Neurocomputing 484 (2022) 183–195

Contents lists available at ScienceDirect

Neurocomputing

journal homepage: www.elsevier.com/locate/neucom

Secure data exchange in Industrial Internet of Things

Anna Sukiasyan, Hasmik Badikyan, Tiago Pedrosa *, Paulo Leitao

Research Centre in Digitalization and Intelligent Robotics (CeDRI), Instituto Politécnico de Bragança, Campus de Santa Apolónia, 5300-253 Bragança, Portugal

ARTICLE INFO

Article history:
Received 29 January 2021
Revised 12 June 2021
Accepted 7 July 2021
Available online 3 November 2021
Communicated by Zidong Wang

2021 MSC:
00-01
99-00

Keywords:
Blockchain
IoT
Industrial IoT
Cybersecurity
Threat modelling
IOTA

ABSTRACT

The use of the Industrial Internet of Things (IoT) is widespread, working as an enabler to implement large, scalable, reliable, and secure industrial environments. Although existing deployments do not meet security standards and have limited resources for each component which leads to several security breaches, such as trust between components, partner factories, or remote-control. These security failures can lead to critical outcomes, from theft of production information to forced production stoppages, accidents, including physical and others.

The combination of blockchain-based solutions with IIoT environments is gaining momentum due to their resilience and security properties. However, chain-structured classic blockchain solutions are very resource-intensive and are not suitable for power-constrained IoT devices. To mitigate the mentioned security concerns, a secure architecture is proposed using a structured asynchronous blockchain DAG (Directed Acyclic Graph) that simultaneously provides security and transaction efficiency for the solution. The solution was modelled with special details in the use cases and sequence diagrams. Security concerns were integrated from the start, and a threat model was created using the STRIDE approach to test the security of the proposed solution. As a result, a flexible solution was been developed that significantly reduces the attack vectors in IIoT environments. The proposed architecture is versatile and flexible, is supported by an extensive security assessment, which allows it to be deployed in a variety of customizable industrial environments and scenarios, as well as to include future hardware and software extensions.

1. Introduction

The Industry 4.0 paradigm is growing every day, and companies are connecting their devices to the Internet to improve system performance and efficiency. In these Internet-connected environments, security concerns are the most complex aspects. 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.

The fourth industrial revolution includes several segments such as logistics and supply chain, transportation, mining, healthcare, oil and gas. The digital transformation processes are performed with adoption of cyber-physical systems, complemented with the use of emergent Information and Communication Technologies (ICT), namely Internet of Things (IoT), cloud computing, artificial intelligence and robotics, that are characterized by smart decentralized manufacturing infrastructures and self-optimizing systems [2].

In the industrial world, Cyber-Physical Systems (CPS) [3] can be considered 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 that must provide communication between components [4]. The systems mentioned above are the building blocks of critical infrastructures, which means that the reliability, availability, and privacy of these systems are the main concerns. Also, research has shown that security analysis should be a part of the software development lifecycle (SDLC). To create secure solutions, security needs to be integrated in all phases, from planing to deployment, because having it

* Corresponding author.
E-mail addresses: an.sukiasyan@gmail.com (A. Sukiasyan), h.badikyan@ipb.pt (H. Badikyan), pedrosa@ipb.pt (T. Pedrosa), pleitao@ipb.pt (P. Leitao).

https://doi.org/10.1016/j.neucom.2021.07.101
0925-2312/

added on top of an existing solution will be much more costly. For this reason, architectural security analysis plays an important role in addressing the security threats contained in the architecture. The purpose of threat analysis is to identify, prioritize, and mitigate potential security threats. System threat analysis is particularly important because it has been proven that many vulnerabilities are caused by architectural design threads.

The Industrial Internet of Things (IIoT) is a subset of the Internet of Things that needs a greater level of security as they are used in industry in real-time and mission-critical operations [5]. The IIoT can be seen as the evolution of Machine to Machine (M2M) technology. Manufacturing is one of the biggest users of IIoT because machine automation, robotics and M2M communications and cooperation in manufacturing has been used for decades [6]. The protection of the system or the state of the system can be achieved by creating and maintaining the system in a way that prevents unauthorized access to the system or its resources. Proactive prevention of attacks in IIoT system can also protect the system from data loss or serious damage in the system. Historically, ICS were isolated systems that used proprietary control protocols. But as IT solutions are integrated into the ICS environment, systems are made available over the Internet, allowing for remote control and improved connectivity between system components. In addition, it is a huge step towards various automation and optimization in the system. Existing standards and solutions for ensuring the security of the IT environment cannot be applied to the ICS due to system constraints, which lead to new requirements regarding resource use, performance and availability of the system [7].

With this in mind, this article explores the current state of security in IIoT environments by identifying potential threats and current capabilities of devices enrolled in industrial environments, and offers a solution to ensure secure data exchange and reduce the attack vector in IIoT environments. The aim of this research is to design a solution that can be applied to IIoT environments that addresses the security concerns raised in the field without requiring major changes in the existing environments. This solution should increase the overall security of the system and reduce the attack vectors. To achieve this goal, this solution uses the IOTA blockchain [8] in an innovative way that allow legacy devices to be used with components with greater security and capabilities, allowing different components to securely exchange data, mitigating security issues that can arise from erroneous information. It also uses a threat modeling approach to analyze the security of the solution, which can be used to compare approaches in the future and study the impact of future evolution.

The rest of the article is organized as follows. Section 2 presents the security characteristics of IIoT environments, overviews the use of blockchain in IIoT and discusses the threat modeling. Section 3 describes the proposed secure data exchange approach for IIoT environments, and Section 4 presents the results of the threat modeling analysis. Finally, Section 5 concludes the document with conclusions and points to future work.

2. Background

This section presents the security characteristics of the industrial Internet of Things, analyzes the use of blockchain in IoT, and provides a brief explanation of threat modeling, with special attention to the use of the STRIDE methodology.

2.1. Security Characteristics of Industrial IoT

IIoT security studies show that IIoT endpoints are a major source of system vulnerabilities. They are managed over a network and are used for data exchange, data collection, or control. About 72% of the endpoints rely on the use of Internet protocols and 53% are domain-specific IP-based 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 are superior to the others in terms of power consumption, data loss prevention, and light weight, which is crucial for IIoT environments with limited power consumption [9].

The ICS architecture consists of 2 layers [10]: the physical layer, which includes all sensors and hardware components, and cyber-layer, which consists mainly of SCADA systems, which are a set of protocols, platforms, and technologies used to manage an ICS. Traditionally, the protection of SCADA systems was based on physical isolation using non-standard protocols. The components responsible for the communication between the nodes of the system are a direct target for attacks. The usage of secure network protocols, combined with complementary secure mechanisms such as IDS/IPS can drastically reduce the risk of such attacks. As the main priority in the mission-critical environments is to meet the real-time constraint, therefore no resource-intensive secure protocols can be applied to these systems [11].

In time-critical infrastructures, it is crucial to find the balance between latency and security, as the use of secure protocols and intermediate pre-checks leads to performance issues and communication delays. The interaction of communication components with external networks implies the importance of protecting transmitted data, as well as the access to communication functions. Network connection points such as wireless access points are also intrusion points and must be monitored by Intrusion Detection System (IDS). For communication on external and internal networks, IDS deploys additional routers and firewalls that can authenticate and analyze traffic. Similar solutions are used to protect the gateway [12].

2.2. Blockchain in IIoT

Blockchain-based systems are distributed systems that can be divided into two main types: permissionless and permitted. Permissionless systems are publicly open for use, while permitted ones are developed in a closed manner with a well-defined and fixed set of nodes [13].

