An Edge Decentralized Security Architecture for Industrial IoT Applications

Gabriel Portal
School of Technology
Pontifical Catholic University
of Rio Grande do Sul (PUCRS)
Brazil
gabriel.portal@edu.pucrs.br

Everton de Matos
School of Technology
Pontifical Catholic University
of Rio Grande do Sul (PUCRS)
Brazil
everton.matos@edu.pucrs.br

Fabiano Hessel
School of Technology
Pontifical Catholic University
of Rio Grande do Sul (PUCRS)
Brazil
fabiano.hessel@pucrs.br

***Abstract*—The deployment of Industrial IoT Applications are quickly spreading around companies and organizations, mainly involving the use of edge computing. At the same time these applications are improving the production process, they introduces new security concerns that can damage the whole system. Lack of knowledge about security aspects of IoT and designers' current understanding that security techniques applied to cloud computing or embedded systems in general can be adapted to IoT, constitute the main points of failure. IoT security needs new methods and architectures designed specifically for IoT, not adaptations. In this paper, we propose a new edge security architecture for industrial IoT, that combines the concepts of Blockchain and Context-Aware Security. We present how such technologies can be integrated in order to mitigate the security issues related to IoT environments. The proposed architecture was deployed in an Additive Manufacturing Units use case.**

***Index terms*—Edge computing, Industrial IoT, Blockchain, Context-aware security**

I. Introduction

The Internet of Things paradigm (IoT) is not new, and has being explored in a range of use cases and scenarios as industry, health and housing [1]. Nevertheless, the concept still facing a range of challenges in aspects as security, policy standards and constrained resource [2].

The security aspect is emerging as a major challenge due to the increasing number of things connected year after year, and because designers are not very concerned about it, after all, who would be interested in hacking a sensor, a baby monitor or an intelligent traffic light? Neglecting the security aspects related to IoT devices is the biggest mistake made by designers. Another important point to note is that security solutions developed for cloud computing systems are not applicable when it comes to edge devices. Cloud computing security systems are quite complex and have a good level of assertiveness, the same is not true when it comes to the edge. This is due to the limited resources available on edge devices, as processor power and memory size, preventing the use of sophisticated security solutions [3]. IoT security needs new methods and architectures that consider edge device constraints.

Also, IoT manages sensitive and personal data that have a high value for hackers. To an industrial IoT scenario the sensitive information encompasses data about identity, history, documentation and behavior [4]. Such data has a substantial impact over the physical world, once its responsible for monitor and control physical processes. As a result, the security in industrial IoT presents a major role, considering that system failures are able to stop a production line [4], causing monetary loses, or even putting the human life at risk [1].

A range of works already documented critical security faults that were presented in the last years and can affect industrial IoT systems [4] [5] [6]. In June 2010, an Iranian nuclear facility has electrical frequencies altered, causing a fail to the centrifuges, the cause was a worm dubbed Stuxnet, that explored zero-day vulnerabilities [6]. In 2016 a botnet called Mirai infected over 600k IoT devices, intending to perform DDoS attacks and successfully executing over 15,000 [7]. Not only are the examples cited above the only cases of attacks, the literature also reports several other attacks on IoT devices used in different applications of our daily lives. Reports already warn that in the next years the number of IoT devices will have a substantial growth followed by a growing number of system failures and vulnerabilities, hence, leading to a catastrophic state of security and privacy [1] [4] [5]. Industries, cities, hospitals, and connected cars have become major targets for attacks. Can you imagine the consequences of an attack caused by IoT device security breaches, such as environment sensors or traffic lights, on cities like New York, Paris or Tokyo? Or what kind of attack can be accomplished by monitoring your personal data through your smart watch, for example?

