Towards a Secure Data Exchange in IIoT

Anna Sukiasyan(✉), Hasmik Badikyan, Tiago Pedrosa, and Paulo Leitão

Research Centre in Digitalization and Intelligent Robotics (CeDRI), Instituto
Politécnico de Bragança, Campus de Santa Apolónia, 5300-253 Bragança, Portugal
an.sukiasyan@gmail.com, {h.badikyan,pedrosa,pleitao}@ipb.pt

Abstract. Industrial Internet of Things (IIoT) plays a central role in the Fourth Industrial Revolution, with many specialists working towards implementing large scalable, reliable and secure industrial environments. However, existing environments are lacking security standards and have limited resources per component which results in various security breaches, e.g., trust in between the components, partner factories or remote control units with the system. Due to the resilience and its security properties, combining blockchain-based solutions with IIoT environments is gaining popularity. Despite that, chain-structured classic blockchain solutions are extremely resource-intensive and are not suitable for power-constrained IoT devices. To mitigate the referred security challenges, a secure architecture is proposed by using a DAG-structured asynchronous blockchain that can provide system security and transactions efficiency at the same time. Use-cases and sequence diagrams were created to model the solution. The achieved results are robust, supported by an extensive security evaluation, which foster future developments over the proposed architecture. Therefore, as the proposed architecture is generic and flexible, its deployment in diverse customized industrial environments and scenarios, as well as the incorporation of future hardware and software, is possible.

Keywords: Blockchain · IoT · Industrial IoT · Cybersecurity

1 Introduction

The number of companies approaching the Industry 4.0 paradigm is growing on daily bases. Companies are connecting their devices to the internet to increase the system's productivity and efficiency. In these Internet-connected environments, the security issues are the most challenging aspects to deal with. According to Cisco Annual Cybersecurity Reports, 31% of companies have experienced attacks on Operational Technologies (OT) [1]. Despite the fact that 75% of experts think of security as a high priority component, only 16% are sure that the company is prepared to face the cybersecurity issues. The main reason for that is the lack of standards for Industrial Internet of Things (IIoT) environments, endpoints and communication protocols.

J. Prieto et al. (Eds.): BLOCKCHAIN 2020, AISC 1238, pp. 61–70, 2020.
https://doi.org/10.1007/978-3-030-52535-4_7

The fourth industrial revolution includes several segments such as logistics and supply chain, transportation, mining, healthcare, oil and gas. The digital transformations are implemented with the use of Information and Communication technologies (ICT), Internet of Things (IoT), artificial intelligence, robotics, smart decentralized manufacturing infrastructures and self-optimizing systems in information-driven, cyber-physical environments. In the industrial world, Cyber-Physical Systems (CPS) can be seen as Industrial Control Systems (ICS), which can ensure that technical facilities run automatically by controlling business processes. ICS usually comprise Supervisory Control and Data Acquisition (SCADA), Distributed Control System (DCS), Programmable Logic Controller (PLC), Remote Terminal Unit (RTU), Intelligent Electronic Device (IED) and the interface which is to ensure the communication of components. Systems mentioned above are the building blocks of the critical infrastructures, meaning that reliability, availability and privacy of those systems are the main concerns. The protection of an IIoT system or the system state can be achieved by establishing and maintaining the system in a way to prevent unauthorized access to the system or its resources. This will also prevent data loss or major damage in the system. ICS were usually isolated systems using proprietary control protocols. Nowadays, as IT solutions are being integrated into ICS environments, they are becoming open for remote access and working on improving connectivity between system components. There are various standards and solutions for IT environments security, but those can not be applied to ICS due to several specific requirements [2]:

- Functional requirements: ICS as part of production processes have many components of the system that are embedded, which reduces the possibility of classic security solutions being directly applicable to the production. From the production perspective, confidentiality is the main risk, but availability still stays the first priority in the requirements list.
- Resource requirements: Many ICS are running on real-time operating systems which is a highly resource consuming process. Also the components of the ICS normally have low processing power and machine specific limitations that reduce the chance of being able to perform security updates on the system components.
- Security requirements: Industrial systems can contain confidential information about the production processes or the industry components. Loss of this information can result in the violation of company confidentiality or data leaks related to the production environment topology. These data leaks will not result in the loss of equipment, but can be used in future attacks.