To mitigate some security issues the features of the blockchain's decentralized consensus may be integrated with IIoT environments. Most of the existing solutions are adopting chain-structured blockchain in IoT systems, which can bring limitations related to the consensus model as it can collide with the requirements in the IoT field, such as low latency and high performance. Also, this type of blockchain can introduce new costs per transaction (costs spent on Proof Of Work (POW)). Three main challenges of integrating IIoT 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, 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 or DAG structured blockchains.

In chain-structured blockchain systems (Fig. 1), the longest chain of blocks is considered as the main chain for the system. If more than one block has been generated at the same time, the first generated block will join the main chain and for the other blocks, 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.

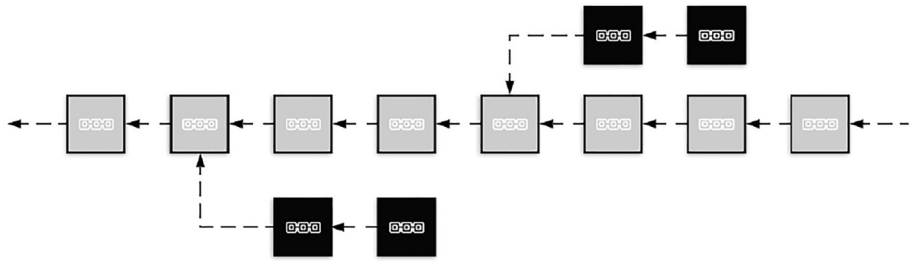

Fig. 1. Chain-structured blokchain architecture diagram.

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 [14]. 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.

DAG-Structured Blockchains aim 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 an asynchronous consensus model and as shown on 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 blockchains, such as IOTA [15], ByteBall [16] and NANO [17].

2.3. Threat modeling

The goal of the threat analysis is to identify, prioritize and mitigate potential security threats. Threat analysis of the system is especially important since the cause of many vulnerabilities is proven to be architectural design flows. Fixing those vulnerabilities in the early stages will reduce the waste in the process and decrease the attack vector. The goal of this overview is to study existing and widely used security analysis methodologies in the aspects like applicability, input, procedure, and outcomes.

Based on the research results presented by [18] most commonly used methodologies are misuse cases, attack trees, problem frames, and several software-centric approaches. In general, we can group all approaches by risk-centric, attack-centric, and software-centric techniques. One of the most commonly used methodologies is STRIDE, which stands for security threat analysis in 6 categories: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service (DOS), and Elevation of Privilege. This methodology can be defined on various abstraction levels and provides a clear understanding of the vulnerabilities of the system and the possible impacts of each component's vulnerability on the entire system. For that reason, it's considered one of the most flexible models to perform threat modeling with. It can provide full coverage for the threat analysis. The threat modeling can be implemented on the component level or system functionality level.

As mentioned on Table 1, the STRIDE categories can be described as follows [19]:

- Spoofing: Spoofing is a type of attack where the attacker takes over a component/user and performs actions on their behalf by falsifying its own identity. For example, extracting a cryptographic key from the device by using vulnerabilities in the hardware or software of the device and periodically accessing the system, and performing actions under the identity of the original key owner.
- Tampering: Tampering can represent any form of sabotage but mainly it means an intentional modification of component/network to make it harmful for the system. Tampering includes unauthorized changes in the data exchanged between the components or stored in one of them. Tampering on the device level can be performed by fully or partially replacing the software of the device. This action potentially opens up the component for the spoofing attack described above.
- Repudiation: Non-repudiation is a term in security describing the inability of the component acting to change the ownership of the action. For example, signed transactions in the system proving the authenticity of the transaction owner.
- Information disclosure: Information disclosure is a term describing a scenario when the component can expose information to unauthorized third parties. For example, if the component is running with the infected software, the attacker can let himself into the component and leak information or inject himself into the communication path between the components.
- Denial of Service(DOS): Denial-of-Service attacks are mainly targeting the goal to make the service/component temporarily unavailable or deny service to the valid users of the system. DOS attacks may cause major damage to the overall system if the components are codependent. Denial of service is typically accomplished by flooding, by sending an abnormal amount of

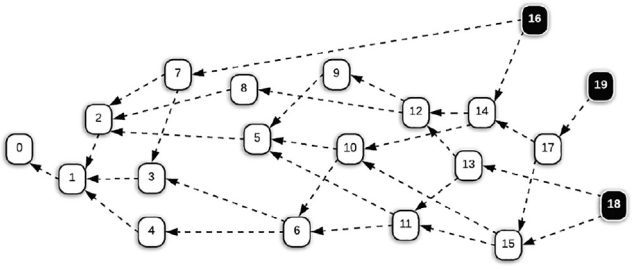

Fig. 2. DAG-structured blockchain diagram.

Table 1
STRIDE threat analysis categories.

Threat	Security category
Spoofing	Authentication
Tampering	Integrity
Repudiation	Non-reputability
Information disclosure	Confidentiality
Denial of Service (DOS)	Availability
Elevation of Privilege	Authorization

requests to the target service in a short period of time. In the industrial world, this attack can also be performed on the physical level.
- Elevation of Privilege: In this attack, the unprivileged component/user is gaining privileged access and can perform unauthorized actions in the system. This attack can be performed by using weak spots of design flow or system configurations.

Threat analysis is performed (in Section 4) on the proposed architecture to make sure that the solution covers the most important aspects of the security. STRIDE analyses helps to evaluate the proposed architecture based on the main attack categories and course-correct if any gaps are identified in the architecture. Performing this in the early stages of the development and design of the solution will decrease the possibility of it reaching production with major security breaches.

3. Proposal for a secure data exchange in IIoT

This section presents a solution that is meant to increase security in IIoT environments and is built on blockchain technology. The proposed architecture relies on a DAG-structured blockchain solution called IOTA tangle and can be added on top of the existing industrial environments. The real-time constraints of the IIoT environments have been taken into consideration during the design of the solution. This solution covers two main objectives: access control and generation of secure transactions to ensure trust between the nodes and data consistency in the system. As discussed previously, we can divide the existing components of industrial environments into two main categories, based on their resources: light nodes and full nodes. In our solution, only full nodes, such as gateways and managers, are considered to be full members of the tangle network and perform resource-intensive tasks. The light nodes will communicate through the full node, which will be able to publish and receive transactions by signing them on behalf of the light node. As the light nodes are also improving, our solution is flexible enough to be adjusted. So if the light node can handle its transactions it can be connected to the tangle network without having the full node as a middleware.

3.1. Architecture

Fig. 3 depicts the architecture of the proposed solution. The architecture comprises various components such as wireless devices, gateways, managers, and the tangle network.

3.1.1. Devices

In the given architecture the devices can be of 3 main types: sensors, actuators and controllers. In IIoT environments, these devices are considered to be the light nodes as they have limited resources and are not capable of participating in any resource-intensive processes. Each device normally has a unique identifier in the system which can be used to authenticate the device. As the light nodes do not have enough processing power to perform proof of work, they are not considered to be a member of the tangle network. Light nodes will communicate through the device group gateway, which will serve as a middleware between the device and the tangle. During the registration process, each device will be granted by a public/private key pair. The key pair will be used in the future to sign the transactions. Only the gateway should have the right of generating and granting keys to the devices.

3.1.2. Gateways

The gateway serves as a middleware between the light nodes and the tangle network and takes over the role of performing resource-intensive actions to ensure secure communication of the light node. The gateways are considered as full nodes and are a member of the tangle. They also perform as an additional filter to submit only transactions from the nodes that are authorized by the manager. There can be 2 types of gateways in the system: device gateway and external gateway. The first one is responsible for light node related tasks, such as the generation of the key pair, authentication of the devices, and management of the communication on their behalf. It is also responsible for making the communication protocol agnostic, meaning that the gateway has the capability of translating various protocols to HTTP(S) to deliver the transaction to the HTTP endpoint of the tangle. The second type of gateways are the external ones, that are responsible for providing secure communication between two or more industrial environments. External gateways are the first access point for all the requests coming into our industrial environment from the outside. Gateways are the core components of the architecture and are required to be set up and configured to enable the communication of the light nodes.