To avoid this general state of insecurity and uncertainty, a number of measures are being explored. Policies and regulations as General Data Protection Regulation (GDPR) [8] has being implemented in view of protect personal data from users and legally forcing companies to keep data owners informed about data leaks. Organizations as NIST devote efforts to establish architecture standards aiming to map and develop frameworks to improve the management of data and attack mitigation [9]. Simultaneously, a range of works explores new technologies to be applied to secure IoT devices, as example, approaches as lightweight Blockchains, Context-aware security, virtualization and machine learning has being highlighted as promising [2] [3] [10].

This work has as a major contribution the propose of

978-1-7281-5503-6/20/$31.00 ©2020 IEEE

an edge security architecture that explores a decentralized approach to behavior assertion and attack detection. To achieve the decentralization, the architecture aim to combine lightweight Blockchain and Context-aware security approaches. The Blockchain contributes to the proposed architecture by providing decentralization (edge to edge communication), data integrity and availability. The Context-Aware Security (CAS) provide behavior assertions analyzing context information searching for security anomalies while actions are performed. The context-aware security is used to take decisions based on a collected data set in real time that is safely shared among IoT edge devices via lightweight Blockchain. Each edge device has an instance of the CAS and the device is autonomous to take the decisions based on your context information and the context information shared by the others edge devices. For example, suppose a production line robot receives a production order from a spare part to an equipment. Before submitting the order for production, CAS verifies the authenticity of the production order by processing context information such as: (1) the production history of this part, (2) if this part is in the equipment build of materials (BOM), (3) if the same order has been submitted for other robots at the same time (or at short time intervals), (4) if the person who sent the order is allowed to send it, (5) and if this person is or has been near the equipment that needs the part. After processing these information, the CAS determines if the order is valid or if someone is trying to send a false order (ghost order) to damage the company.

In this paper we introduce the background basis for the proposed architecture, presenting some correlated works on the literature (Section II). Also, the proposed architecture is detailed (Section III). The implementation details are described and discussed to the industrial IoT use case of additive manufacturing units (Section IV). Finally, the paper is concluded, pointing possible next steps (Section V).

II. Background and Related Work

To understand the security architecture proposed in this work and the contribution of this paper to the industrial IoT research scenario, first, the concepts of Blockchain and Context-aware security shall be presented, as well as an overview in some related researches.

The Blockchain has been foreseen as a disruptive technology to secure IoT devices, discussed by previous works as a powerful tool to improve industry management and security, if properly deployed [11] [12]. Technically, the Blockchain is a decentralized, immutable and shared database ledger, able to store data over multiple nodes in a peer-to-peer (P2P) network [3]. The technology operation together the use of elliptic curve cryptography (ECC) and SHA-256 hashing provide a range of security requirements as availability, integrity, privacy and auditability [10] [12]. However, Blockchain technology needs a lot of available memory on the device, which makes it incompatible with the features of edge devices. In order to be able to use Blockchain in edge devices it is necessary to make adaptations, such as storing only the hash keys in the chain, and off-chain data, or lighter consensus algorithms, creating the so-called lightweight Blockchains. The limitation of this type of approach is that there is not a single Blockchain, but several Blockchain versions which in most cases are incompatible with each other. In this work we use one lightweight Blockchain to validate our approach.

The context-aware security (CAS) consists of the use of context information (i.e. information that characterize the state of an object or thing [10]) to infer a security decision. This technique can strength the security of IoT applications, acting as a double check to perform a task or as a decision maker to detect security anomalies [13]. One of the key features of CAS is its ability to use dynamic data to make a decision, as opposed to traditional security methods that mostly use static parameters. The technique characteristic presents an interesting compatibility to IoT applications, contributing with security requirements as authentication, identification and attack detection [13].

Previous works already explored separately Blockchain and Context-aware security architectures to IoT environments [2] [3] [14] [15], however, to the best of our knowledge, there is no propose that combine the two approaches. Giaretta et al. [2] proposed an architecture for Context-aware security on the Fog, defining as an approach of Security-by-contract. In his architecture contracts are defined as a behavior specification of IoT devices, that includes a set of security rules for an expected behavior, hence, the contracts are executed during data exchanges intending to maintain the system integrity.