Having this in mind, this paper explores the current state of the art of the security in IIoT environments by identifying the potential threats and the current capability of devices enrolled in the industrial environments, and purposes a solution to enable secure data exchange in IIoT.

The rest of the paper is organized as follows. Section 2 presents a characterization of the security issues in IIoT environments and Sect. 3 overviews the use of blockchain in IIoT. Section 4 describes the proposed secure data exchange approach for IIoT environments, and finally, Sect. 5 rounds up the paper with the conclusions and points out the future work.

2 Security Characterization of Industrial IoT

IIoT security surveys show that IIoT endpoints are the main source of system's vulnerabilities, their definition being dependent on the system architecture, i.e. an endpoint can mean the IoT device itself or a group of devices that are responsible for any particular operation or performing any role in the system. Endpoints are managed through the network and are used for the data exchange, data collection or control purposes. Around 72% of the endpoints rely on the use of Internet protocols and 53% are IP-based, domain-specific protocols that are replacing point-to-point, non-routable protocols for control systems. The most commonly used protocols are MQTT (Message Queuing Telemetry Transport) and CoAP (Constrained Application Protocol) as they overcome others in terms of header size, power consumption, and data loss [3].

The ICS architecture consists of 2 layers: physical layer that includes all sensors and hardware components, and cyber-layer composed mainly from SCADA systems. SCADA systems are a set of protocols, platforms and technologies used to manage an ICS. Traditionally, the protection of SCADA systems has been based on the physical isolation, using non-standard protocols. The components responsible for the communication between other services are a direct target for attacks that can be solved by using secure network protocols covering authentication, confidentiality and integrity aspects. But in industrial automation, similar protocols are hard to find, so the main priority is meeting the real-time requirements [4].

The use of secure protocols and intermediate pre-checks leads to performance issues and communication delays in time-critical infrastructures, so it is crucial to find the balance between latency and security. The interaction of communication components with external networks implies the importance of protecting transmitted data, as well as the access to communication functions. Network interconnection points, e.g., wireless access points, are also intrusion points and need to be monitored by Intrusion Detection System (IDS). For sharing information in external and internal networks, additional routers and firewalls are being deployed by IDS, which are capable of identity checks and traffic analysis. Similar solutions are used to protect the gateways [5].

3 Blockchain in IoT

Blockchain based systems are classical distributed systems that can be classified into two main types: permissionless and permissioned. Permissionless systems are publicly open for use while permissioned platforms are designed in a close-ended manner. This means that the permissioned system has a well defined and fixed set of nodes [6].

The features of the blockain's decentralized consensus system may be integrated with IIoT environments to mitigate some security issues. Most of the existing solutions are adopting chain-structured blockchain in IoT systems. This type of blockchain can bring limitations related with the consensus model as it can collide with the requirements in IoT field, such as low latency and high performance. Three main challenges of integrating IoT with blockchain are:

1. The trade-off between efficiency and security.
2. The coexistence of transparency and privacy.
3. The conflicts between high concurrency and low throughput.

Based on the referred challenges, the blockchain development is evolving into different variations of the classical idea, which according to the differences in the structure can be classified as:

Chain-Structured Blockchain: In chain-structured blockchain systems (Fig. 1), the longest chain of blocks is considered as the main chain for the system. If more then one block has been generated at the same time, the first generated block will join the main chain and for the other blocks, there a fork will be created. Only transactions placed in the main chain will be considered valid, which means that all transactions in secondary chains will be labeled as invalid blocks. Mechanisms implemented in traditional blockchains such as ZK-snark and the AZTEC protocol now used in the Ethereum are creating a highly secure environment, but at the same time elliptic curve arithmetic operations required by the AZTEC protocol are highly resource intensive [7]. Overall, chain-structured blockchain solutions are not suitable for power-constrained IIoT environments, where most of the components have low processing power and all transactions are performed in a time critical manner.