3.1.3. Manager

The manager is also a full node that is responsible for device management in the system. When a new device is trying to join the system for the first time, it should be registered in the device list by the manager and the registration should be approved by the system administrator. Only after the registration is approved the device can be considered a part of the system and start performing any tasks. Only the manager has a right to perform write action on the device list. Other full nodes of the system have read-only access to the device list and are using this list to perform authorization. These access control rules are designed to increase the security in the system by protecting it from any authorized changes. The devices are divided into groups. Each group will have a dedicated manager node assigned to it. The manager should be provisioned and configured to enable the registration process of the light nodes.

3.1.4. Tangle network

The tangle in our solution is a private blockchain network that serves as a backbone for exchanging transactions across the system without any transactional fees. It is a distributed network of nodes that should reach a consensus to be able to approve a transaction. The tangle is designed to prevent several attacks, such as Distributed Denial of Service (DDoS), double-spending, etc., and add trust to the system. It is designed specifically for time and resource critical environments which bring it to a leading position in comparison to the chain-structured blockchain implementations.

3.2. 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 device groups [20].

3.2.1. Registration of the device in the system

When a new device is being added to the existing IIoT environment, it needs to be registered in the tangle network device list.

The device registration is partially a manual process, which allows having control over added/removed devices instead of granting unlimited access control permissions to one of the components and having it as the main vulnerable attack point. Three main components participating in this process are administrator, device manager, and device gateway. The process of registration should be performed as follows and is shown on Fig. 4.

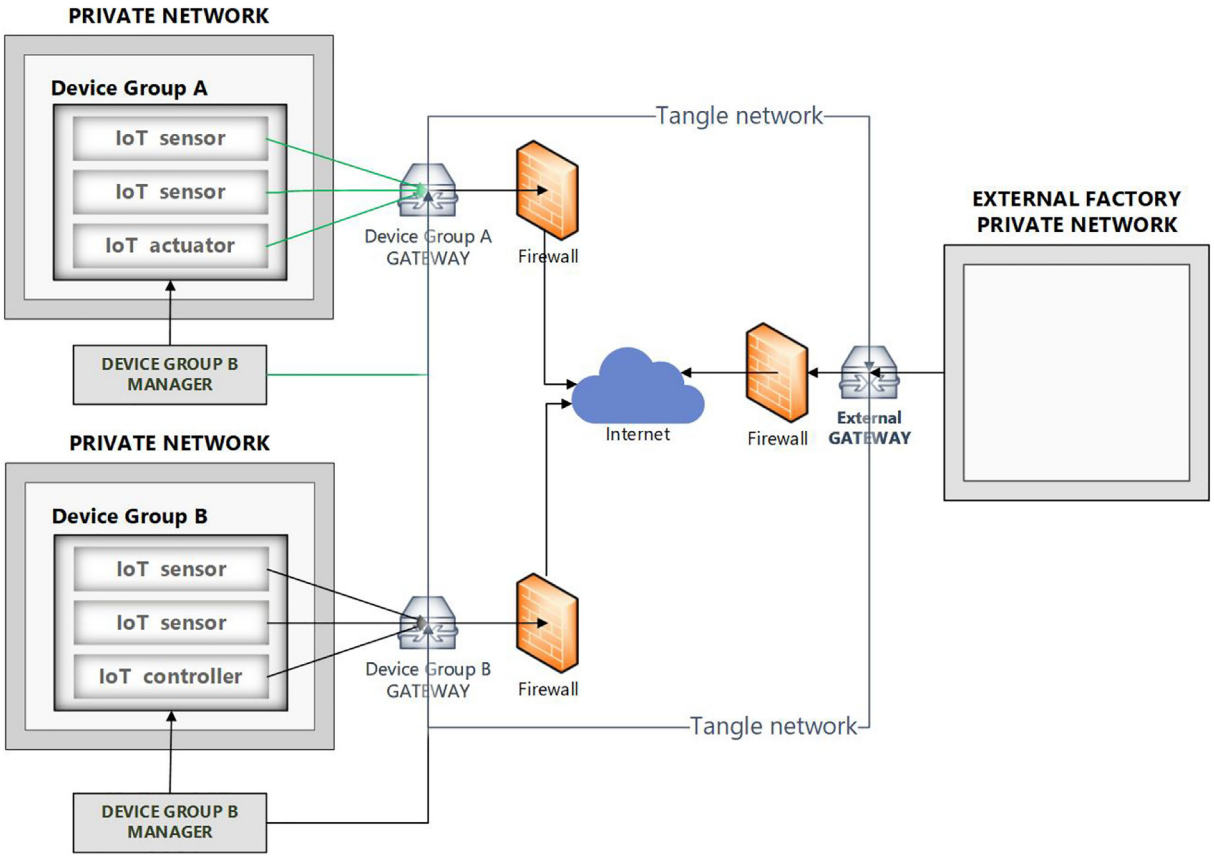

Fig. 3. Architecture diagram of the proposed solution.

Admin user of the system inserts device credentials into the system, through the interface. If the device is capable to generate its public/private key pair, the public key is added by the admin during the registration process.

The manager verifies that the device is not already registered in the device list. If the device with provided credentials already exists in the device list, the registration request will be denied and an error message will be returned to the requester.

Manager checks if the public key was provided in the registration process. If the public key is provided it continues with registering the device to the device list step. If the public key is not provided, the Manager registers the requested device in the device list and sends key generation request to the device gateway. A gateway receiving the request generates a public/private key pair for the device, saves generated key pair associated with the device Universally Unique Identifier (UUID), and sends generated public key to the manager. The manager registers the device's public key into the device list, signing the device list with its public key. After all steps manager publishes the latest version of the device list to the tangle network.

3.2.2. Revoking the device from the system

The admin user can request to revoke a specific device from the system. This can be due to malicious software/hardware of the device, the component, or simply due to the changes in the IIoT environment's architecture. The process is detailed on the sequence diagram illustrated on Fig. 5.

The device should be revoked from the system and all access control rules for it should be reset. For that matter is needed to revoke both the device from the device list and the key pair generated in the gateway. If the key is not generated in the gateway it skips the key revoking steps and jumps into device list revoking as shown on the sequence diagram illustrated on Fig. 5.

For revoking the device, the Admin user inserts UUID of the device that needs to be revoked from the device list, which existence should be verified by the manager, then sends revoke request to the device gateway. If it does not exist the request will fail and an error will be returned.

Receiving a request the gateway verifies that the key pair for the requested device exists on the gateway. If the key pair exists, the gateway revokes keys of the device otherwise, a response will be sent to the manager. The manager revokes the device from the device list and signs it. After all, latest device list should be published to the tangle network.

3.2.3. Disable/restore the device

There can be a case when is needed to disable the device temporarily for maintenance reasons and prevent communication with it. For not doing any extra actions such as revoking the keys and regenerating them later, it will just revoke the device from the device list to prevent communication with it. So only 2 main components will participate in the process as illustrated on Fig. 6.

To start the process in the system, the admin user sends a request containing the UUID of the device for disabling it. By getting a request, the device manager verifies if the device exists in the device list, and if it does not exist, it returns a response with an error message. After confirmation, the manager revokes the device from the device list, signs it, and publishes the latest device list to the tangle network.