In [3] Khan et al. performs a survey over Blockchain solution approaches for IoT environments. According to the survey, the technology stands out in providing data authentication, integrity and privacy, highlighting the Blockchain use for secure communications. Protocols as HTTP and MQTT are not secure by design, needing complex security stacks with DTLS or TLS to secure communication. Using Blockchain, such stacks can be eliminated, simplifying the data exchanges and eliminating the need to handle and exchange PKI certificates at the handshake phases.

Gochhayat et al. [14] proposes LISA, a lightweight architecture for context-aware in IoT. The architecture consists of the use of agents to lead the processing of relevant information to the edge, while data and services are allocated in the cloud and accessed by means of webservices. By spread the processing between edge and cloud, LISA provides a reduced overhead between the client and server domain. Hence, providing an efficient decision making to fault tolerance.

In [15] Seok et al. a lightweight Blockchain architecture for Industrial IoT was proposed. The architecture explores different lightweight hashing functions according to the number of transactions to be processed. As a result, the architecture is able to adapt the Blockchain node to heterogeneous devices, enabling a more efficient use of the technology to applications as supply chain and smart diagnostics in Industrial IoT.

The architecture presented in this paper attempt to combine the state of art from approaches presented on some related works. As example, the present architecture explores the use of

contracts and rules similar to the presented in the Security-by-contract provided by [2]. However, in order to supply a gap for context-sharing, we included a Blockchain solution inheriting the security and organizational improvements discussed in [3]. Additionally, our architecture takes advantage from the edge processing model as viewed in LISA [14], however, the context data is also conducted to the edge with the Blockchain, achieving less overhead between client and server domain than the previous discussed approaches.

Additionally, security techniques as Software Defined Networks (SDN) and Network Function Virtualization (NFV) are effective to detect a range of attacks [10]. However, such techniques encompasses a network layer, using centralized and distributed approaches, that aren't designed for new industry trends as decentralized or autonomous organizations [16] [17]. Our architecture aims to provide a decentralized heuristic assertion over the application behavior of distributed and decentralized systems. Thus, being able to detect a range of application level attacks as Sybil or poisoning. A real world example was recently performed by Simon Weckert, that succeeded on poison the Google Maps with 99 second-hand smartphones in a handcart [18].

We recognize that the proposed architecture also inherit some challenges as the deployment in heterogeneous devices, constrained resources, Blockchain vulnerabilities and performance [3] [11]. Nevertheless, such challenges are out of our present scope, fitting the exploration of works as [11] [15] in future efforts. All things considered, the proposed architecture is able to fill some security gaps required for the industrial IoT implantation, as example, a data integrity verification and an edge-to-edge secure communication for decentralized applications [4] [15].

III. Proposed Architecture

The proposed architecture is composed by two core approaches, Context-aware security (CAS) and Blockchain. The CAS provide an intelligent and dynamic model to assert the validity of a given process being executed over a certain environment. As example, given a set of rules, a variable set of information can be inferred and a dynamic result that changes according to the entry and the rules are obtained. The Blockchain provides a secure and unified model to an entity share its context information to other interested entities, also, granting improved integrity of historical and shared data. In our proposed approach, we explore the Blockchain model to decentralize part of the architecture, eliminating the need for retrieve context data in cloud, as needed by other architectures [2] [14].

In other words, the technologies in the architecture are utilized to an edge model, exempting the client/server communication from security mechanisms data. As a consequence, the communication overhead for the security infrastructure is reduced and the bandwidth can be better explored for complex processing. To this architecture, we consider an edge node as a gateway present on IoT environments acting as an intermediate between an individual requesting access to an IoT device. Physically, the edge node can represent a factory floor computer, that receives requests to perform tasks or acquire data from devices.