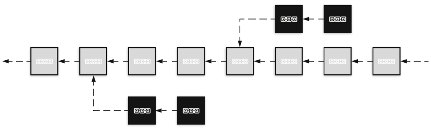

Fig. 1. Chain-structured blockchain architecture diagram

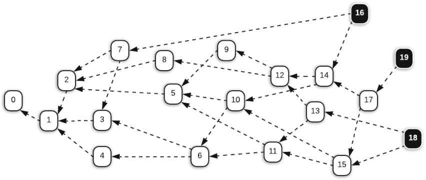

Fig. 2. DAG-structured blockchain diagram

DAG-Structured Blockchain: Aiming to integrate blockchain with more critical environments such as IoT, a new structure of blockchain has been created based on acyclic graph architecture, which is called tangle. In tangle, the concept of blocks is changed to an individual node representing each transaction in the distributed ledger. Unlike the first blockchain, the tangle uses different approaches to improve the throughput of the system which is a critical metric in the IIoT environment. It adopts asynchronous consensus model and as shown in the Fig. 2, the network is not limited to one main chain. It forks all the time by forming a tangle net. There are several implementations of DAG-structured blockchain, such as IOTA, ByteBall and NANO [8].

4 Proposal for Secure Data Exchange in IIoT

This section presents a solution for increasing security in IIoT environments by using the blockchain technology. The proposed approach considers a DAG-Structured blockchain security solution implemented on top of existing components in IIoT architectures. Due to the specifications of IIoT environments, which are time and resource critical, these requirements have been taken into consideration during the designing of the solution. The solution consists of 2 main parts: access control and secure transaction chain generation to ensure trust and data consistency in the system. As previously discussed, nodes of the industrial environment may have limited resources and can be divided into 2 types based on their processing power capabilities: light nodes and full nodes. In our solution only full nodes, such as gateways and managers, are considered members of a tangle network. The light nodes are connecting to the full nodes to publish a transaction to the network. The full node will sign each transaction received from a light node on their behalf, if the light node doesn't have this capability, and will publish it to the tangle network by using the IRI interface (IRI is an implementation of IOTA that also provides HTTP REST interface, so that light nodes can send transactions to the full nodes).

4.1 Architecture

Figure 3 depicts the architecture that will support the proposed solution. The architecture is composed by diverse components, namely the wireless devices, gateways, managers and the tangle network.

Wireless Devices: Wireless devices can be of the main 3 types: sensors, actuators and controllers. In IIoT environments, wireless devices are categorized as light nodes as they have limited resources and are not capable of using secure protocols or performing any power-consuming actions. Each device needs to have a unique identifier in the system and has to pass the authentication every time when trying to perform a transaction. As light nodes do not have enough processing power to implement Proof of Work (POW), they are not considered to be a direct part of the network. Light nodes will be able to send transactions to the network through the middleware which will serve as a gateway. During the registration process, each device in the system will be granted with a public/private key pair that will be used in future for signing transactions. The key pair generation will be performed by the gateway.