During the restoring process, the device restores request will be sent to the manager to add the device to the device list. If the key pair was generated on the device, the public-key should be pro-

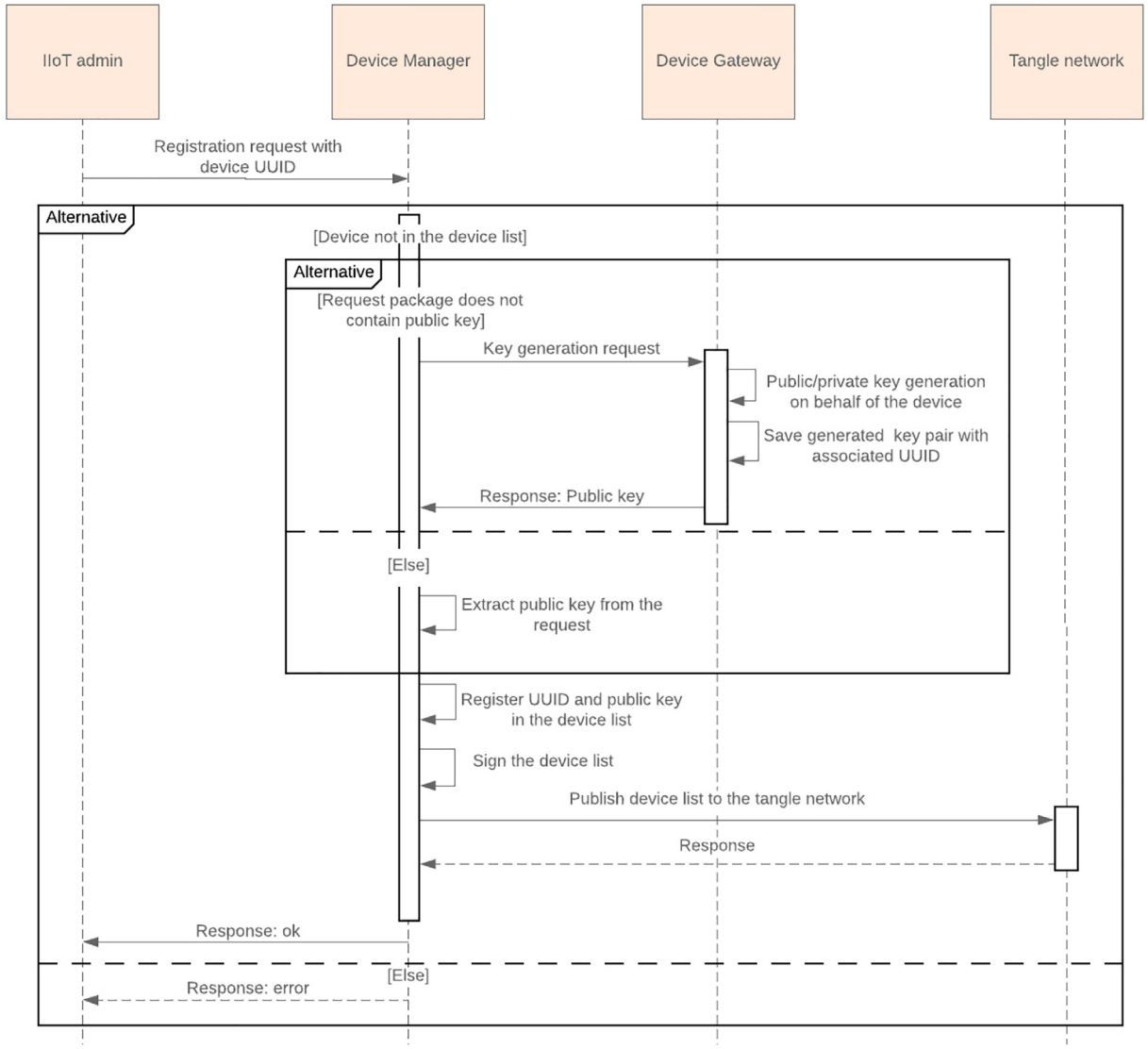

Fig. 4. Sequence diagram: device registration in the system.

vided in the restore request. If not the manager will request the public key of the device from the gateway and will publish the latest version of the device list to the tangle network.

3.2.4. Communication in between 2 devices from different device groups

The communication between two devices from different device groups is organized through the device group gateways. There are 4 main components participating in the communication flow: sender and receiver devices and their gateways.

As mentioned earlier in the architecture, illustrated on Fig. 3, the communication is performed via tangle network. The sender will generate the package that needs to be delivered to the receiver. The package should have the receiver specified as the destination. The sender light node first sends the package to its gateway. Normally, as the sensors are using non-standard industrial protocols for communication, the package will be sent to the translation module of the gateway first. After being converted to the HTTP, the gateway will issue a transaction to the tangle on behalf of the sender light node. After the transaction is confirmed on the tangle, the destination device group gateway will read the transaction, translate it to the appropriate protocol and send it to the destination light node.

More detailed actions performed during the communication process are shown on the sequence diagram represented on Fig. 7.

The sequence diagram illustrated on Fig. 7 is showing the steps performed to deliver data from device A to device B. The tangle network is pictured as a separate node on the diagram, which is just meant to show its role in the system. In the implementation of the solution, the full nodes will be IOTA Hornet nodes and they will be forming the tangle network.

The proposed architecture is flexible enough to adjust to future transformations, brought by the rapid development of the IIoT field, such as eliminating the device group gateways and allowing the light nodes to directly publish transactions to the tangle. This scenario can be achieved when the light nodes will have the required processing power to handle all the processes of the workflow described above.

The lack of standards for IIoT communication protocols brings challenges that can be addressed with the described translation modules in the gateways. This type of semantic gateway will make the system agnostic to the protocol related limitations and will make the system more homogeneous.

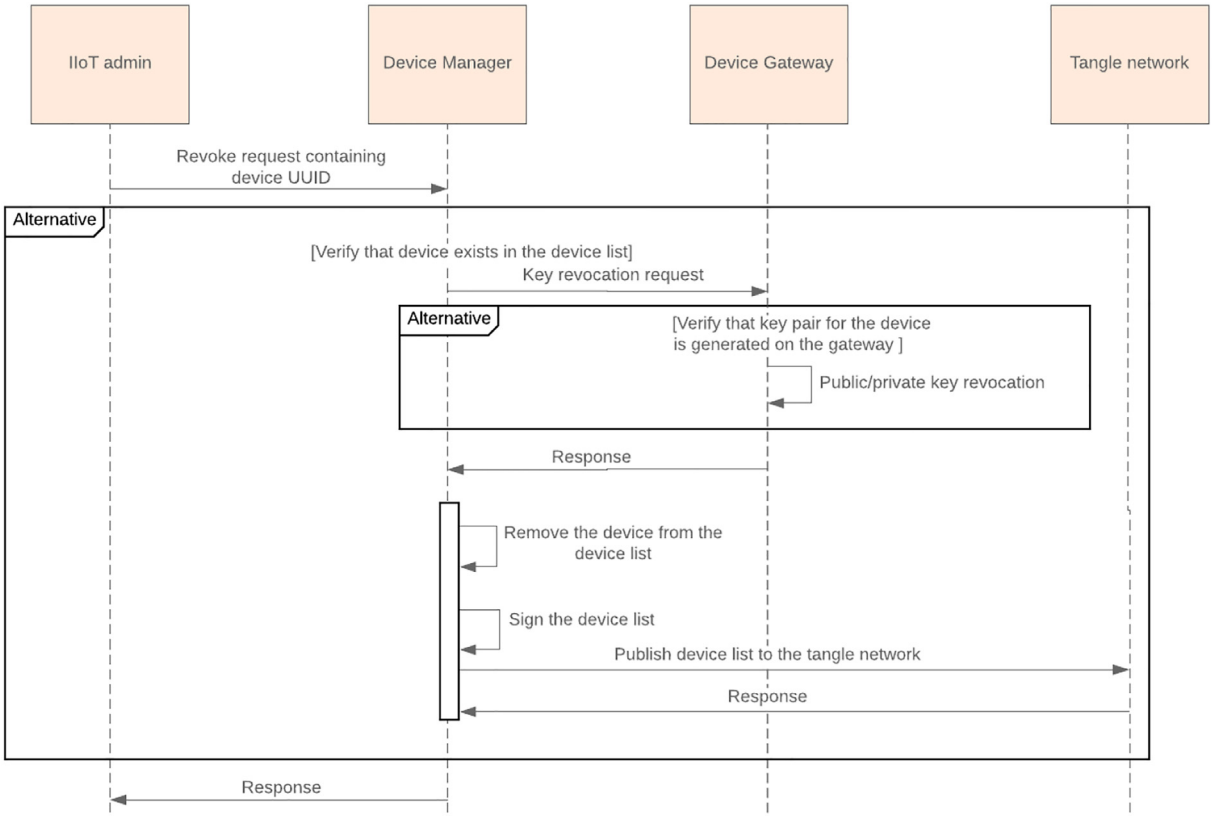

Fig. 5. Sequence diagram: revoke the device.

