SEC-BlockEdge: Security Threats in Blockchain-Edge based Industrial IoT Networks

Tanesh Kumar*, An Braeken†, Vidhya Ramani*, Ijaz Ahmad‡, Erkki Harjula* and Mika Ylianttila*
*Centre for Wireless Communication, University of Oulu, Finland
†Industrial Sciences Department (INDI), Vrije Universiteit Brussel, Brussels, Belgium
‡VTT Technical Research Centre of Finland
{firstname.lastname}@oulu.fi*, an.braeken@vub.ac.be†, ijaz.ahmad@vtt.fi‡

***Abstract*—Internet of Things (IoT), together with fifth-generation (5G) mobile systems and related enabling communication technologies, constantly contributing for the enhancement in various industrial applications and driving towards the vision of complete industrial automation. In this context, both Blockchain and Edge computing are considered as promising technologies to fulfill the vision and requirements for the future Industry 4.0. The integration of these technologies together with massive scale Industrial IoT (IIoT) applications would be vital in addressing several key challenges related to e.g. latency, scalability and security of data processing and sharing, among others. However, such complex IIoT systems are constantly exposed to security threats from various sources. This paper focuses on identifying the major security challenges in the IIoT blockchain-edge related networks. In addition, some potential security solutions are presented in order to overcome these challenges.**

***Index Terms*—Security; Blockchain; Edge Computing; IIoT; Industry 4.0.**

I. Introduction

The fourth industrial revolution (Industry 4.0) will certainly change the existing dimensions of the industrial processes due to the high-demanding requirements from the customers in the context of the current technological developments. Industry 4.0 will bring the intelligence and digitization in the manufacturing, production, logistics and many other industrial processes. It will provide a connected and automated industrial ecosystem where data analysis and process optimization can be done based on machine learning techniques, and intelligent context-aware and real-time decisions can be made accordingly [1], [2]. The transition towards Industry 4.0 is not very straightforward and bounded with respect to the technological evolutions and developments. Some of the key requirements in IIoT applications are scalability, better performance, resource-saving on higher tiers due to data reduction on lower tiers, and maintaining the security and privacy of overall processes. There are two current trends that help addressing these requirements, i.e Blockchain and Edge computing [3].

On one hand, there is the Blockchain technology, which has been already getting huge attention because of its decentralized and distributed nature and applicability in large number of IoT applications. For example, Blockchain in smart healthcare system has a lot to offer in terms of secure sharing of clinical data, managing Electronic Medical Records (EMR), maintaining medical history, organizing smart billing and payments [4]. Other important applications include the domains of logistics, supply chain management and transportation. The utilization of blockchain in IIoT would enable new features in industrial processes, e.g, smart tracking and monitoring of each phase and sharing of crucial information within the system etc. Security is another significant advantage behind using Blockchain for critical IIoT applications [5].

On the other hand, Edge computing pushes the needed services/functionality and computation to the edges of the network and closer to the user's proximity [6]. Furthermore, 5G, together with Mobile Edge Computing (MEC) will provide ultra-low latency and reliable services which is vital for smart factory and manufacturing industries. Computation, processing and storage at the edge ensure more privacy to the critical information and relieves the burden on core networks and data centers by reducing the amount of data that needs to be transferred outside the edge network. Therefore, edge computing is a potential enabling technology considering the requirements in industrial automation processes. Thus, Blockchain and Edge are well suited for the critical demands of smart manufacturing industries and various IIoT based applications [7]. As these networks would be much more complex than the traditional ones, it requires strong security measures for successful deployments.

Motivation:

The industrial intelligence and automation promised by Industry 4.0 made it necessary to explore various enabling technologies that can address the requirements for this vision. Recent state-of-the-art suggest that research community rank Edge computing and Blockchain as key technological enablers for improving the quality and performance of industrial processes. Each of these two have been integrated separately with IoT for better security and quality services. The integration of both Blockchain and Edge together with IIoT networks will open door for several new opportunities in domain of industrial automation.

Our Contributions and Organization of Paper:

Hence, the core objective of this paper is to study the key security challenges based on an IIoT Blockchain-Edge use case scenario for smart industrial processes. The rest of the paper is organized as follows: Section II presents related work, section III defines the log-house construction scenario as IIoT use case and section IV provides the corresponding Blockchain-Edge framework. Section V and VI discusses the potential security requirements and challenges respectively for

proposed framework and recommend some of the probable solutions. We provide a final discussion in Section VII and conclude the paper in section VIII.