The edge devices can store security policies that consider historical context and the context from other related edge devices, and evaluate if the behavior of the node comply to such policy. According to the policies established, the architecture is able to detect a range of attacks as Sybil, Spoofing and Denial of sleep [3] [16]. Hence, the proposed architecture is able to provide security to the execution of tasks in a protected resource that is an IoT device. Additionally, the communication between the edge devices is also secured by the cryptography present on Blockchain [3]. As seen in Figure 1 the architecture is distributed over different edge devices, being decomposed in the following modules:

- **Proxy:** A proxy can be defined as an intermediary between clients seeking resources from servers. To our architecture, the proxy acts as a filter responsible for receive the requests from a server to an IoT environments which the architecture is deployed, also known as reverse proxy. The proxy is responsible to manage the requests in the architecture, specifically, receive and redirect to the Context Reasoning module, allowing access to a protected resource or deny case a security anomaly be detected.
- **Context Reasoning:** This module encompasses the procedures to execute the Context-aware security. It receives a request from the proxy, searches for relevant information in the Blockchain node, and applies an inference model (e.g. a set of rules) that processes the context information in a logical security decision. We assume that the context information is already modeled, and is safely produced by an internal module or included inside the requests, due to the purpose of this paper, further explanations can be found in related works [19] [13].
- **Blockchain node:** Each Edge node containing the proposed architecture has a Blockchain node inside, that is responsible for store and provide reliable data to the Context reasoning. Such module includes the Blockchain infrastructure, as consensus algorithms and cryptographic keys management. All Blockchain nodes have a unique identifier and are connected to each other by means of a peer-to-peer connection, that establish an edge communication for context sharing.
- **Protected Resource:** This module represents an IoT device or resource that shall be protected by the proposed mechanism, as example, a 3D printer in a smart manufacturing environment or a smart lock in a home. The protected resource is managed and connected to the edge.

As seen in Figure 2, the modules operational flow can be represented in 6 stages:

- **Stage 1:** The proxy receives a request to access the protected resource from a server or individual, and send to the Context Reasoning.

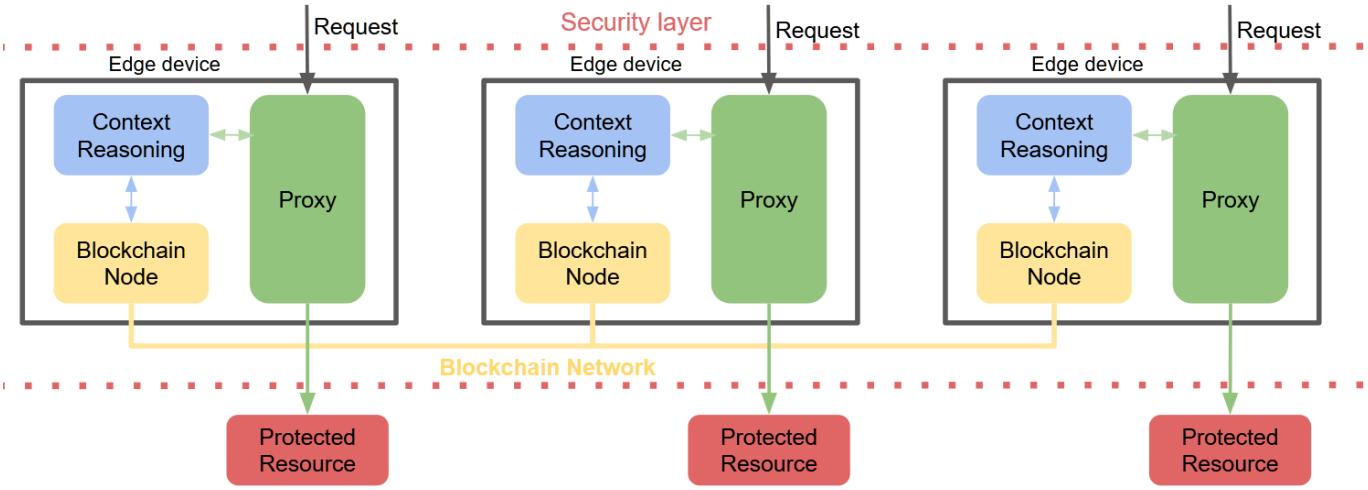

Fig. 1. Proposed architecture.