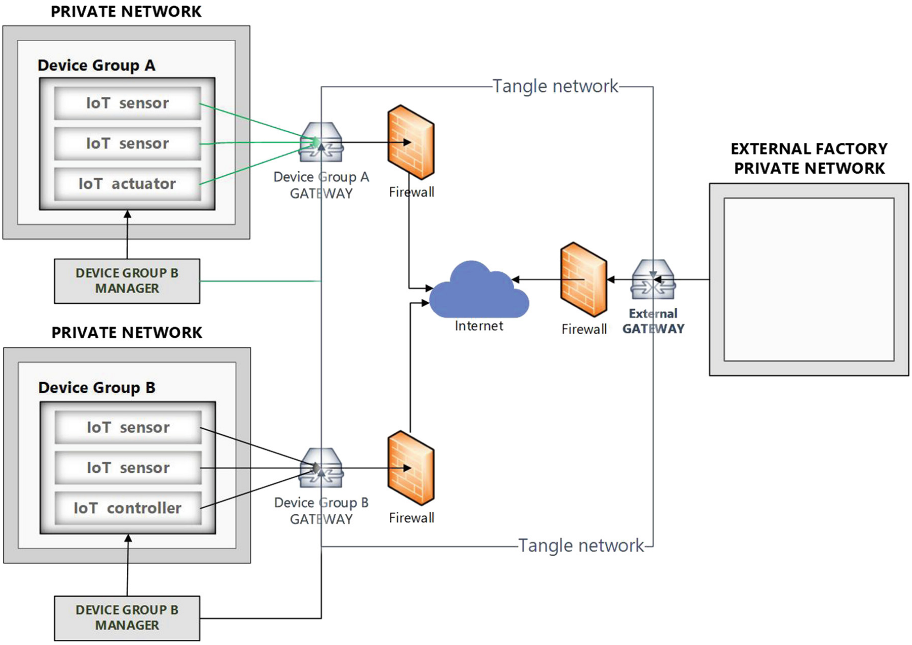

Fig. 3. Architecture diagram of the proposed solution

Gateways: Gateways serve as a secure middleware in between light nodes and the tangle network. As gateways are considered as full nodes, they are responsible for the tangle network maintenance. They also perform a role of a checkpoint which only submits transactions from the light nodes that are authorized by the manager. Gateways can be of 2 types: device gateway and external gateway. The first one is responsible for the key generation, authentication of group of devices (light nodes) and organization of the communication on their behalf. It also has capability to translate commonly used protocols to HTTP to deliver messages from device to the http endpoint of the tangle network. External gateways are responsible for the communication between 2 factories. They are the first access point for all the requests incoming to our industrial infrastructure from the outside. Gateways are the core components of the architecture that need to be set up in order to be able to start devices registration and communication processes in the system.

Manager: The manager is also a full node that is responsible for the device management in the system. The registration of the IoT device in the system is performed manually by the system administrator. After the device enters in the system, it will be registered in the device list by the manager, which is the only one that has permission to write for the device list. Other full nodes of the system only have read permission for the device list. These access control rules are also designed to increase the security in the system by preventing third party devices from making unauthorized changes. As mentioned above, devices will be divided by device groups. There is a limitation to have one manager node per device group. Manager has to be predefined and set up before being able to start the registration process for the light nodes.

Tangle Network: Tangle network in our architecture is a public blockchain network which allows any parties to participate in the process. It serves as the main solution for the trust issue in the system and allows us to have a consensus in the system for all published transactions. This is a requirement in order to be able to perform transactions between different industrial environments or remote nodes of the system regardless of their geo-location and security implemented on each individual device. The tangle network structure allows protecting system against several attacks, such as Distributed Denial of Service (DDoS), double-spending, etc. It also improves throughput of time and resource critical environment in comparison to chain-structured blockchain.

4.2 Functionalities

The functionalities provided by the proposed solution are the registration of devices, revoking devices, disable/restore devices and communion between 2 devices from different devices groups [9]. This paper focuses on the description of the communication between the devices as this is the scenario where most of the attacks are identified and should be mitigated by the proposed solution.

The communication between the devices that belong to different device groups is organized through the device group gateways, with 4 main components participating in this process: source and destination devices and their gateways. As mentioned earlier in the architecture diagram Fig. 3, the communication is performed through the tangle network. The source device will generate the package that need to be delivered to the destination. In the destination of the package, both gateway and device need to be specified. The package is sent by the source device to the device group gateway. Normally, as sensors are using industrial protocols for communication, the package will be passed to the translation module of the gateway. After being translated from industrial protocols to HTTP, the gateway is submitting the package as a transaction to the tangle network on behalf of the source device. After the transaction is approved on the tangle network by other nodes, the destination device group gateway will be notified about a new transaction in the network, as all the gateways are full nodes on the tangle network. As soon as the gateway will get the notification about the published transaction, it will convert the package from HTTP to industrial protocol appropriate for the destination device. After the translation, the package will be sent to the destination device.