II. Related Work

Today, IoT is considered as a back-bone technology for future massive-scale applications and other enabling technologies can be added on top of it to get the required features/functionalities. This article discusses the importance of Blockchain and Edge computing for smart IIoT systems from the viewpoint of security. Thus, in the following paragraphs, we explain the related state-of-the-art.

A. Blockchain for IoT

An overview is given [8] of the different Blockchain solutions for IoT related to the domains of (1) identity of things and governance, (2) data authentication and integrity, (3) authentication, authorization and privacy, and (4) secure communication. A survey on applications for smart contracts involving IoT is provided in [9] and described how smart contracts facilitate autonomous work flow and sharing of services among IoT devices by providing support for issues like billing, shipping, supply management and e-trading. Blockchain is vital in providing security and privacy solutions to manufacturing and industrial processes as discussed in [5]. However, Blockchain does require more resource-intensive computation for its process execution. To deal with this challenge, a Blockchain based credit-based consensus mechanism for industrial IoT is proposed in [10], which discusses the trade-off between security and efficiency.

B. Edge Computing for IoT

Cloud services are transforming from monolithic architectures towards microservice architectures [11], [12]. This approach brings several benefits over monolithic architectures, including better efficiency, scalability and maintainability. The microservice approach is also very flexible in the geographical distribution of computational tasks, since each microservice can be independently developed, tested, deployed, scaled, operated, and upgraded. Edge computing, brings a new computational tier between the datacenter and local devices [13]. By deploying some service functions to the edge, cloud systems can better serve applications requiring low latency, while at the same time saving computational and networking resources at core networks and datacenters [14].

Strong security measures are vital, not only for edge networks but also for the other connected IoT networks. A comprehensive study on security for edge paradigms is carried out in [15], which discusses vulnerabilities from various dimensions such as from core networks to edge servers and edge devices. Authors in [16] explain the role of Edge Data Centres (EDC) and Cloud Data Centres (CDC) and presented security challenges for three IoT layers, i.e. perception layer, network layer and application layer. In [17], a detailed survey is presented that give insight about various security lapses in edge paradigms.

C. Blockchain-Edge Integration for IoT

IoT is continuously evolving since more than a decade with the addition of new enabling technologies. The inclusion of blockchain and edge paradigms for IoT networks will enhance the performance and quality of services. Recently, there are some studies summarized the important requirements and framework for integration of these technologies with IoT networks [18]. Such systems are expected to be more vulnerable as multiple entities would be involved within the network. As this concept is relatively new, there have not been much explored about the associated security threats. However, some of the security and privacy requirements are mentioned in [19], [20] highlighting that data authentication, data integrity and verifiable transactions among others are crucial for these systems. This paper aims to contribute further in this direction and primarily focuses on exploiting security on various layers for blockchain-edge enabled IoT networks.

III. IIoT Usecase: Log-house Construction

Here, we present a ”log-house construction” scenario as an IIoT use case [21]. This use case comprises of key industrial processes such as monitoring of critical phases, maintaining the record of overall steps, low latency services etc. Following, we have explained the six major operational steps of the selected use case.

Harvesting: This step is meant for collecting the information regarding the harvesting of raw material and related activities. Sensors/actuators and low-power devices will sense, collect and process the gathered information related to the harvested material and utilize the information for other phases.

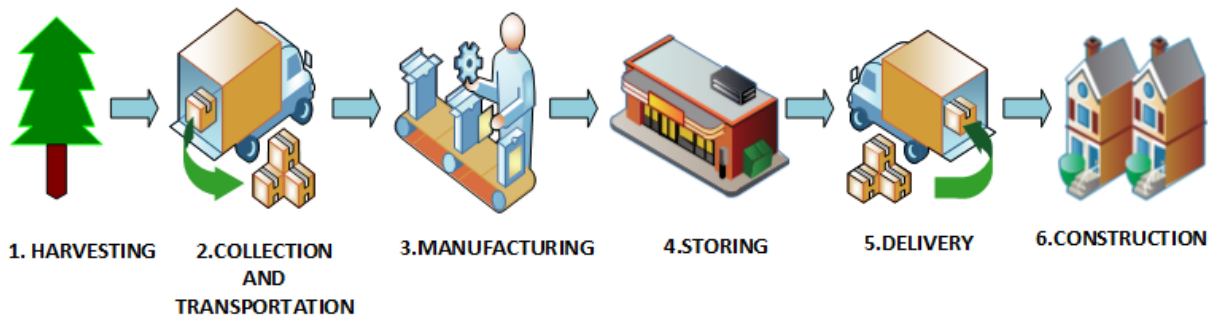

Fig. 1: Log-house construction usecase.

