INTEGRATION OF SAFETY MEANS WITH FUNCTIONS OF BLOCKCHAIN IN MULTI-LAYERED ARCHITECTURE OF IOT FOR SAFER DATA TRANSMISSION PROCEDURES

Raimundas Savukynas

Institute of Data Science and Digital Technologies,
Vilnius University, Vilnius, Lithuania

ABSTRACT

The launching and linking process of heterogeneous objects to the Internet of Things (IoT) is related to some important problems of the identification, authentication for ensuring safety over the wireless connections. The possibilities of connections to the IoT differ in a broad spectrum of different equipment, the functionality of objects, communication protocols, etc. This research study is related to the implementation of safeguard algorithms on the first stages of object identification and authentication before the permission stage for launching into the working area of the IoT. The application domain is related to the requirements for the safety of the multi-layered infrastructure of objects by linking to the whole IoT. Such infrastructure became more complex according to the risks of very unsafe possibilities. The aim of this research is to evaluate some safety means related to the identification and authentication stages of objects by integrating them with the functionality of blockchain. The objectives of this research are related to the development of more safety working algorithms by representing the stages of checking of the identity of objects. The results demonstrated integration possibilities of implementing the blockchain functionality for establishing and managing the operational rules for pre-connection stages of objects to the IoT. The paper shows new results of developing protection means for ensuring reliable communication in the transmission of outgoing confidential data and transmission data integrity from different smart objects. As a result, components of necessary functional capabilities of the communication of IoT are developed by intending to ensure the safety and reliability of the wireless connection of objects.

KEYWORDS

Internet of Things (IoT), data transferring, smart environment, safety means, distributed databases.

1. INTRODUCTION

The research area is related to the problems of solving of more secure communication and data transferring process of IoT on the stages of identification and authentications of smart objects. The communication of objects in the IoT environment is often interfering with some disturbances and unsafety threats under the wireless and smart conditions. The insecurity can occur when disturbing radio communication channels, inserting fake network nodes, performing unsafe actions with sending data aggregation, implementing of the authorizing information changes in the network [11], [24], [42], [43], [51]. The violations can occur when the exhausts of energy supply occur during attacks. The essential aspects of safety are the privacy and safety of transferring processes when data scanned from the smart equipment [52]. The smart sensors are

David C. Wyld et al. (Eds): CCSEA, BIoT, DKMP, CLOUD, NLCAI, SIPRO - 2020
pp. 33-50, 2020. CS & IT - CSCP 2020 DOI: 10.5121/csit.2020.101004

working on wireless networking background and can be easily applied for unauthorized activities. The smart sensors have possibilities for the provision of unsafety and dangerous actions with the secret data implementation. The creation of a trusting and intelligent environment, internet-based items of things are required for secure and intellectual services. The objects have equipped with smart decision-makers, interacting agents. The IoT itself can act as a large multi-agent system, as well. One of the most critical issues currently being addressed is the development of multi-agent systems for control of embedded smart environments by ensuring the safety of systems through the interface. The intelligent environment should be backgrounded to ensure the safer operations of integrated into the IoT heterogenic objects and support more safety communication. The implementation of intelligence elements in the system could exploit the recently-expanded multi-agent systems [1], [2], [13], [19], [37].

The possibility of integration of safety means with blockchain functions described in this paper by proposing the extension of obtaining algorithms, which help avoid some types of IoT risks. The spectrum of threats has a variety of possibilities, and the detection process became complicated. The experimentation with the concrete simulation modeling environment has restrictions on the detection of hazardous activities. But some types of risks are described as flood or de-synchronization attacks, which can be carried out and revealed by [54]. The safety requirements vary significantly from the scope of functional possibilities of integrating objects. The requirements, according to the Internet Protocol for Smart Objects (IPSO) Alliance, can help in developing secure communication of smart objects [49].

The approach is based on the multi-layered structure of identification and authentication of IoT objects by implementing some functions of the blockchain technology to search, record and delete data, as the black box with the implementation of outside functions of the blockchain. The objects have to interact in a smart environment of IoT only on the application level [32]. The protocols ensure access to information of authorized users, reliability of the messages between senders and receivers, and transmission of the data at any time [18]. Some types of vertical safety means are analyzed. The results of using blockchain methods for safety communication described on the level of step-wise algorithm development to ensure safer communication between IoT objects in their data transferring process [55]. Another critical factor is the impact of safety methods, which are implementing in the creating of safety techniques [6] for safer IoT by providing structures for more safety mechanisms. The safety should be ensured at all levels of the protocols and middleware.