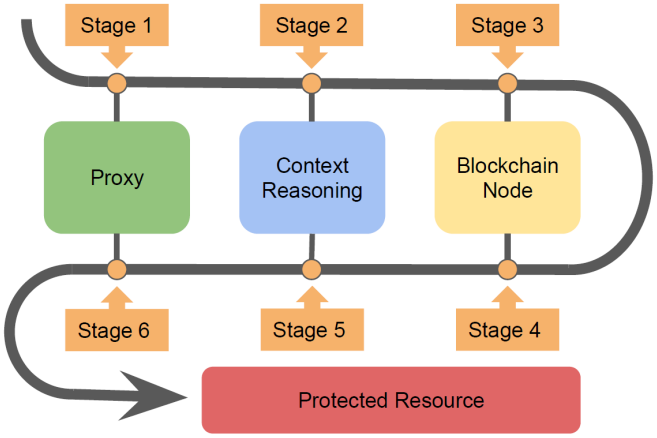

Fig. 2. Architecture operation flow.

- **Stage 2:** The Context Reasoning module send to the Blockchain node the actual status of the IoT environment, also, requiring the information needed to take a security decision.
- **Stage 3:** The Blockchain node add to the Blockchain the context information from the actual IoT environment.
- **Stage 4:** The Blockchain node search for the required information (that can include the context from other IoT environments) and send to the Context Reasoning.
- **Stage 5:** The Context Reasoning infers the information received from the Blockchain node and the current edge node context and take a security decision, sending the result (detected anomaly security or expected behavior) to the proxy.
- **Stage 6:** The Proxy allow or deny the access to the Protected Resource according the decision received from the Context Reasoning.

By means of the described architecture, an extra security layer is achieved. That is, traditional client/server architectures rely on the authentication and authorization provided by assertions on the server side. Whereas, the proposed architecture perform a security verification on the edge. Thus, some security flaws on communications or systems from the server side, should not impact on the physical world.

IV. Use Case and Implementation

The proposed approach was deployed in a real industrial IoT use case. The industrial IoT consists of an initiative that combines IoT devices and manufacturing equipment to redesigns production and sales processes [11]. The use case consists in a set of additive manufacturing units (AMU), each one compose by a network of 3D printers that shall produce spare parts. In each AMU we can have 3D printers with different characteristics that use different materials and, of course, can have different printing costs and printing time. The AMUs are physically located strategically in the country in order to supply the demand in terms of printing costs, printing material, delivery logistics and printing time. In addition, each AMU may be owned by the company or may be from a third party accredited by the company. When a part needs to be replaced, a production order is sent to the company software platform by the company technician. The platform analyzes the order and determines which AMU will print the part, considering the costs and printing time, and the time to deliver the part to the customer [17].

Regarding the security aspects, identify malicious participants on the network can not be considered a straightforward task, as well as the complexity increases according the growing of AMUs [7] [1]. The typical attacks of this type of application are Sybil and Spoofing attacks. Such attacks can have the following results:

- A Spoofing attack between a requesting a print order and an AMU can generate undue printing requests, intending to flood the unit availability and compromise the printing operations.