Collection and Transportation: This phase is mainly responsible for collecting the harvested goods and then deliver them to the manufacturing factory through optimized route.

Manufacturing: Wood logs will be manufactured from the raw material, which will be utilized for the construction phase.

Storage: The manufactured wood logs are then carried to a secure location for the storage. Thus, it will require functionalities for dynamic monitoring during the storage.

Delivery: This phase ensures the delivery of stored wood logs to the construction site. It includes the selection of vehicle and route along with monitoring conditions of wood logs placed at the storage.

Construction: Finally, all the material is made available to the construction site and it is used for respective purposes.

IV. Proposed Blockchain-Edge Framework

The efficient utilization of blockchain-edge concepts for optimization of various industrial processes is under investigation in the Industrial Edge Project [21]. Based on IIoT usecase, this proposed framework comprises of four major parts, i.e. local layer, edge layer, global layer and blockchain/ledger. Below we explain each of them briefly:

Local Layer: By local layer, we mean the network of IoT nodes comprising of low-power sensors/actuators with resource-constrained capabilities. This layer is responsible for gathering raw data and processing the information further on the edge and the centralized cloud. The data at this layer will also processed by the Blockchain in order to monitor the local sensors and weather.

Edge Layer: The role of this layer is to provide high computational resources compared with the local layer. In general, the concept of edge/fog is useful as it brings some of the resources and capabilities to the edge from the centralized cloud. It processes the raw data and track the collection and delivery of the material. In addition, Edge together with Blockchain at this layer monitor and provide resources for manufacturing phase.

Global Layer: The global layer presents the highest capabilities based resources, for example, some frequent used information will be stored at edge and rest will be sent to this layer at cloud. The Blockchain at the global layer would need higher storage and capabilities to store overall tracking/monitoring details of each phase.

Ledger Layer: The ledger layer provides transaction specific services for the other three layers: global, edge and local. In the local layer, services provided are mainly related to authentication and monitoring of conditions to check whether conditions are satisfied. In the edge layer, the blockchain can offer services to facilitate the processing, storage and sharing of data coming from different places. Finally, at the global layer, the services offered by the blockchain are focused on overall supervision and trading functionalities.

V. Security Requirements

Before analyzing the security challenges and their potential solutions, we first go through the major security requirements for the IIoT usecase [19], [14], [22]. In the following we mention some of the requirements which the system must follow.

A. Authentication

Our IIoT use case is comprises of several diverse actors such as sensors/actuators, edge devices/servers, service/network providers, and third parties among others. It is important that only correct entities should access or provide the required resources. If not, attackers or competitors would be in the possibility to change or utilize business essential data and leading to dramatic situations. Here, the blockchain can add