The analysis performed how the object integration stacks and protocols have to be created to ensure the maximum level of protection, and based on the defined guidelines, a method of IoT objects identification and authentication was developed in the Fog computing layer by using functions of blockchain technology. The open-source systems and tools have selected for the method, which allows the developed prototype to be transferred to cloud or virtualization platforms and used for functionality development [30]. The architecture is modular, supports the possibility of extensibility of functions, and allows adding new specialized servers or containers to the fog layer. The information received during message processing from the objects is transmitted to the aggregation servers, systems, or applications to perform further operations with the received data. The use of the representational state transfer (REST) application interface (API) server allows operations to be performed in a blockchain, so new system components can use defined API references to provide additional functionality. The ability to receive AMQP messages in the RabbitMQ broker also implemented, but this broker can also receive messages sent using the MQTT and STOMP protocols. This method is not adaptive to the IoT objects, which requires additional manual configuration.

2. RELATED WORKS

The safety dimension is a key issue for developing of smart environments of IoT, especially considering the means for the protection of this environment, because integrated objects and control software have possibilities to interact with people and other objects in the environment. Therefore, it is necessary to ensure safety between the IoT objects for equipment safer and reliable communication, but also to ensure safety in the sense of the intelligent environment [59]. The information safety model typically consists of three components proposed [33] as confidentiality, integrity, and availability (CIA). Although this model has traditionally used in conventional systems, it is also fully suited to intelligent environments for online content control systems. Confidentiality ensures that information is available to authorized users [50]. As a general rule, confidentiality is realized by blocking information or restricting access to this information [35]. Integrity ensures that the data has not been changed without their author's knowledge. Integrity realized using special message integrity codes (so-called hash codes) that allow the message recipient to determine whether it has been changed. Accessibility means that information is available whenever needed. To ensure availability, the system itself must be resistant to various internal errors, failures, and external attacks such as denial-of-service (DoS). As [23] points out, looking at open systems interconnection (OSI) protocol stack levels in practice for every level, there are several threats and attack types:

- at the physical level the Internet of Things objects are susceptible to interference and data packet analysis;

- at the communication level, you can use the MAC protocol for vulnerable causing conflict at the physical level, unloading the batteries of the IoT objects, or simply contaminating the channel so that it is impossible to communicate;

- at the routing level, you can perform: blackhole attacks, at the routing level, you can perform: blackhole attacks, creating network segments where packets are lost.

The wormhole attacks are described in [22], when network nodes are cheated and do not perform standard routing searches, thus preventing important data forwarding, and spoofing attacks when the sender does not pretend to be another person or the IoT object than is a real. The selective forwarding does not reach addressee malicious network nodes pretend to be real network nodes by filtering out certain data packets. The sinkhole attacks are described in [12] when malicious nodes collect data from neighboring nodes by preventing the recipient from receiving packets. The mechanisms of the attacks on flooding "hello" messages described by [58].

An essential aspect of safety is the privacy of people and organizations, as smart environments are immediately embedded in people's living or working environments that can be directly used to collect illegal and secret data on the surrounding environment. The blockchain is used and adapted for their particular properties. The researchers agree [16] that blockchains and networks have distinctive properties and can be used in various applications. The most frequently mentioned and most important advantages of the blockchain [9]:

- accountability - information written into blocks and blocks are chained together, data already recorded cannot be deleted, and data stored in the blockchain can be traced;

- integrity - each node in a blockchain network has a complete copy of the blockchain, so even if the data stored in one or more nodes is changed, the other nodes do not recognize these changes, and which is impractical;

- availability - since a blockchain network distributed and the same information stored on all nodes, once one or more nodes fail, the network can continue to function - all you need to do is read and write to another node;

- confidence - new information is added to the blockchain only when some or most of the network nodes agree on the information to be recorded, using consensus algorithms;

- access - when a network made up of multiple nodes, it can connect to the node to access the information stored on it, thus ensuring fast data access;

- privacy - depending on the application of blockchains, a high level of privacy can be maintained for network users, since it is sufficient to have a pair of cryptographic keys to participate in network activities.

The blockchain network types divided into open and closed [41]. The difference between them who can read the information and add new blocks to the chain. The open blockchain networks used for cryptocurrencies such as Bitcoin [31], Ethereum [4], Zcash [28], Ethereum Smart Contracts [14]. These networks can be accessed by anyone who wants and has the necessary physical and software connections. The participants can “dig” a network currency, create transactions, and transfer money. The open blockchain networks cannot be censored because you need to allocate computing resources, buy currency, or it’s equivalent in the network [45]. As mentioned, the integrity of such blockchain networks ensured through consensus protocols.

The access to closed blockchain networks is restricted, and access is granted only for participants. These blockchain networks can be divided into two groups: public and private [36]. In situations where one has to control who can write to the blockchain, and everyone is allowed to read, it is used in public closed networks. For example, public authorities may store financial or job statements on a blockchain network for transparency purposes and allow the public to view important information, but only employees of the authority are authorized to enter it. When information stored on the blockchain requires access to both read and write, private closed networks are used. In the closed blockchain, nodes with known and trusted identities have the right to process transactions in private blockchain networks, eliminating the need to use PoW or other algorithms to build consensus. In this case, the incentive to process transactions and build blocks is not an obligation, an agreement, or benefit, rather than seeking the cryptocurrency [21].