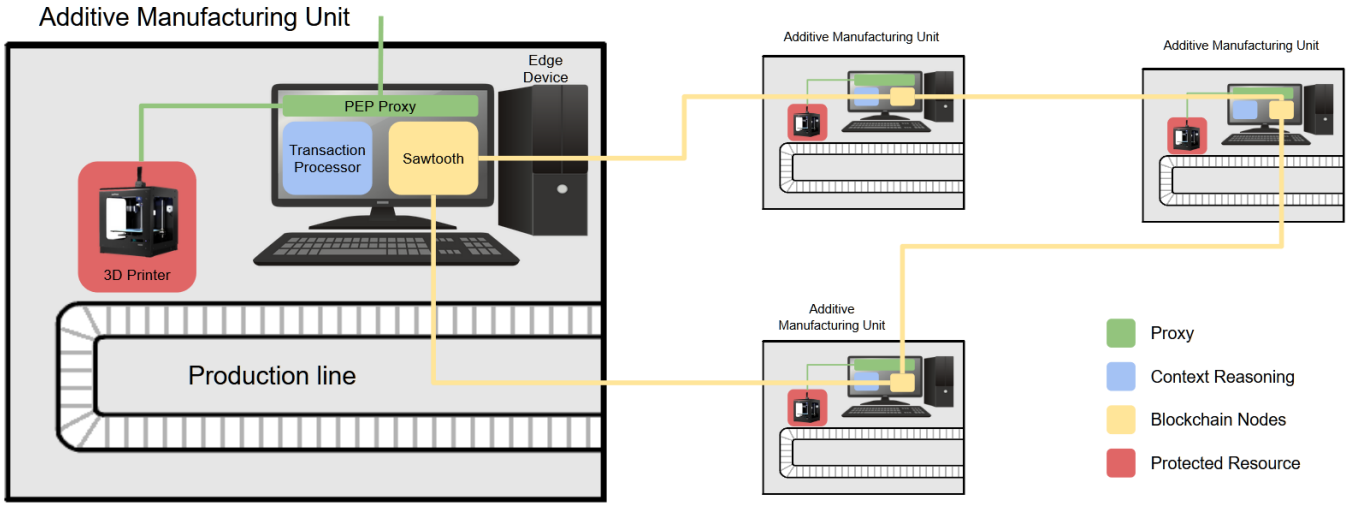

Fig. 3. Architecture use case and implementation.

- A Spoofing attack between a requesting a print order and an AMU can also impersonate an attacker as a unit, hence, isolating the access to the real unit and disabling the printers.
- A Sybil attack can create a ghost AMU that receives valid print requests but does not execute them.

Figure 3 presents the AMU network deployed for this use case. Each AMU is located in a different region of the country (one in the south, two in the southeast, one in the northeast) and each one have a printer connected to an edge device as described in section III. The architecture prevent that requests detected as undue or corrupted be physically executed by the printer, also, identifying ghost units from Sybil attacks [16]. For proof of concept, the proposed architecture implementation uses a software stack that includes FIWARE and Hyperledger tools. Specifically, was utilized the FIWARE [20] Policy Enforcement Point (PEP) Proxy and the Hyperledger Sawtooth [21].

The standard FIWARE PEP implementation enforce the access control to applications using rules created on the FIWARE identity management also called KeyRock. Specifically, it acts as a proxy that receives requests from an entity that need to access a protected resource, verify in the KeyRock if the requester has permission to access such resources, and provides or deny access to the resource. To the implementation of the proposed architecture, a custom PEP implementations is utilized. Such custom implementation adds to the PEP a step that consult the context reasoning for security assertion. Thus, executing the proxy function described in the section III.

The Hyperledger Sawtooth provides to the proposed architecture technological resources to implement both context reasoning and Blockchain node. The Sawtooth is a distributed ledger software that provides a peer-to-peer infrastructure to develop Blockchain applications uncoupled from a predefined structure (i.e. there is no cryptocurrency value, enabling a clean and lightweight implementation). To implement the Blockchain node, the Sawtooth distribution was configured to share information using the Practical Byzantine Fault Tolerance (pBFT) consensus algorithm in a private network. Hence, the implementation provides to each node a single identity address that we assume not be corrupted, performing the information decentralization as proposed in the section III.