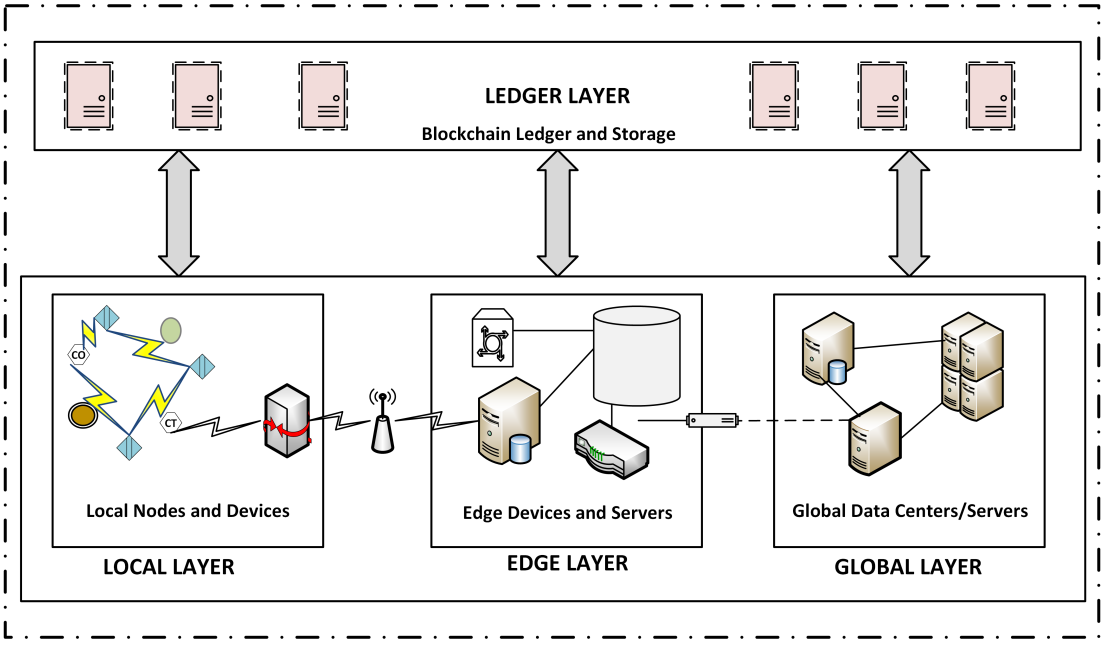

Fig. 2: High level view of BlockEdge Framework.

a smart contract functionality where various entities sign the agreement and accessibility is established following the rules of the contract. In this use case for instance, the companies involved in the collection and transportation process should be the only ones with access to the sensors on the field.

B. Integrity

This BlockEdge framework in the log-house use case run multiple processes which involves data processing and sharing by various stakeholders. There are numerous instances where the data integrity can be compromised. For example, edge devices in certain cases share and replicate the data over other edge servers/centers which may result in data inconsistency, inaccuracy, and loss of critical information.

C. Privacy

In certain cases, companies or users are not willing to share their identity. It is even not desirable that everybody can follow the complete activity pattern of a player, leaking important business related data to the competitors. In particular, if the transactions are stored on a public blockchain, they can be traced by anybody and a complete profile can be built out of it. Therefore, it is very important to include the required privacy enhancing mechanisms, especially at the global layer where trading services are offered.

D. Trustworthy Computation

Along with data integrity, the verification of computations/processing for various transactions within the system is vital to ensure trusted data sharing. In the context of our use case, some of the computation/processing capabilities may be required to be offloaded to an un-trusted node/server and thus it is crucial to keep the valid results/information and the possibility to track the flow afterwards in case of any problem.

E. Availability

It is crucial to ensure the required data is continuously available at each of the layer in the BlockEdge framework to execute various process successfully. For example, the data stored at the edge servers would be vital to improve data availability at local and edge layer.

F. Network Security

The edge layer in log-house use case is certainly the main target point for the adversaries to attack, mainly because of the heterogeneous nature of various devices associated with the edge. The inclusion of blockchain would likely to provide key features at the edge to enhance the security and reduce unnecessary overhead.

VI. Security Challenges in Edge-Blockchain Framework

This section highlights the potential security issues for the proposed Blockchain-Edge framework in the context of the selected use case.

A. Security at local layer

The local layer consists mostly of constrained nodes/devices that are connected together to sense and gather the raw data from the forest/field.

1) Docker/Container based Security Threats:

Challenges: The container can provide lightweight virtualized micro-services which are needed to execute various local processes. Container virtualization is mainly dependent on the characteristics provided by the kernels, thus it requires to have specific attention to the security threats such as spectre and melt down attacks. In addition, with its frequent utilization in the recent usecases, several attacks have been emerged such as image related threats, host and operating system (OS) based vulnerabilities and hardware based threats among others mentioned in [23], [24].

Solutions: There have been various potential solutions drafted for threats at the local layer because of the lapses in the virtualized container. For example, image vulnerabilities can be countered by periodic scanning of image and applications. The verification of trusted as well as registered images is necessary and can be done through cryptographic signatures to ensure the utilization of only trusted images in the process. Related to kernel and OS related threats, it is vital to deploy the management tools which can verify and validate the secure elements for the OS and kernel.

2) Local Nodes/Devices Security Threats:

Challenges: Low power nodes at the local layer are exposed to various adversaries, which are able to alter/modify or steal the necessary information. Due to limited resources, it is prone to attacks such as nodes tampering, malicious code injection, side channel attack, fake node and physical damage [25]. All these attacks end up with compromising the local network and effect the performance and security of the overall IoT system. Therefore, lightweight security mechanisms, in particular key management procedures, are required to protect from all possible threats and to guarantee authentication, integrity and also confidentiality.