3. DEVELOPMENT OF CHECKING ALGORITHM FOR SAFER CONNECTION OF OBJECTS INTO THE IOT INFRASTRUCTURE

The proposed algorithm of expression of the extended functionality of the checking process of objects before their connection to the IoT environment is developed with the implementation of safety procedures presented in Figure 1. The blockchain is an append-only database maintained in a distributed fashion by the nodes in the peer to peer (P2P) network. The P2P function implies that there is no central control, and all nodes can communicate directly with each other using an appropriate protocol, allowing for transactions to be exchanged among the peers. Following the recommendations of representation of the hierarchical structure of the blockchain working structure that consisting of four layers, as provided [38]:

- network layer is the bottom layer of computing nodes guarantees that the system can work and ensuring communication blockchain nodes in a decentralized way;

- protocol layer consists of fundamental blockchain technologies, such as consensus algorithms, cryptology methods, and ensures that the system works properly;

- ledger layer is responsible for the primary blockchain mission by transmitting transactions securely and assures that system functions are working correctly;

- application layer provides APIs for the usability of the object's and is responsible for interaction with the blockchain system when needed for the business logic.

The identification and authentication process starts when the object initializes the process of data transmission. The data from object Oi,j,k, transmitted to the Fog layer of the whole architecture. The process of registering and recognizing the object Oi,j,k, is analyzed in a detailed manner. There are important identifiers of Oi,j,k, where i is the identifier of equipment, j is an authentic index of the object, and k indicates the functional status of the object. On the stage of registration object Oi,j,k sends a message to the message broker in the Fog layer, which forwards the message for processing. An object Oi,j,k identifier i consists of the least two variables $i=\{i_1,i_2\}$, where:

- i1 – variable represents the unidirectional function of object hardware;

- i2 – variable represents of usage of a physical unclonable function (PUF).

The fog object receives a message from the object and applies it to the blockchain using an API with a request to verify the object's identity. In the previously proposed structures of recognition of objects at the registration stage [39], were proposed the obtaining process only for checking of the object identifier matching with the registering information in the blockchain. Then data transmitted in the Fog layer for running processes, some checking procedures are included in the recognition process of the proposed algorithm of the object's connection before starting the work process in the IoT environment. The necessary steps needed in the verification procedures for increased safety to start work with a connected object. These three checking procedures are:

- procedure ISCS – is responsible for checking registration conditions of identifier Oi,j,k;

- procedure ACSS – is responsible for checking of authentication conditions;

- procedure SCSS – is responsible for checking of conditions of safety means.

If such types of conditions are not satisfied, the object Oi,j,k removed from the environment, and some activities performed to informing about the unsafety conditions of Oi,j,k, which forwarded to the stage of removal of the object from the IoT environment.

