defined networking. He is also an Editor of *Wireless Networks* journal.