More detailed actions performed during the communication process are shown on the sequence diagram represented in Fig. 4.

The sequence diagram illustrated in Fig. 4 is showing the steps performed to deliver data from device A to device B. The tangle network is shown as a

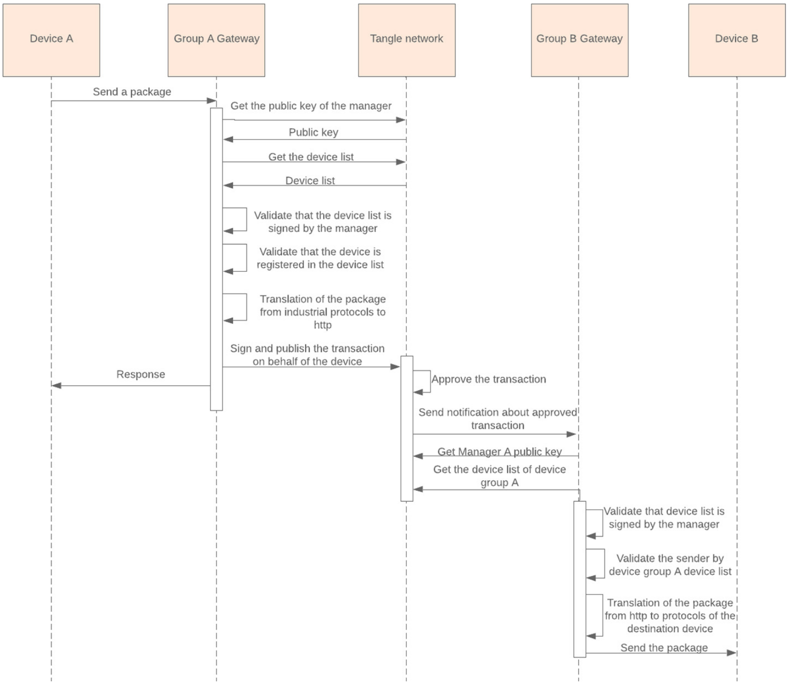
Device A
Group A Gateway
Tangle network
Group B Gateway
Device B
Send a package
Get the public key of the manager
Public key
Get the device list
Device list
Validate that the device list is signed by the manager
Validate that the device is registered in the device list
Translation of the package from industrial protocols to http
Sign and publish the transaction on behalf of the device
Response
Approve the transaction
Send notification about approved transaction
Get Manager A public key
Get the device list of device group A
Validate that device list is signed by the manager
Validate the sender by device group A device list
Translation of the package from http to protocols of the destination device
Send the package

Fig. 4. Sequence diagram: communication between 2 devices from different device groups

separate node on the diagram but in the actual implementation all gateways will be published to the tangle network as full nodes, so the network will not be a standalone component of the system.

This architecture is flexible enough to allow removing the device group gateways from the current position and organizing direct communication between devices by using the tangle network in the future when the devices will have required processing power to be able to handle all the processes of the workflow described above. The lack of standards for IIoT devices and communication protocols brings challenges that can be addressed by the implementation of translation modules on the gateways. The semantic gateways can serve as a translator between the various communication protocols to allow the industrial environment growth independent from vendor-specific implementations.

4.3 Bootstrapping the System

The IOTA technology is used for the implementation of the tangled network, specifically the approach to create a private network, which allows to isolate the network and keep it accessible only for the nodes in our environment. Also, the current architecture allows to have a shared private network between multiple factories or industrial environments that will serve as a communication method in between them.

All components are set up and running on docker containers. For bootstrapping, a private tangle network, the components need to be set up and configured in the following order. First deploy of the Coordinator (COO), then start the IRI node and then launch the Coordinator service. At last, configure the node to subscribe the events in order to be notified when such are sent to the network.

After having the tangle network setup and running, device group gateways need to perform their first transactions in the network. The first transaction performed by the manager will be publishing its public key to the tangle, and the first transaction performed by the gateway is reading and storing the service group manager's published public key and storing it in the cache in order to be able to do the verification checks during the future communications. If for some reason, the manager will change or the key pair will be regenerated, a new public key will be published by the manager and all the nodes with already cached public key will be notified about the changes. On the other hand, the first transaction of all full nodes in the device group except for the manager is read request for the public key of the manager.