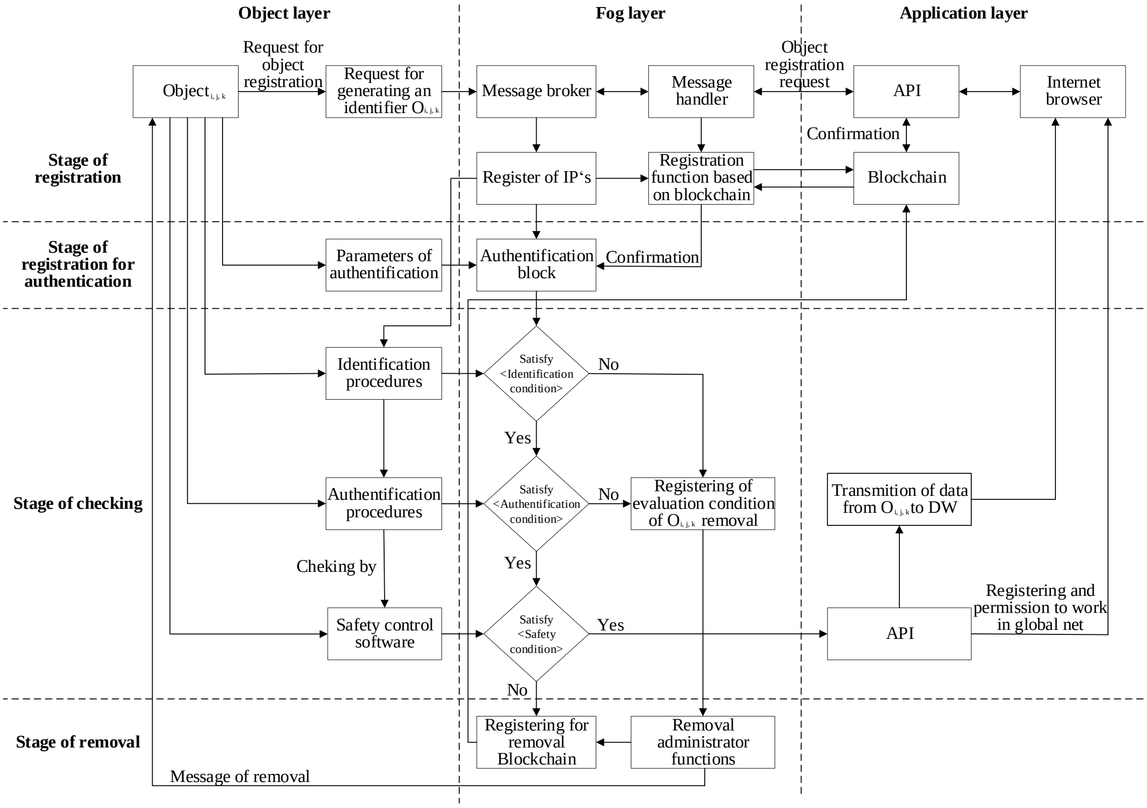

Object layer
Fog layer
Application layer
Request for object registration
Object i, j, k
Request for generating an identifier O i, j, k
Message broker
Message handler
Object registration request
API
Internet browser
Confirmation
Stage of registration
Register of IP's
Registration function based on blockchain
Blockchain
Stage of registration for authentication
Parameters of authentification
Authentification block
Confirmation
Identification procedures
Satisfy <Identification condition>
No
Yes
Stage of checking
Authentification procedures
Satisfy <Authentification condition>
No
Registering of evaluation condition of O i, j, k removal
Transmition of data from O i, j, k to DW
Yes
Cheking by
Safety control software
Satisfy <Safety condition>
Yes
API
Registering and permission to work in global net
No
Stage of removal
Registering for removal Blockchain
Removal administrator functions
Message of removal

Figure 1. Stages of checking of objects before connection to the IoT environment

The registration procedure is initiated by the object and requires sending the name and identifier, which is sent to the message broker, who later forwards the registration message for processing. The object identification and authentication occur each time when the object accesses the Fog layer, and the data transmission process must always be transmitted with the object identifier. The object removal process is performed by the block of system administrator functionality in the Fog layer server if this action is affected by consensus or satisfaction checking activities. The Fog server or administrator functional block can refer to the blockchain by using an API request and remove the object from the blockchain. The structures of the blockchain functionality by implementing the authentication method in the Fog computing side is presented in Figure 2.

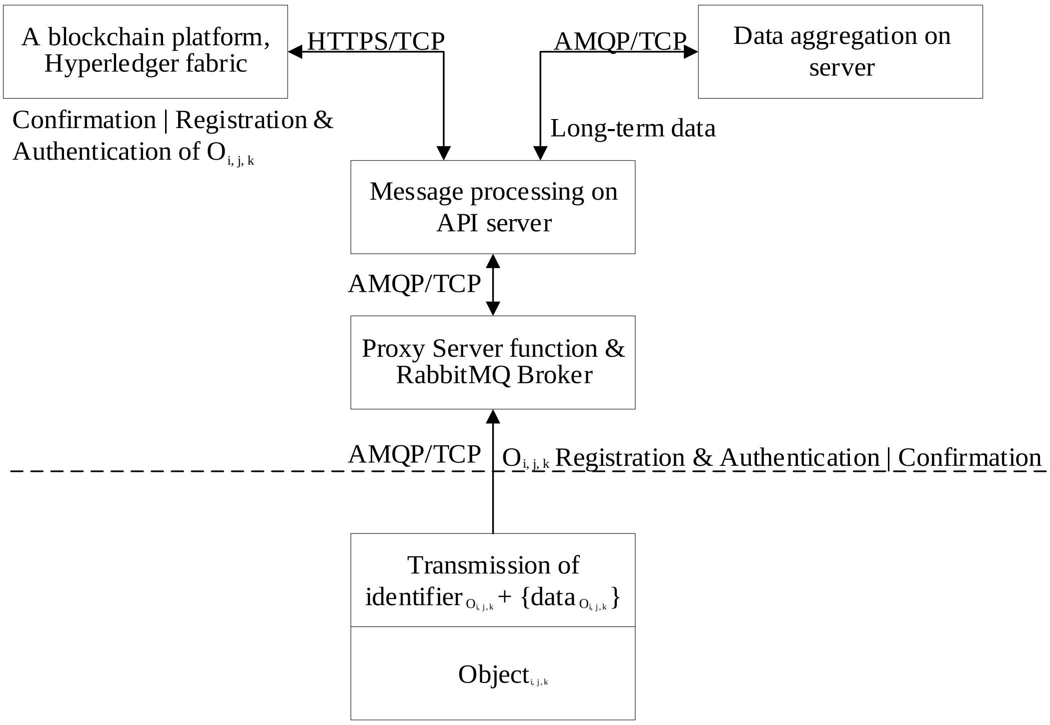

A blockchain platform, Hyperledger fabric
HTTPS/TCP
AMQP/TCP
Data aggregation on server
Confirmation | Registration & Authentication of $O_{i,j,k}$
Long-term data
Message processing on API server
AMQP/TCP
Proxy Server function & RabbitMQ Broker
AMQP/TCP
$O_{i,j,k}$ Registration & Authentication | Confirmation
Transmission of identifier$_{O_{i,j,k}}$ + {data$_{O_{i,j,k}}$}
Object$_{i,j,k}$