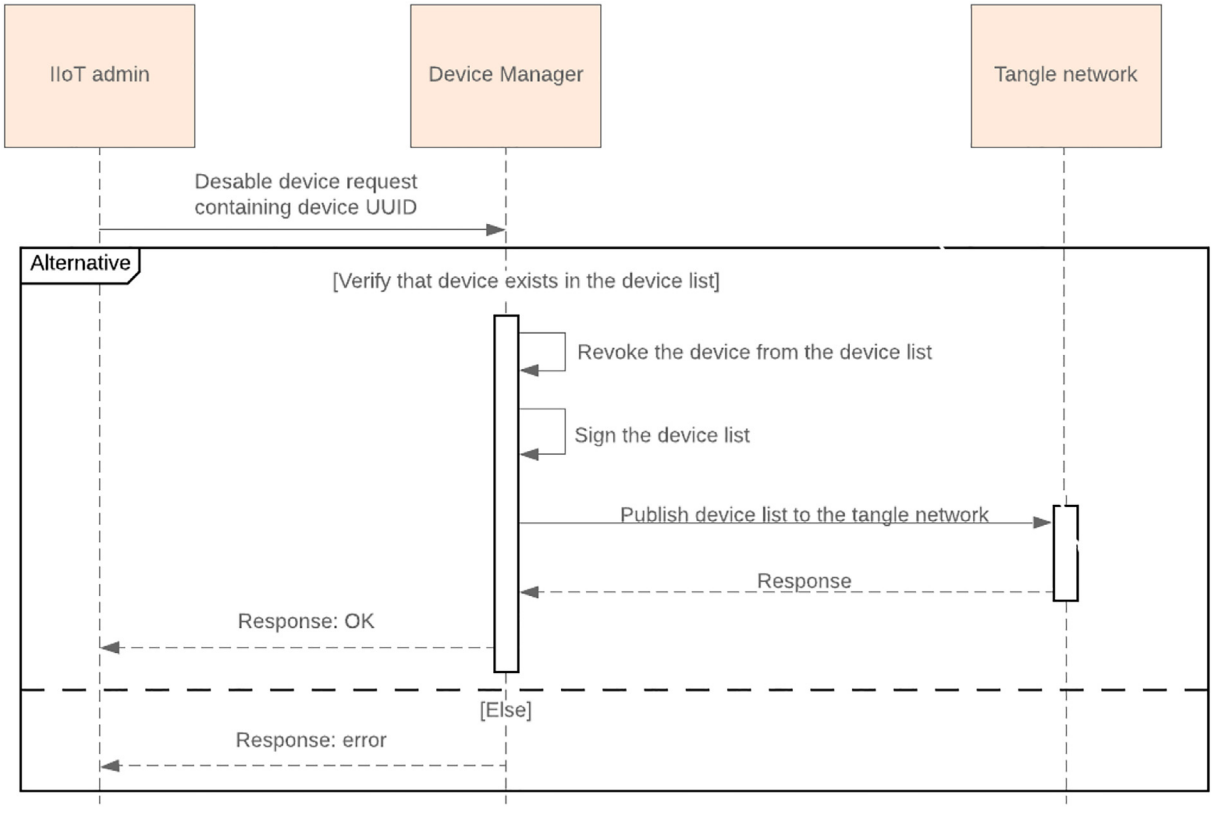

Fig. 6. Sequence diagram: disable the device.

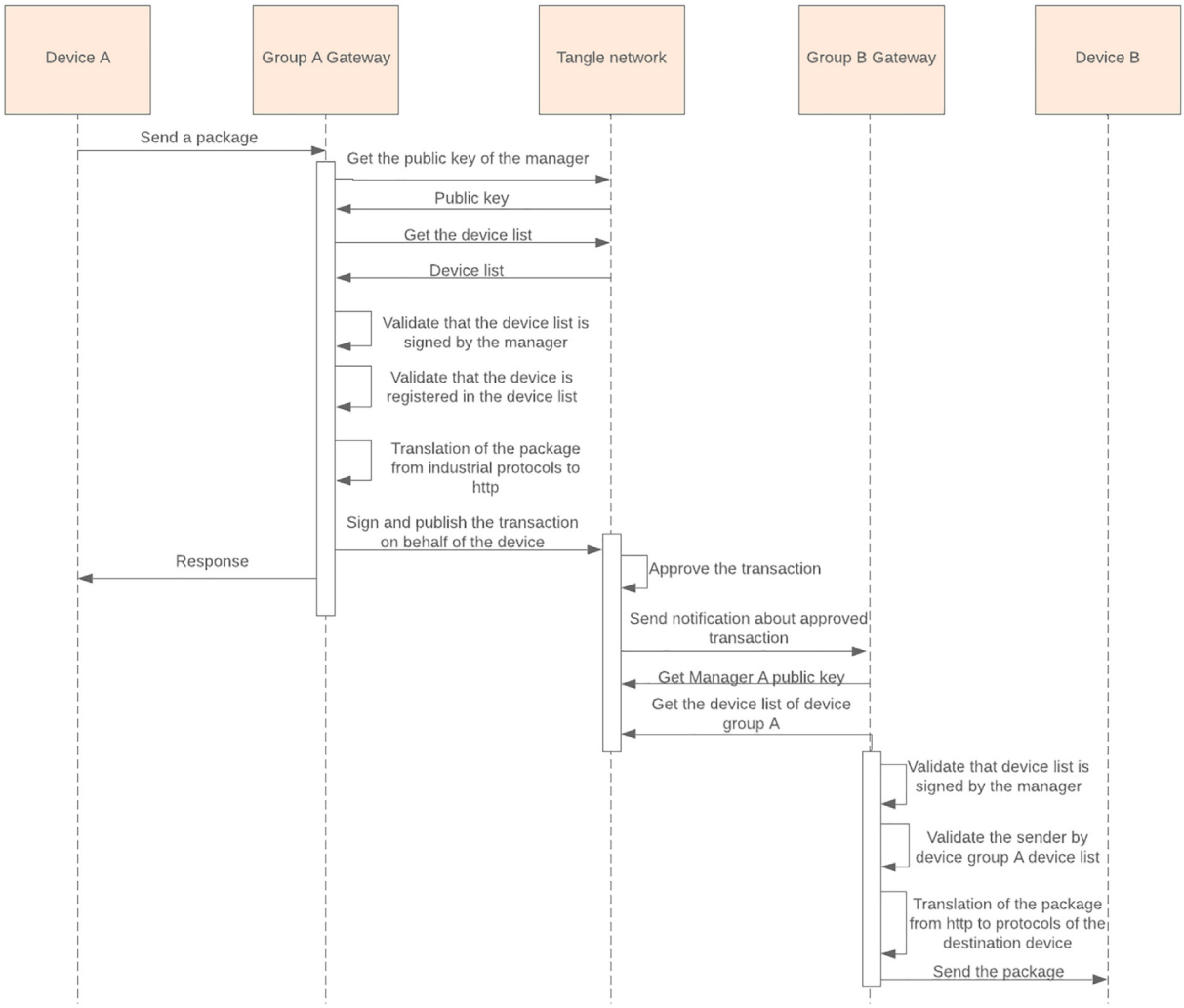

Fig. 7. Sequence diagram: communication between 2 devices from different device groups.