After performing this bootstrapping sequence, the system will be fully functional and all previous presented functionalities will be ready to use.

5 Conclusion and Future Work

This paper analyses how blockchain technology can be used to improve secure data exchange in IIoT, addressing specific requirements, such as time and resource critical that have an impact in the type of consensus that can be used on the blockchain.

The proposed solution is based in 2 logical groups: light nodes and full nodes. Light nodes are considered to be the ones that don't have the capability to implement any security functions, communicate via secure protocols or participate in the transaction approval and proof of work processes on the tangle. Full nodes participate in all processes, in the tangle and in the industrial environment and are also responsible for publishing transactions to the tangle network in behalf of the light nodes. Public/private keys are generated for each component of the system that are used for authentication and authorization purposes. The designed architecture provides a solid ground for trust assurance between all industrial components, by also providing a secure communication channels for remote control and data exchange. STRIDE threat analysis performed has shown that most of the attack vectors falling into the scope of the mitigation mechanisms presented are covered in the designed solution.

For future work is considered the development of the proposed architecture. After will follow the test in industrial environment replicating a real world scenario, to check the usability of the solution. Performance analysis should be done and optimization of various processes might be required because industrial environments are highly time and resource critical. One of the risks related to the performance that can arise is due to the growing chain of transactions in the tangle network. Growth of the transaction chain can increase decision making time for the approval of the transactions by all the nodes participating in the consensus. With the continuous monitoring of the implemented solution we need to make sure that no perceptible downgrade of the performance is identified.

Overall, the tangle network is a growing project used in various IoT based environments. Every day devices and sensors enrolled in the industrial systems are gaining more processing power and becoming capable of performing more complex calculations. Some security related functions will start to be made based on the light nodes, which will improve the trust and security. Probably some of the light nodes will gain capabilities to turn into full nodes and will participate in all processes equally. Our architecture is designed in a way to be agnostic to that future use case scenario. That means that the architecture is flexible enough to easily adjust to the predictable nearest future.

Acknowledgements. This work has been supported by FCT – Fundação para a Ciência e Tecnologia within the Project Scope: UIDB/05757/2020.

References

1. Cisco. Annual cybersecurity report (2018)
2. Fan, X., Fan, K., Wang, Y., Zhou, R.: Overview of cyber-security of industrial control system. In: Proceedings of the 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications, SSIC 2015, pp. 1–7 (2015). https://doi.org/10.1109/SSIC.2015.7245324
3. Frustaci, M., Pace, P., Aloi, G., Fortino, G.: Evaluating critical security issues of the IoT world: present and future challenges. IEEE IoT J. **5**(4), 2483–2495 (2018). ISSN: 23274662
4. Neumann, P.: Communication in industrial automation-what is going on? Control Eng. Pract. **15**(11), 1332–1347 (2007). https://doi.org/10.1016/j.conengprac.2006.10.004. ISSN: 09670661
5. Hong, S., Lee, M.: Challenges and direction toward secure communication in the SCADA system. In: CNSR 2010 Proceedings - 8th Annual Conference on Communication Networks and Services Research (2010)
6. Baliga, A.: Understanding blockchain consensus models. Whitepaper, no. April, pp. 1–14 (2017). https://www.persistent.com/wp-content/uploads/2017/04/WP-Understanding-Blockchain-Consensus-Models.pdf
7. Williamson, Z.J.: The AZTEC protocol. Whitepaper, pp. 1–24 (2018)
8. Huang, J., Kong, L., Chen, G., Wu, M.-Y., Liu, X., Zeng, P.: Towards secure industrial IoT: blockchain system with credit-based consensus mechanism. IEEE Trans. Ind. Inf. **15**(6), 3680–3689 (2019)
9. Sukiasyan, A.: Secure data exchange in IIoT. Master thesis in Information Systems – Polytechnic Institute of Bragança (2019)