Figure 2. A detailed description of the integration of functionality of blockchain with identification and authentication stages of objects of IoT

The fog servers consist of brokerage functions with functions of API, message processing servers, and data aggregation servers. The blockchain platform always operates in the Fog layer [48]. The blockchain servers with the Fog servers exchange data only through the API service calls. The system architecture designed with scalability and the total number of servers running in the computing farm can be increased to expand the IoT system performance and capabilities [56]. This is necessary to adapt to the increasing number of IoT objects, and based on the Fog layer architecture and components study of the data transfer protocols, have to be performed [10]. After comparing some proposals of the existing IoT architecture [5] compatible objects data communication protocols, we would like to propose using the AMQP protocol, which has higher safety, extensive compatibility, and more scalability capabilities.

Three processes are distinguished: object registration, authentication, and removal. The object identifier generated each time the fog computer layer is accessed. The value of the password is not stored on the terminal object, which reduces the risk of password leakage and ensures the identity of the IoT object. The authentication processes performed on the blockchain platform and object authentication information stored on the blockchain.

4. Application of Functionality of Blockchain Technology for the Secure Data Transmission Process

The blockchain is a decentralized transaction storage database system where any broker does not record of transactions. The transaction list stored with all members of the network about funds transfers, issued loans, or property information. The main advantage of blockchain technology is that it is impossible to modify or falsify records. Each block that records the most recent transactions in the form of digital records connects to the previously recorded block in chronological order, thereby forming a blockchain. Each new block is placed only at the end of the circuit and has a past block diagram, as described in [53]. The main aspects of the safety of blockchain technology are openness, safety, and decentralized data storage is presented in Figure 3.

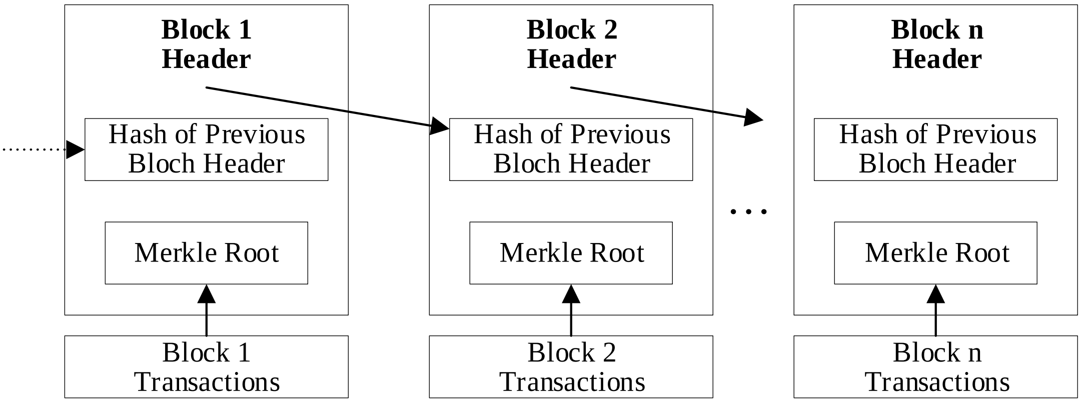


Figure. 3. Simplified blockchain working structure [20]

The blockchain is an append-only database maintained in a distributed fashion by all nodes in the P2P network. The P2P network function implies that there is no complete central control, and all nodes in the P2P network can communicate with each other using an appropriate protocol, allow for transactions to be exchanged directly among the peers.

4.1. Decentralization Opportunities in the IoT with Blockchain Functionality

The blockchain system consists of independent servers that are members of the network and has a copy of the data. These computers networked without any particular connection can operate from anywhere in the world, by performing some mathematical operations of blockchain function that ensure the procedures of correct execution of the transactions. When a new transaction arrives on one of the computers, it spread over the network. The network participants then mathematically check the transaction, add it to the block, and, depending on the consensus algorithm used, perform mathematical calculations to validate the entire data block. The first member of the plaster sends the found solution to others, who, after checking the block and approving it, add it to their blockchain. If there is more consensus than a certain number of participants in the blockchain network is considered correct [40].