To implement the Context Reasoning, was used the transaction processors infrastructure present in the Sawtooth. The transactions processors consist of a code that can be executed in the Blockchain, as well as smart contracts. However, smart contracts presents a coupling to the Blockchain, while transactions processors presents a modular scheme that allow improved malleability to the code execution environment [21]. In practice, the Context Reasoning is executed by a set of rules, a transaction processor host such rules and execute according the need. As example, the following set of rules can be defined:

- An AMU geographically nearby to other ones can't exclusively receive requests in a short time. Assuming that nearby units shall share the workload, the execution in a single one can represent that an attacker has attempting to flood such unit.
- An AMU can't present abrupt behavior changes. Compare historical context searching for changes in characteristics as network utilized interfaces, operation hours, previous requests and model characteristics (e.g. type of material utilized by the printers and current part composition) can be effective to detect units tampered by attacks as spoofing [2].
- A same unique identifier (Blockchain node address) can not produce more than one spare part at time. Assuming that the Blockchain node address is unique for each AMU and knowing that a unit is able to produce one part at time. A single address producing two parts represents a duplicated unit, hence a cloned entity in the network pointing to a possible Sybil attack.

Besides the rules mentioned previously, the enterprise or

consortium that manages the 3D printer network can use rules intending to maintain a personal policy. Specifically, considering that a 3D printer can be managed by an unreliable third party, the architecture deployed at the edge can ensure the execution of a defined set of management policies. As example, if the 3D printers network have time restrictions for operate, specific rules can be established specifying when each printer have permission to operate. Hence, different procedures can be taken according to the result of the rules' execution.

V. Conclusion

In this paper we proposed a decentralized edge approach to secure industrial IoT environments. We argue that an architecture that combine Blockchain and Context-aware security can strongly improve the security in IoT environments. The Blockchain contributes by providing data integrity and a unified and secure context sharing architecture, while techniques of Context-aware security provides an efficient manner to execute behavior assertions. Specifically, our architecture its more exploitable for uses cases of decentralized approaches, as example, the industrial IoT trend for decentralized additive manufacturing.

We highlight that the implementation in this work demonstrates the architecture feasibility, hence, the approaches utilized to implement each module can be further explored [10] [15]. In the future works we intend to present an environment simulation using the Common Open Research Emulator (CORE) to demonstrate the network configuration and operation. We expect that the deployment of the proposed architecture in a controlled environment can further clarify the architecture contribution by means of practical demonstrations. Simultaneously, more use cases shall be explored in the future.

We believe that this paper presented contributions to different verticals. The exploration of an edge security architecture contributes to the edge computing researches, showing a use case that unloads the client-server communication from heavy security processing. Simultaneously, the research explicitly contributes to the industrial IoT development, proposing an approach for secure smart resources in decentralized use cases. Finally, we argue that our proposed architecture has potential to be explored in future trends [22] as decentralized and autonomous organizations.

Acknowledgment

We acknowledge and thank the FASTEN project for contributing in a practical use case and the INESC P&D Brasil for the financial support. This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nivel Superior - Brasil (CAPES) - Finance Code 001.

References

[1] N. Dragoni, A. Giaretta, and M. Mazzara, "The internet of hackable things," in *International Conference in Software Engineering for Defence Applications*. Springer, 2016, pp. 129–140.

[2] A. Giaretta, N. Dragoni, and F. Massacci, "Protecting the internet of things with security-by-contract and fog computing," in *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, April 2019, pp. 1–6.

[3] M. A. Khan and K. Salah, "Iot security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395 – 411, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167739X17315765

[4] A. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," in *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, June 2015, pp. 1–6.

[5] B. Miller and D. C. Rowe, "A survey scada of and critical infrastructure incidents." *RIIT*, vol. 12, pp. 51–56, 2012.