Solutions: Pre-installment of key material is the easiest way to initialize the security mechanisms. Based on that, a lot of either symmetric key or public key based mechanisms have been proposed in literature, satisfying a whole range of features going beyond the classical security features like resistance against tampering, anonymity, etc. However, pre-installment of key material requires the existence of a trusted third party (TTP), who becomes in the possession of all the security material and thus makes the system vulnerable of key escrow attacks. Therefore, implicit based certificate schemes like e.g. the Elliptic Curve Qu-Vanstone (ECQV) [26] provide an efficient method to allow the generation of a private-public key pair without a TTP being able to derive the private key itself.

3) Local Communication Security Threats:

Challenges: The short-range communication protocols/technologies at local layer may include: Bluetooth Low Energy (BLE), ZigBee, Near-Field Communication (NFC), and Wi-Fi among others. For example, in the case of

BLE, attacks like relay, MiTM and eavesdropping are some of the common and frequent attacks. In the case of Zigbee, the recent state-of-the-art present several security threats such as replay attacks, jamming attacks and key attacks. NFC suffers with a number of threats including DDoS attacks, phishing, tags related threats among others. Moreover, special care should be taken to devices that are captured by adversaries and where security material is leaked, potentially leading to impersonation attacks or even resulting in a complete loss of the security [14], [27].

Solutions: One of the major solutions to offer resistance against these type of attacks is to install a secure key agreement protocol in order to negotiate a common shared symmetric key to be used for secure communication later on, which is often well defined in the different short-range communication protocols. However, if some addition security requirements need to be established, the classical mechanisms are not sufficient and dedicated protocols as described in literature need to be used. With respect to protection against device capturing, primitives like physical unclonable functions (PUFs) can be used.

B. Security at Edge layer

Here, we discuss the security risks at the network edge which will be critical for IIoT applications.

1) Virtualization Related Threats:

Challenges: The Edge network possess a virtualization platform, which enables the scope of utilizing cloud services and resources to the edge of the network. Virtual machines would play a key role to provide application related services and computations. The lack of secure access control may allow the available edge devices to misuse or modify the information. DoS attacks are quite significant in effecting the resources through malicious virtual machines. The VM itself can be manipulated through various means by malicious entities at the host system [6], [17].

Solutions: In order to resolve the security issues related to virtualization, various approaches have been taken into the considerations. For example, by hardening the hypervisor can relatively ensure the system security and can be installed both on host Virtual Machine (VM) and hypervisor. The other way to counter these attacks is through isolation of security features and controlling the polices for virtual environments. Also, the best practice suggests that the roles of various involved entities should be clearly defined i.e. multiple administrators having different roles and responsibilities would likely govern the virtual environments [17].

2) Edge Devices Related Threats:

Challenges: Edge networks will be comprised of various devices such as gateways, IoT devices and edge data servers which is crucial for both as data consumer and producers. Thus, these devices can be accessed physically by the attacker and can be damaged [17]. Edge data center and servers are considered as a critical target point for adversaries to attack through various means. For example rogue attacks can cause complete loss of control by the administrator as the adversary can install its own fake infrastructure. Once the adversary takes the control, it can manipulate the resources as well as with the connected other devices. The security of edge servers can be compromised by both internal and external attacks [15], [16].

Solutions: Solutions to such threats may include the secure identity management and lightweight authentication for these devices to avoid any tampering or altering the node. Intrusion Detection Systems (IDS) will also be vital to detect and monitor various threats on the edge servers and edge data centers [15], [17].

C. Security at global layer

This probably is the most explored layer compared to the previous two layers. Following, we discuss some of the important challenges.

1) Virtualization Related Threats:

Challenges: The cloud computing utilizes the virtualization approaches like load balancing through dynamic provisioning and for virtualization of cloud services/resources to the other sections of the system, i.e, physical. Though virtualization more security features are added to the cloud by making the security mechanisms simpler for various clusters in the network and by tracing the VMs for potential security risks. However, it also creates several new security threats, for example, VM escape attacks allow the adversary to inject the code on VM and can take the control over the host OS and other VMs. Another very common and frequent attack on VMs is DoS/DDoS that would cause unavailability of the required resources [28], [29].

Solutions: To overcome these security breaches on the global layer, there are a number of solution proposed in the literature. For example, VM patch management can be applied to minimize the possibility of threats at virtual environment as it allows a mechanism to identify, check and test the code. VM image management mechanism is another solution that take care of VM images while bootstrapping or migration of VM. Other security approaches include: VM auditing mechanism and VM migration management [28].