By implementing decentralization infrastructure, the system damage is impossible, because all computers on the network should be decentralized. As long as there is at least one running computer, the system is running. So new computers are connecting to the system, expanding and strengthening the entire network. Each transaction in the system is created by a network of participants, validated and recorded in typical blockchain data. The real-time transactions can be tracked in the P2P network, and each member of the network can see how many transactions are made by one participant, but cannot identify it in a real-life [29].

In the case of blockchain, there is no direct way to restrict access to some data, but cryptographic data can only be encrypted and shared with certain participants. In the case of blockchain, there is no direct way to restrict access to some data, but cryptographic data can only be encrypted and shared with individual participants. The data safety and reliability are based on mathematical calculations and algorithms. The network members may be restricted from writing or read access rights to the entire network. The blockchain technology is based on public-key cryptography. Each transaction is signed by the transaction creator’s private contract. This allows you to quickly check the authenticity of the data for any modifications that were made at the time of upload using the published public key. To falsify records in the blockchain, a hacker should compromise cryptography so that more than half of the computers on the network make the wrong decision and approve the transaction [57]. Encryption methods used to ensure confidentiality, integrity, and authenticity of the information.

4.2. Implementation of Consensus Algorithm in Blockchain Communication

The possibilities of implementation of consensus algorithms in the blockchain communication process are proposed by [3], [8], [15] with the application of mechanisms of working objects structures. The blockchain network members continuously communicate with each other, synchronize blockchain and new transactions, approve blocks and add them to an existing chain. The most popular consensus algorithms - Proof of Work (PoW) is proposed by [7]. By using the PoW algorithm, participants must find a block with once value to add a new block to the circuit, so that block header hash is smaller than the networks then defined the significance of gravity. Because hash functions are unidirectional, this process is random, and singular the way to find the required nonce value is to randomly select it, count the hash code and repeat this process until a suitable one found. The meaning of nonce usually requires a lot of computing power. Those who use this algorithm the severity of the blockchain in the network controlled by the objects currently connected to the network computing power, so even if a particular participant allocates a large amount of computing power to the computation, while other participants also use powerful computers, this participant has a unique chance to find what the other unit needs. The value of nonce is small, proportional to its ratio to the computing power of the network. What the participant is the more computational resources he has, the higher his chances of “digging” the next block, and getting paid for it. PoW is resource inefficient not only because participants race for computational computing in terms of capacity, but even when one of the participants “digs” the block and writes it to the circuit, everyone else of participants who had begun to “dig” the block, i.e., that is, after trying some of the meanings of nonce becomes useless because the tested nonce values will no longer apply to blocks. These participants provided more resources for calculations that were of no use [17].

Another consensus algorithm - Proof of Stake (PoS) based on the number of cryptocurrency participants who are working on a given network, but not on the amount of computing power allocated as propose in the PoW method. For example, if a participant has 1% of the total amount of cryptocurrency available, it may “dig” 1% of the blocks. The PoS was proposed as an alternative to PoW to make the network more secure and reduce the energy costs required to operate a blockchain network while reducing transaction costs. As more participants connect computing power to a network using the PoW algorithm, the total energy resources required to maintain the network and validate transactions increase while increasing transaction costs. It is based on the fact that those users who own more coins are more interested in the survival and the correct functioning of the system, and therefore are the most suitable to carry the responsibility of protecting the system. Basically, the idea behind using PoS is to move the opportunity costs from outside the system to inside the system. The algorithm randomly determines a user responsible for the creation of each block based on only the number of coins. A common critique is that this approach does not provide incentives for nodes to vote on the correct block. Additionally, it is negative in the sense that it promotes the enrichment of the rich. The election is performed by voting, and each time a witness successfully produces another block, it is rewarded. In PoS, participants do not struggle to allocate as much computing power as possible, reducing costs and transaction costs. Also, in the long run, PoS more secure because you need to have most or almost cryptocurrency to gain most of the network management power. Not only would the more widely used and valuable cryptocurrencies cost a lot to buy at current prices, but buying a large amount of currency raises its price [25].

When designing a new network, it is decided according to its needs, which protocol will be used, and what algorithms the network will be based on as the network evolves and expands, the network protocol may need to be rewritten, or another functionality changed if needs a change. In this case, hard work performed and network operation is improved. After a complete change, it is up to each member of the network to decide which branch they will support and participate. In the case of cryptocurrencies, both branches often maintained further [46]. The algorithm of working of such layers presented in Figure 4 with the implementation of blockchain functionality.