[6] J. P. Farwell and R. Rohozinski, "Stuxnet and the future of cyber war," *Survival*, vol. 53, no. 1, pp. 23–40, 2011. [Online]. Available: https://doi.org/10.1080/00396338.2011.555586

[7] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis *et al.*, "Understanding the mirai botnet," in *26th {USENIX} Security Symposium ({USENIX} Security 17)*, 2017, pp. 1093–1110.

[8] S. Wachter, "Normative challenges of identification in the internet of things: Privacy, profiling, discrimination, and the gdpr," *Computer Law & Security Review*, vol. 34, no. 3, pp. 436 – 449, 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0267364917303904

[9] K. Boeckl, M. Fagan, W. Fisher, N. Lefkovitz, K. Megas, E. Nadeau, B. Piccarreta, D. G. O'Rourke, and K. Scarfone, "Considerations for managing internet of things (iot) cybersecurity and privacy risks," *National Institute of Standards and Technology, NISTIR 8228 (Draft)*, 2018.

[10] H. Das, N. Dey, and V. E. Balas, *Real-Time Data Analytics for Large Scale Sensor Data*. Academic Press, 2019.

[11] N. V. Vafiadis and T. T. Taefi, "Differentiating blockchain technology to optimize the processes quality in industry 4.0," in *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, April 2019, pp. 864–869.

[12] K. Wüst and A. Gervais, "Do you need a blockchain?" in *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*, June 2018, pp. 45–54.

[13] M. J. Covington, P. Fogla, Z. Zhan, and M. Ahamad, "A context-aware security architecture for emerging applications," *18th Annual Computer Security Applications Conference, 2002. Proceedings.*, pp. 249–258, 2002.

[14] S. P. Gochhayat, P. Kaliyar, M. Conti, P. Tiwari, V. Prasath, D. Gupta, and A. Khanna, "Lisa: Lightweight context-aware iot service architecture," *Journal of Cleaner Production*, vol. 212, pp. 1345 – 1356, 2019. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0959652618338046

[15] B. Seok, J. Park, and J. H. Park, "A lightweight hash-based blockchain architecture for industrial iot," *Applied Sciences*, vol. 9, no. 18, 2019. [Online]. Available: https://www.mdpi.com/2076-3417/9/18/3740

[16] G. Wang, B. Wang, T. Wang, A. Nika, H. Zheng, and B. Y. Zhao, "Ghost riders: Sybil attacks on crowdsourced mobile mapping services," *IEEE/ACM Transactions on Networking*, vol. 26, no. 3, pp. 1123–1136, June 2018.

[17] D. Mourtzis and M. Doukas, "Decentralized manufacturing systems review: Challenges and outlook," in *Robust Manufacturing Control*, K. Windt, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 355–369.

[18] S. Raponi, S. Sciancalepore, G. Oligeri, and R. Di Pietro, "Fridges on the highway: Road traffic poisoning of navigation apps," *arXiv preprint arXiv:2002.05051*, 2020.

[19] E. de Matos, R. T. Tiburski, C. R. Moratelli, S. J. Filho, L. A. Amaral, G. Ramachandran, B. Krishnamachari, and F. Hessel, "Context information sharing for the internet of things: A survey," *Computer Networks*, vol. 166, p. 106988, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128619310400

[20] L. Barreto, A. Celesti, M. Villari, M. Fazio, and A. Puliafito, "Identity management in iot clouds: A fiware case of study," in *2015 IEEE Conference on Communications and Network Security (CNS)*, Sep. 2015, pp. 680–684.

[21] K. Olson, M. Bowman, J. Mitchell, S. Amundson, D. Middleton, and C. Montgomery, "Sawtooth: An introduction," *The Linux Foundation, Jan*, 2018.

[22] M. Swan, "Blockchain thinking: The brain as a dac (decentralized autonomous organization)," in *Texas Bitcoin Conference*. Chicago, 2015, pp. 27–29.