3.3. Bootstrapping the system

The IOTA open-source distributed ledger is used for our implementation. The tangle is IOTA's network used to immutably record data exchanged between the nodes. A private tangle setup was chosen, which allows to have an isolated network and to ensure that it is accessible only for the known nodes in our environment. Also, the current architecture allows having a shared private network between multiple factories or industrial environments that will serve as a communication method in between them.

For testing purposes the minimal tangle network setup should include the following components:

- Coordinator (Coordicide) – Is a node that periodically issues milestones. These milestones are used by the nodes to confirm transactions. The coordinator's role is to protect the network from double spending attacks, while the network does not have enough cumulative hashing power to protect itself. However, it is considered to be a single point of failure and also a single point of attack. If it stops working or is taken over by the attacker, confirmations of transactions will be suspended. Considering all those disadvantages, the coordinator will be eventually removed from the IOTA network. There is an improved version of the Coordinator used nowadays, called Coordicide [21].
- Spammer – Is a node that periodically sends 0 value transactions, meaning transactions not containing IOTA tokens just to keep the minimal message load on the network to support approval of the transactions.
- Hornet nodes – The regular IOTA node, which is exposed to the network through IOTA protocol. It can peer with other nodes, be recipient or sender of the messages on the network. For testing the communication scenario of the proposed architecture, at least 2 hornet nodes should be deployed. Hornet is the second version of IOTA node implementation. The first generation implementation was called IRI node. Hornet claims to be more lightweight, with much less resource consumption and much higher performance.

All components are set up and running in docker containers. For bootstrapping the private tangle the components need to be set up and configured according to IOTA's documentation [22].

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, also known as the Hornet nodes, 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 to be able to do the verification checks during the future communications. If for some reason, the manager will

Table 2
Spoofing threats.

Component	Attack	Risk
Light node (sensor/ actuator)	Impersonate the light nodes	Injection of fake info. to the system, performing actions, and sending commands to different devices.
	Steal digital identity	Performing any actions through vulnerabilities in the hardware or software of the light node.
Device group manager	Steal digital identity	Any device can be injected into the system and gain access to perform various actions by using a private key of the original manager.
Device group manager & gateway	Steal digital identity of a tangle node	By stealing the seed of the node gains rights to publish fake transactions to the private tangle network of the system.
Device gateway	Faking the identity of the gateway	Performance of various actions in the system by masking as a device gateway (taking over the key generation functionality, publishing transactions, etc.).
Admin panel	Gain control over admin panel on its behalf	Registering, revoking, or disabling devices from the system by gaining control over the admin panel, causing partial or full failure of the system.
Tangle network coordinator	Steal the seed	Sending fake milestones and disrupt processes in the tangle network by stealing the seed.

Table 3
Tampering threats.

Component	Attack	Risk
Light node (sensor/ actuator)	Modification of collected data stored on the node	Physical attacks modifying the environment and components of the sensor responsible for the environment analysis
	Man in the middle attack	Sent packages can be modified, causing delivery to nods that shouldn't have access or receive it with fake data and source.
	Modification of configurations on the sensors	Nodes produce fake data, send/perform commands, can cause unexpected behavior in the physical world.
Device group manager	Modification of the private key	May cause a DoS for the devices as the manager key will not be recognized in the system.
	Modification of the stored device list	Nodes can be added or removed from the system which opens up a risk of injections to the information disclosure and DoS attacks.
Device gateway	Modification of the stored device keys	May cause a conflict in the authentication process.
	Modify the packages	Sent packages can be modified, causing delivery to nods that shouldn't have access or receive it with fake data and source.
Admin panel	Modify requests to register/ revoke devices	May cause DoS for the nodes that are revoked or inject untrusted devices into the system.

Table 4
Repudiation threats.

Component	Attack	Risk
Device group manager	Publish device list to the tangle	The device list can be published without a signature or with a fake one attempting to affect the authentication mechanism of the system.
Device gateway	Publishing packages with fake signature to the tangle	The receiver may not be able to identify the sender if the signature is not recognized in the system or may accept the package with a faked signature of a trusted node in the system.
	Sending packages with the fake signature to the light nodes	The monitoring system will not be able to track the source of the package that resulted in the misbehavior of the destination node.
Admin panel	Create and use fake admin account	Attacker may gain the same privileges in the system as the original admin users.

change or the key pair will be regenerated, a new public key will be published by the manager and all the nodes with an 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 a read request for the public key of the manager.

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

4. Security evaluation

Security was integrated during all the phases of development. To reason how security resilient is the proposed solution, a thorough threat analysis was made, based on STRIDE methodology to identify possible attacks, risks, and mitigation per type of the component of the suggested architecture.

For each considered threat a table resuming the attacks and risks was created, for Spoofing Table 2, for Tampering Table 3, for Repudiation Table 4, for Information Disclosure Table 5, for Denial of Services Table 6 and for Elevation of Privileges Table 7. For each threat is also presented the mitigation for the attacks and risk scenarios described.

The mitigation for the attacks and risk scenarios described on Table 2 are explained as follows. Mitigation on the attack scenario on light nodes organized by having a manual registration of each device in the device list and performing authentication of the node in the communication flow. As well as having an intrusion detec-

Table 5
Information disclosure threats.

Component	Attack	Risk
Light node (sensor/ actuator)	Device breach by exploiting the software/ hardware vulnerabilities	A leak of information stored on the device, causing the loss of confidential information about the state of the system or functionality of the node.
	Sniffing the communications	Access to all exchanged data of the node by attacking the communication network between the light node and gateway.
Device group manager	Sniffing the communications	Possible to collect confidential information of devices like UUID and collect public keys of registered devices by sniffing communication between the device manager and the gateway.
	Stored data disclosure via software/ hardware vulnerabilities	Information about the existing environment and its' components can be collected by gaining access to the stored data such as the latest device list.
Device gateway	Unauthorized access to the exchanged data packages	Can be collected information of generated public keys for newly registered devices or exchanged data packages.
	Stored data disclosure via software/ hardware vulnerabilities	Extraction of all the key pairs generated on the gateway for all the devices existing in the environment.

Table 6
Denial of service threats.

Component	Attack	Risk
Light node (sensor/ actuator)	Physical attack on the node	By damaging device or connectivity can cause availability issues and stop the normal its operation by flooding and exploiting vulnerabilities.
Device group manager	Causing loss of the device list	Loss of device list may cause DoS for all the devices trying to register to the system or requested to be revoked/ disabled.
Device group manager, Device gateway	Flooding	Flooding of the network will result in the DoS, as services wouldn't be able to accept requests, or the exploiting vulnerabilities stop the normal operation of devices.
	Physical DoS attack	Attacks on the full nodes may cause damage to the servers hosting those components.
Admin panel	Revoke existing devices, managers, and gateways	This attack affects the authentication mechanism directly, as any revoked component will not pass the authentication in the system.
Tangle network coordinator	Remove the seed	By removing the coordinator seed the snapshots for the decision making process would not be generated causing DoS and downtime of the overall infrastructure.

Table 7
Elevation of privilege threats.