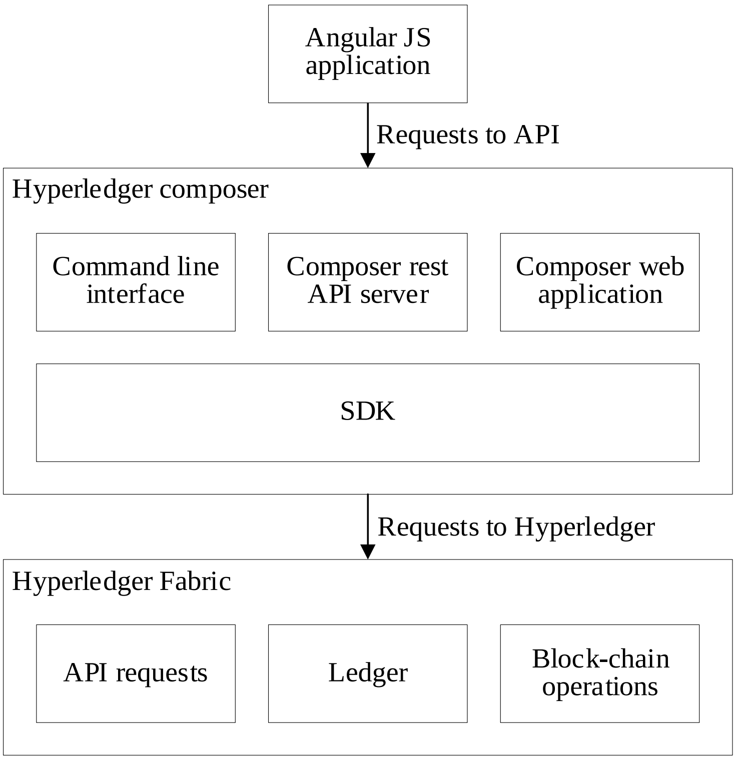


Figure 4. Example of a working algorithm with a more detailed description of infrastructure

5. Experimental Results on the Extension of Checking Functionality for Registration of Objects to IoT Environment

The experimental steps described in this chapter by the demonstration of the stages of performing the model of formation of data transmission and processing in the IoT environment developing. Some models required for developing, which needful for the secure performing of identification and authentication stages of smart objects by connecting them into the infrastructure of the IoT. At the starting position, needful safety requirements defined in Table 1. The detailed analysis of the safety requirements for the identification and authentication stages of smart objects of the IoT became the requirements for developing the informational model of the system performing.

Table 1. Main safety requirements for connection of smart objects to the IoT environment

No.	Safety requirements	Influence for effects of safety
1	The identification information of smart objects for comparison of needful parameters have to be stored in the authentication database [27].	Privacy of smart objects
2	The authentication of the smart objects must be performed using a system of encryption keys [47].	Confidentiality of smart objects
3	Smart objects attack and prevention methods must be implemented [26].	Protection from unauthorized use of smart objects
4	Transmitted data of smart objects provided to the IoT information system must be encrypted [44].	Data confidentiality of smart objects
5	Data on smart objects must be encrypted and stored in the IoT information system [34].	Data privacy of smart objects

The structural model of the information of data transmission and processing stages by connecting the smart objects in the IoT environment is presented in Figure 5. This structural model connected with a few identification and authentication stages of smart objects in the IoT environment. Some additional databases are developed and included in the overall information system of the IoT, which represents data of control units and smart objects. The databases store data received from smart objects. The smart objects are receiving data from sensors and transmit to the control units. The control units allow control of collecting data from smart objects. The storage processes performed in data-warehouses. The processing algorithms help to present data for users.

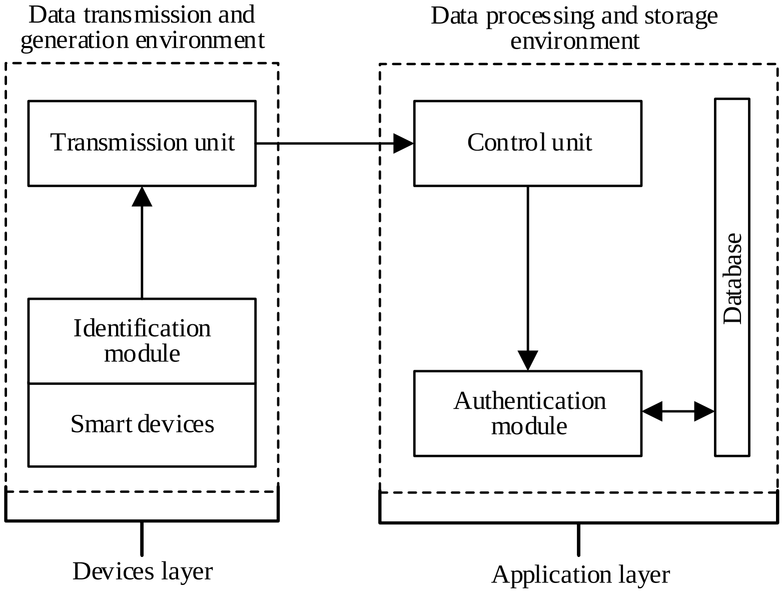


Figure 5. The model of formation of data transmission and processing in the IoT environment by connecting the smart objects