2) Cloud Related Threats:

Challenges:

DoS/DDoS attacks are more frequent at the cloud and considered as the major cause for unavailability of data and service. Consumers are also concerned about their data storage at the cloud as it is not very clear how the data can be protected at the server. Hence the lack of user's control over their data makes it prone to various security threats [29], [30]. Clouds are also vulnerable web and Application Programming Interface (APIs) security attacks. Access control and identity management would get complex in such cloud environment and require significant attention. As cloud services are provided and utilized by multiple stakeholders, it is crucial to have legal agreements between users and other entities about various aspects of services [31].

Solutions: Various encryption (e.g, Fully Homomorphic Encryption, Attribute Based Encryption) based techniques can be applied to ensure the cloud data security, confidentiality and

integrity of users data and access control challenges. Secure development and execution of life cycle is needed for web and APIs as the cloud security alliance suggested number of such recommendations to ensure the API security [31].

D. Security at Blockchain layer

1) Smart Contract Security Threats::

Challenges: The most common attacks while writing the codes in the smart contract are multiple function attack and self destruct functions [9], [32]. The multiple function attack is writing code, which can be easily accessed by third parties and track the product using the product ID. A self destruct() function specifies without any address that the attackers can send all ethers (in case of Ethereum) to the target address using the self destruct (target). Another common attack is timestamp dependency, where the attackers can easily attack the block timestamp, when the smart contract transfers ether based on the timestamp.

Solutions: A better solution for the multiple function attack is to avoid writing the code directly to the external function and to write internal functions which can call the external function. For locking the codes, some keywords like mutex and untrusted should be specified. The solution for protection against the self destruct attack is to specify the exact user address.

2) Node Security Threats:

Challenges: In case of eclipse attack, only one node at particular time can be attacked rather than the whole network. It can change the user's IP address to the attacker's IP address to track the record of log house system. The Sybil attack can target the normal nodes by blocking the communication using Sybil nodes and adversaries can take control over the whole network [33].

Solutions: The IP address can be stored locally to reconnect the same network and to continue the process with the user's address. One key point to control the sybil attack is by using the flood fill measures to check if the nodes are working.

3) Platform based Security Threats:

Challenges: The Decentralized Autonomous Organization (DAO) attack is very common in Ethereum. If the adversary attack the mining node A, it will continue to mine until the mining node A wants complete its task and eventually nodes are compromised. With this threat, the attackers can easily enter into the log house system and can easily change the delivery route or product ID. Another major attack is the re-entrance attack, which is also more common in the Ethereum smart contract. When the attackers call the contract, which is connected to another external contract and also calls back, as can happen in a single transaction, then the attackers can easily attack the sender's address and receive the details of the whole product. The most reasonable attack is then to perform a transaction-ordering dependence. In this attack, attackers can target the transaction price before the user's transaction is complete. There is also much chance to attack the miner [19], [34], [35].

Solutions: Securing the Ethereum platform is the best solution to check the Ethereum based transaction and will also reduce the attack level. Another option is to use the locking system. The best solution for the transaction-ordering dependence is to increase the gas price higher so that attackers are not willing to attack the system.

4) General Blockchain Security Threats:

Challenges: The highest vulnerabilities in blockchain are the 51% probem and private key security threats. The 51% vulnerability can be applied during the consensus mechanism. This attack can easily affect the product information of the system. Private key issues can come by losing the private key by the consent user or giving access to some other person. If the attackers attack the system, then it is not easy to get the private key [36], [37].

Solutions: The 51% vulnerability can be avoided by using the private key or by creating the hybrid blockchain. Saving the private key and also authorize two or more persons can provide a solution.

VII. Discussion

The research related to utilization of the blockchain and edge computing for industrial applications is still at very early stage. This transition towards intelligent and automated industries is directly proportional with evolution and maturity of various enabling technologies. In order to gain success for multiple stakeholders, this vision has to overcome several obstacles in the shape of scalability, reliability, adaptability and security among others. However, the main focus of this paper lies within the security domain. The security threats at each layer are equally critical and must need equal consideration. For example, the lightweight security solutions will be appropriate for the local layer but in the case of edge networks, both lightweight and high computational security mechanisms would be required because of the nature of the edge networks.