Component	Attack	Risk
Light node (sensor/ actuator)	Gaining access to the device configuration	Unauthorized configuration changes can be made leading to misbehavior of the host or open up the backdoor.
Device group manager	Abuse component's functionalities by exploiting vulnerabilities in the underlying operating systems, services, and hardware	By targeting the business functionality of the manager, internal actions can be performed that were not allowed by design. the key creation functionality can be taking over, letting out device gateway from the registration process.
Device gateway	Abuse component's functionalities by exploiting vulnerabilities in the underlying operating systems, services, and hardware	By targeting business functionality of the gateway attacker can perform unauthorized actions such as publishing the device list or removing generated device keys.

tion system combined with suggested security solutions. Any misbehaving nodes will be reported to the admin automatically. According to the architecture, for the light nodes that do not have the capability to generate their keys, these attacks may result in a stolen UUID that belongs to the device but not the credentials, as they are generated and stored on the gateway.

The attack on the Device group manager is hardly identifiable as no violation of the rights was performed and the mitigation of this attack is storing the manager key securely by using encryption mechanisms. But described attacks on Device group manager and Device gateway can be easily mitigated by the suggested architecture as the node reading the transaction will perform validation of the signature of the package that will allow identifying the faked identity of the source.

The last two attack scenarios on the Admin panel and the Tangle network coordinator can be mitigated, accordingly, by physically securing the admin credentials, isolating the admin panel from the public network, and in the last scenario, storing the seed securely, for example in an encrypted format.

To mitigate described threats (explained on Table 3) on the light node, it is necessary to organize protection on a physical level as well as adding a trusted data channel by having an isolated private network between the light nodes and the gateways. Access to the configurations of the nodes must be protected by a secure password if it can be configured via web or protected physically in the industrial environment.

The mitigation of attacks on the device group manager like modification of the private key and stored device list are as follows. First of all, storing the manager key securely by using encryption mechanisms or secure cloud storage. As in addition to the proposed security solution, a verification process can be implemented to compare the latest version of the published device list to the

modified one by taking into account the requests received from the admin.

For mitigation of attacks on the Device, the gateway needs to take measures like checking keys integrity by keeping a hash of the device key pair. For the mitigation in case of a network attack, there is an HTTPS secure protocol.

The last component analysis is on the Admin panel where attacks can be mitigated by having standard security mechanisms that ensure the secure data exchange in the private network.

The mitigation of the attacks (explained on Table 4) on the Device group is a validation of the signature procedure. Whenever any of the components will read the device list from the tangle network, the signature will be validated by using the public key of the manager placed on the tangle network.

To mitigate the attacks on the Device gateway, it is necessary to perform a validation of the sender by checking the package signature and if it is not valid, the package is dropped. Device gateway is considered a trusted node for the light nodes. As most of the light nodes do not have the capability to perform any authentication procedures, this risk can not be mitigated.

This attack on the Admin panel can be mitigated by using best practices in security in the development process of the admin panel and having a well defined secure flow for the registration of the admin in the system.

To mitigate the attacks (explained on Table 5) on a light node has to be ensured that the device is not accessible by not authorized parties and the confidential information has to be stored in an encrypted format. Also, a secure communication path has to be provided between software and hardware components since mostly they will be placed on the same sector of the private network in the industrial environment.

Mitigation for the Device group manager can be performed by using secure communication protocols for the communication between full nodes and storing the confidential information in an encrypted format.

As mitigation on Device gateway, confidential information has to be stored and exchanged in an encrypted format. Also, some standard network security measures are required.

To mitigate the attacks (explained on Table 6) on a light node can be performed by physical accessibility limitations in the industrial environment, the deployment of IDS and fail-over mechanisms can help to mitigate other types of DoS attacks.

As mitigation for the attack on the Device group manager in the implementation of the suggested architecture the scenario of the data loss recovery should be added. When the manager will detect a missing device list it can be requested from the tangle and restored on the manager. The deployment of IDS and fail-over mechanisms can help to mitigate other types of DoS attacks.

To mitigate described attacks on the Device group manager and gateway the firewall should be configured to drop the traffic or limit the size of incoming ping requests, also IDS and fail-over mechanisms can help to mitigate other types of DoS attacks. In the case of servers being located in the industrial environment, special access rules have to be defined, if they are hosted in a cloud, the service provider should ensure the accessibility of the service.

The attack on the Admin panel can be identified and mitigated by intrusion detection systems identifying anomalies in the behavior of any of the components of the system.

Mitigation of the attack on Tangle network coordinator is having the seed backup stored securely outside the node itself for the seed recovery scenario.

To mitigate the attacks (explained on Table 7) on light node configuration panels of the nodes should be isolated from the outer world and be accessible only for the authorized parties.

To mitigate the risks (explained on Table 7) on Device group manager and Device gateway, roles of the components should be defined and access control should be implemented.

After applying the STRIDE the main risks, mitigation, and also open challenges are presented and discussed. As full nodes of the tangle network have more responsibilities in the system they have the highest risk for attacks. By attacking the full nodes of the tangle network an additional vector of risk opens up which can be described as follows:

- Full node generating transactions tips that will prioritize the attacker's transactions over the regular tip selection algorithm.
- Double spending attacks that are making the coordinator send inconsistent milestones. The nodes will detect the inconsistency in the milestones and will stop the decision making and transaction confirmation processes.
- The full nodes stopping the milestones transactions distribution process which will cause a freeze in the transactions confirmation processes.

Due to dependencies between the components of the system, the security of the entire system can only be ensured by addressing the vulnerabilities of each component in the system. This section demonstrated the mapping of STRIDE threats to the components of the proposed architecture and attack vectors have been reviewed on various layers. The analysis showed that most of the attacks related to the trust issues in the system already have a mitigation scenario included in the proposed architecture because ensuring trust in the industrial environment was the major goal of the performed work. Attacks related to the vulnerabilities in the hardware or the software of the devices in the industrial environments do not have a trivial mitigation scenario, because most of those devices are not able to receive security updates or critical patches in the runtime. That issue should be mitigated by the producers of the devices. Mitigation of other types of attacks can be achieved by combining various security systems with the suggested solution. Even though some of the hardware, software, or network-level attacks are not addressed directly, some of the attacks will be blocked by confinement mechanisms on the gateway. During the implementation stage of the suggested architecture threats analysis can serve as an input to the designing process of the application. Most important risks should be prioritized and mitigated accordingly.

5. Conclusions

This paper highlights the security threats in IIoT environments, and analyses the state of the art and operation of those systems. Based on the gathered information, it analyses the usage of the blockchain technology in IIoT applications and proposes a solution to improve the secure data exchange in those environments, addressing specific requirements, such as the time and resource critical aspects that have an impact on the type of consensus that can be used on the blockchain. The tangle network is a growing and evolving project used in various IIoT based environments. Another important contribution of the proposed approach is the creation of a STRIDE model to analyze the security of the proposed solution, as well, to enable the future comparison between other solutions that may appear and provide hints of how to address common attack vectors in this scenario. The proposed approach also shows that is possible to progressively bring security to heterogeneous environments with legacy devices that have fewer capabilities.

The proposed solution is based on 2 logical groups: light nodes and full nodes. Light nodes are considered to be unable 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 the industrial environment. Also, they are responsible for publishing transactions to the tangle network on 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 secure communication channels for remote control and data exchange.

The STRIDE threat analysis performed for the proposed architecture has shown that most of the attack vectors falling into the scope of the mitigation mechanisms presented are covered in the designed solution. It also showed the open issues in security that can be covered in the implementation or future work stages.

The proposed solution contributes to the smooth transition from historically fully isolated environments to more automated, interconnected, robust, and secure environments moving towards Industry 4.0. It aims to provide a flexible solution that can be integrated into an existing environment, instead of creating everything from scratch. It takes into consideration not only the security aspects of the currently existing environments but also aims to minimize the work that should be done to achieve the given goal.

Everyday 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 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.

At the moment, the automation of bootstrapping scenario is being automated. The goal is to provide an easy way to provision and configure a test environment of the designed solution for anyone who wants to perform extensive testing and development of real-life scenarios.