Looking forward, the security mechanism in such automated industrial environments would require context-aware based decisions. Thus, machine learning based security techniques would be very significant in future smart industrial systems. In the local layer with limited resources, agent-based lightweight security solutions or "guard nodes" may be required that can contribute to monitoring the local layer and provide the necessary security functionalities from other layers to this layer. Though blockchain and edge provide some security features to the current IoT systems but when these both are integrated together with complex IIoT networks, there may arise new security and privacy challenges which are not explored yet. Hence, along with layered-based security solutions, there is a clear need of end-to-end security mechanism. Moreover, device manufacturers and developers are required to add built-in security and privacy features in the product to decrease the probability of threats to equipments.

VIII. Conclusions

In this paper, we have analyzed various security attacks and their potential solutions based on Blockchain-Edge framework

for IIoT applications. Firstly, a log-house construction scenario is presented as an IIoT use case and respective proposed BlockEdge framework is briefly explained. The paper discusses the vital security requirements crucial for such industrial framework. Furthermore, security attacks are identified at each of the four layers for the BlockEdge framework. In the nutshell, this paper provides an overview of security challenges for IIoT Blockchain-Edge systems and along with discusses various dimensions of its security which are open to explore for research community.

ACKNOWLEDGMENT

This work was supported by Academy of Finland, under the projects: Industrial Edge, MEC-AI, WiFiUS: Massive IoT and 6Genesis Flagship projects (grant 318927). Ijaz Ahmad was also supported by the Jorma Ollila grant.

REFERENCES

[1] E. Hofmann and M. Rsch, "Industry 4.0 and the current status as well as future prospects on logistics," *Computers in Industry*, vol. 89, pp. 23 – 34, 2017.

[2] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5g and beyond," *IEEE Communications Surveys & Tutorials*, 2019.

[3] P. Petrali, M. Isaja, and J. K. Soldatos, "Edge computing and distributed ledger technologies for flexible production lines: A white-appliances industry case," *IFAC-PapersOnLine*, vol. 51, no. 11, pp. 388 – 392, 2018, 16th IFAC Symposium on Information Control Problems in Manufacturing INCOM 2018.

[4] T. Kumar, V. Ramani, I. Ahmad, A. Braeken, E. Harjula, and M. Ylianttila, "Blockchain utilization in healthcare: Key requirements and challenges," in *2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom)*, Sep. 2018, pp. 1–7.

[5] J. Wan, J. Li, M. Imran, D. Li, and F. e-Amin, "A blockchain-based solution for enhancing security and privacy in smart factory," *IEEE Transactions on Industrial Informatics*, pp. 1–1, 2019.

[6] W. Z. Khan, E. Ahmed, S. Hakak, I. Yaqoob, and A. Ahmed, "Edge computing: A survey," *Future Generation Computer Systems*, vol. 97, pp. 219–235, 2019.

[7] M. Isaja, J. Soldatos, and V. Gezer, "Combining edge computing and blockchains for flexibility and performance in industrial automation," in *International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies (UBICOMM)*, 2017.

[8] K. S. M.A. Khan, "Iot security: Review, blockchain solutions,and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395 – 411, 2018.

[9] M. D. K. Christidis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, p. 22922303, 2016.

[10] J. Huang, L. Kong, G. Chen, M. Wu, X. Liu, and P. Zeng, "Towards secure industrial iot: Blockchain system with credit-based consensus mechanism," *IEEE Transactions on Industrial Informatics*, pp. 1–1, 2019.

[11] C. Esposito, A. Castiglione, and K. R. Choo, "Challenges in delivering software in the cloud as microservices," *IEEE Cloud Computing*, vol. 3, no. 5, pp. 10–14, Sep. 2016.

[12] M. Villamizar, O. Garcs, H. Castro, M. Verano, L. Salamanca, R. Casallas, and S. Gil, "Evaluating the monolithic and the microservice architecture pattern to deploy web applications in the cloud," in *2015 10th Computing Colombian Conference (10CCC)*, Sep. 2015, pp. 583–590.

[13] A. Reznik and et.al. (2017, September) Etsi white paper no. 20: Developing software for multi-access edge computing. [Online]. Available: https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp20_MEC_SoftwareDevelopment_FINAL.pdf

[14] I. Sittón-Candanedo, R. S. Alonso, J. M. Corchado, S. Rodríguez-González, and R. Casado-Vara, "A review of edge computing reference architectures and a new global edge proposal," *Future Generation Computer Systems*, vol. 99, pp. 278–294, 2019.

[15] J. Zhang, B. Chen, Y. Zhao, X. Cheng, and F. Hu, "Data security and privacy-preserving in edge computing paradigm: Survey and open issues," *IEEE Access*, vol. 6, pp. 18 209–18 237, 2018.

[16] D. Puthal, S. Nepal, R. Ranjan, and J. Chen, "Threats to networking cloud and edge datacenters in the internet of things," *IEEE Cloud Computing*, vol. 3, no. 3, pp. 64–71, May 2016.

[17] R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," *Future Generation Computer Systems*, vol. 78, pp. 680–698, 2018.

[18] R. Casado-Vara, F. de la Prieta, J. Prieto, and J. M. Corchado, "Blockchain framework for iot data quality via edge computing," in *Proceedings of the 1st Workshop on Blockchain-enabled Networked Sensor Systems*. ACM, 2018, pp. 19–24.

[19] 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 Communications Surveys Tutorials*, pp. 1–1, 2019.

[20] M. A. Rahman, M. S. Hossain, G. Loukas, E. Hassanain, S. S. Rahman, M. F. Alhamid, and M. Guizani, "Blockchain-based mobile edge computing framework for secure therapy applications," *IEEE Access*, vol. 6, pp. 72 469–72 478, 2018.

[21] Industrial Edge. [Online]. Available: {https://www.oulu.fi/cwc/industrialedge}

[22] Y. Yao, X. Chang, J. Mišić, V. B. Mišić, and L. Li, "Bla: Blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3775–3784, 2019.

[23] T. Bui, "Analysis of docker security," *arXiv preprint arXiv:1501.02967*, 2015.

[24] A. Manu, J. K. Patel, S. Akhtar, V. Agrawal, and K. B. S. Murthy, "Docker container security via heuristics-based multilateral security-conceptual and pragmatic study," in *2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT)*. IEEE, 2016, pp. 1–14.

[25] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of things: Security vulnerabilities and challenges," in *2015 IEEE Symposium on Computers and Communication (ISCC)*. IEEE, 2015, pp. 180–187.

[26] V. Qu, "Implicit certificate scheme," *URL: https://patents.google.com/patent/US6792530.*, 2000.

[27] 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, no. 3/4, pp. 438–449, 2014.

[28] S. Luo, Z. Lin, X. Chen, Z. Yang, and J. Chen, "Virtualization security for cloud computing service," in *2011 International Conference on Cloud and Service Computing*, Dec 2011, pp. 174–179.

[29] S. Basu, A. Bardhan, K. Gupta, P. Saha, M. Pal, M. Bose, K. Basu, S. Chaudhury, and P. Sarkar, "Cloud computing security challenges amp; solutions-a survey," in *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*, Jan 2018, pp. 347–356.

[30] Z. Tari, X. Yi, U. S. Premarathne, P. Bertok, and I. Khalil, "Security and privacy in cloud computing: Vision, trends, and challenges," *IEEE Cloud Computing*, vol. 2, no. 2, pp. 30–38, Mar 2015.

[31] M. Ali, S. U. Khan, and A. V. Vasilakos, "Security in cloud computing: Opportunities and challenges," *Information sciences*, vol. 305, pp. 357–383, 2015.

[32] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F. Wang, "Blockchain-enabled smart contracts: Architecture, applications, and future trends," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, pp. 1–12, 2019.

[33] M. Conti, E. Sandeep Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Communications Surveys Tutorials*, vol. 20, no. 4, pp. 3416–3452, Fourthquarter 2018.

[34] J. Moubarak, E. Filiol, and M. Chamoun, "On blockchain security and relevant attacks," in *2018 IEEE Middle East and North Africa Communications Conference (MENACOMM)*, April 2018, pp. 1–6.

[35] X. Wang, X. Zha, G. Yu, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, and K. Zheng, "Attack and defence of ethereum remote apis," in *2018 IEEE Globecom Workshops (GC Wkshps)*, Dec 2018, pp. 1–6.

[36] A. Davenport, S. Shetty, and X. Liang, "Attack surface analysis of permissioned blockchain platforms for smart cities," in *2018 IEEE International Smart Cities Conference (ISC2)*, Sep. 2018, pp. 1–6.

[37] V. Ramani, T. Kumar, A. Bracken, M. Liyanage, and M. Ylianttila, "Secure and efficient data accessibility in blockchain based healthcare systems," in *2018 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2018, pp. 206–212.