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.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

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..
[2] Industry 4.0 technologies: Implementation patterns in manufacturing companies, International Journal of Production Economics 210 (2019) 15–26. doi:https://doi.org/10.1016/j.ijpe.2019.01.004..
[3] E.A. Lee, Computing foundations and practice for cyber-physical systems: A preliminary report, University of California, Berkeley, Tech. Rep. UCB/EECS-2007-72 21..
[4] X. Fan, K. Fan, Y. Wang, R. Zhou, Overview of cyber-security of industrial control system, in: 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), 2015, pp. 1–7, https://doi.org/10.1109/SSIC.2015.7245324.
[5] Industrial internet of things, Recent advances, enabling technologies and open challenges, Computers & Electrical Engineering 81 (2020), https://doi.org/10.1016/j.compeleceng.2019.106522 106522.
[6] A. Gilchrist, Industry 4.0: The Industrial Internet of Things, Springer, 2016.
[7] X. Fan, K. Fan, Y. Wang, R. Zhou, Overview of cyber-security of industrial control system, in: 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications, SSIC 2015 – Proceedings, 2015, pp. 1–7, doi:10.1109/SSIC.2015.7245324..
[8] Iota org website. https://www.iota.org/..
[9] M. Frustaci, P. Pace, G. Aloi, G. Fortino, Evaluating critical security issues of the IoT world: Present and future challenges, IEEE Internet of Things Journal 5 (4) (2018) 2483–2495, https://doi.org/10.1109/JIOT.2017.2767291.
[10] D.G. Pivoto, L.F. de Almeida, R. da Rosa Righi, J.J. Rodrigues, A.B. Lugli, A.M. Alberti, Cyber-physical systems architectures for industrial internet of things applications in industry 4.0: A literature review, Journal of Manufacturing Systems 58 (2021) 176–192, https://doi.org/10.1016/j.jmsy.2020.11.017.
[11] P. Neumann, Communication in industrial automation-What is going on?, Control Engineering Practice 15 (11) (2007) 1332–1347, https://doiorg/10.1016/j.conengprac.2006.10.004.
[12] S. Hong, M. Lee, CNSR 2010 Proceedings – 8th Annual Conference on Communication Networks and Services Research, doi:10.1109/CNSR.2010.52..
[13] A. Baliga, Understanding Blockchain Consensus Models, Whitepaper (April) 1–14..
[14] Z.J. Williamson, The AZTEC Protocol, Whitepaper (2018) 1–24.
[15] Iota tangle: A cryptocurrency to communicate internet-of-things data, Future Generation Computer Systems 112 (2020) 307–319, doi:https://doi.org/10.1016/j.future.2020.05.047..
[16] A. Churyumov, Byteball: A decentralized system for storage and transfer of value. https://obyte.org/Byteball.pdf..
[17] J. Huang, L. Kong, G. Chen, M.-Y. Wu, X. Liu, P. Zeng, Towards Secure Industrial IoT: Blockchain System with Credit-Based Consensus Mechanism, IEEE Transactions on Industrial Informatics 15 (6) (2019) 3680–3689, https://doi.org/10.1109/TII.2019.2903342.
[18] K. Tuma, G. Calikli, R. Scandariato, Threat analysis of software systems: A systematic literature review, Journal of Systems and Software 144 (February) (2018) 275–294, https://doi.org/10.1016/j.jss.2018.06.073.
[19] R. Khan, K. McLaughlin, D. Laverty, S. Sezer, Stride-based threat modeling for cyber-physical systems, in: 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), 2017, pp. 1–6, https://doi.org/10.1109/ISGTEurope.2017.8260283.
[20] A. Sukiasyan, Secure data exchange in IIoT, Master Thesis in Information Systems – Polytechnic Institute of Bragança. http://hdl.handle.net/10198/19785..
[21] S. Popov, H. Moog, D. Camargo, A. Capossele, V. Dimitrov, A. Gal, A. Greve, B. Kusmierz, S. Mueller, A. Penzkofer, O. Saa, W. Sanders, L. Vigneri, W. Welz, V. Attias, The Coordicide, IOTA Foundation..
[22] I. Foundation, Deploy a (hornet-based) Private Tangle in one click, https://docs.iota.org/docs/hornet/1.1/tutorials/one-click-private-tangle/ (Online; accessed 15-January-2021), 2020..

Anna Sukiasyan is an alumni in Information Security from the National Polytechnic University of Armenia and in Information systems from the Polytechnic Institute of Bragança. She is a researcher in the field of Information Security. Also, she has experience in the software development field. Currently specializes in Operations and Systems Engineering. She develops research in the area of Information Security as well as Industrial IoT and IoT in general.
The preferred areas of activity are: Architecture and design of robust scalable, reliable and secure enterprise systems. Incident management. Improvement of the existing infrastructures. Cloud migrations and automation. Implementation of various DevOps practices. Huge infrastructure as a code lover and an open source enthusiast.
Research topics: Cybersecurity and Information Security; Secure Architectures; IIoT.

Hasmik Badikyan holds her Bachelor's and Master's Degrees in Information Security, both at National Polytechnic University of Armenia (NPUA). She also holds a Master's in Information Systems at Instituto Politécnico de Bragança (IPB), Portugal. Currently she is a researcher at the Research Centre in Digitalization and Intelligent Robotics (CeDRI) at the same institution where she participates at Intelligent and Predictive Maintenance in Manufacturing Systems (Maintenance 4.0) project.

Tiago Pedrosa is a Ph.D. in computer science from the University of Minho, Aveiro and Porto, and a Bachelor in informatics engineering from the Polytechnic Institute of Bragança. He is adjunct professor, researcher and consultant in the field of cybersecurity and information security at the informatics and communications department of School of Technology and Management of the Polytechnic Institute of Bragança. He is also Chief Information Security Officer, Coordinator of the Cybersecurity Competence Center, Coordinator of the Computer Security Incident Response Team and Director of the Short Cycle Course in Cybersecurity. He develops research in the area of applied computer security, integrates projects, makes technology transfer and consultancy. He has several published scientific works, he supervises several masters, bachelor and internships.
The preferred areas of activity are: Design of secure architectures, Hardening of systems, services and networks, Implementation and management of Intrusion Detection and Prevention Systems, Collection and Analysis of Strategic Information on Computer Security, Computer Security Incidents Response, Computer Security Audit and Pentesting, Forensic Analysis, and administration of systems and networks.
Research topics: Cybersecurity and Information Security; Hardening; Secure Architectures; Security Incident Response; Security Intelligence; Auditing and Penetration Testing.

Paulo Leitao received the MSc and PhD degrees in Electrical and Computer Engineering, both from the University of Porto, in 1997 and 2004, respectively. He joined the Polytechnic Institute of Bragança in 1995, where he is Professor at the Department of Electrical Engineering. His research interests are in the field of intelligent and reconfigurable systems, cyber-physical systems, Internet of Things, multi-agent systems and self-organized systems. He participated in several R&D projects (e.g., EU GO0DMAN, PERFoRM, ARUM and GRACE) and Networks of Excellence (e.g. IMS and CONET), served as general co-chair of several international conferences, namely IFAC IMS'10, HoloMAS'11, IEEE ICARSC'16 and SOHOMA'16, and published more than 200 papers in international scientific journals and conference proceedings. He is co-author of three patents and received four paper awards at INCOM'06, BASYS'06, INDIN'10 and INFOCOMP'13 conferences. Dr. Leitao is Senior member of IEEE Industrial Electronics Society (IES) and Systems, Man and Cybernetics Society (SMCS), past Chair of the IEEE IES Technical Committee on Industrial Agents and member at-large of the IEEE IES Administrative Committee (AdCom). Currently he is chair of the IEEE Standards Association P2660.1 Working Group.