The wireless data transmission protocol is used for communication between smart objects and the control unit. The encryption of data transmitted by smart objects is performed using the Advanced Encryption Standard (AES) algorithm, which uses a 128-bit key. This key consists of 16 hexadecimal numbers, each with a small data length of the 8 bits. The data transmission of smart objects is performed using Gaussian Frequency Shift Keying (GFSK) modulation at 2,4

GHz. The transmitted packets consist of a preamble, an access address, a protocol data unit, and cyclic redundancy control. Figure 6 presents the structure of a data transmission protocol packet. The preamble addressed to the recipient, who synchronizes the packets according to the received data from smart objects. The access address is broadcast before a connection is established and used for packets routing and smart object identification. The minimum protocol data unit size is two octets because it consists of a logical identifier and protocol data unit length. The cyclic redundancy control used to check bits for distortion during the smart objects data transmission.

Minimum significant bit — Maximum significant bit

Preamble (1 octet)	Access address (4 octets)	Protocol data unit (2 - 39 octets)	Cyclic redundancy control (3 octets)

Figure 6. Structure of a data transmission protocol packet

The safety management in data transmission consists of protocols and algorithms for creating an encrypted connection, which performed by exchanging the encrypted private key for communication between the IoT smart objects. The key exchange is performed in three stages:

1. Information exchanged for temporary communication.

2. The master and slave of the smart objects create temporary keys that encrypt the packets and calculate a value that confirms that both objects use the same key.

3. The master and slave of the smart objects exchange a private key, which used for continuous data encryption.

The data transmission and processing of the IoT information system successively can be checked by performing the suitability of the smart objects according to the following criteria:

- smart objects names and media access control addresses match stored in the database;

- encryption keys of the IoT smart objects exactly match the one stored in the database;

- number of sensors detected by the smart objects corresponds to stored in the database.

The requests sent to smart objects that are activated from the control unit to enable the reading of data from sensors every second. The scanned data is encrypted with a private key on the smart objects but is only decrypted and verified on the control unit. The validity of the decrypted data of smart objects is defined according to the points:

a) the decrypted data on the smart objects are successful;

b) the sensor data of the smart objects is the default size;

c) the sensor data value of the smart objects is the usual size.

The blocked smart objects are registered in a database, and about these events reported in the graphical user interface. These incidents considered attacks against the IoT information system. This data can be used for a review of the events history or the attack detection, and safety methods. This model helps to fully integrate the IoT objects into the common structure of the docker network of a blockchain platform, which is presented in Figure 7.

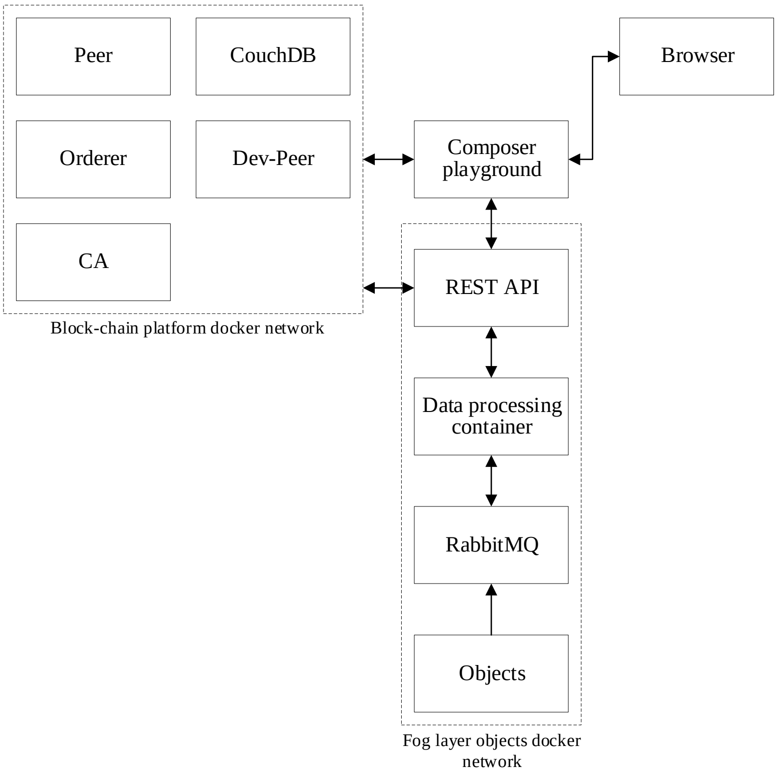

Peer
CouchDB
Browser
Orderer
Dev-Peer
Composer playground
CA
REST API
Block-chain platform docker network
Data processing container
RabbitMQ
Objects
Fog layer objects docker network

Figure 7. The structure of integration of objects in the docker network of a blockchain platform

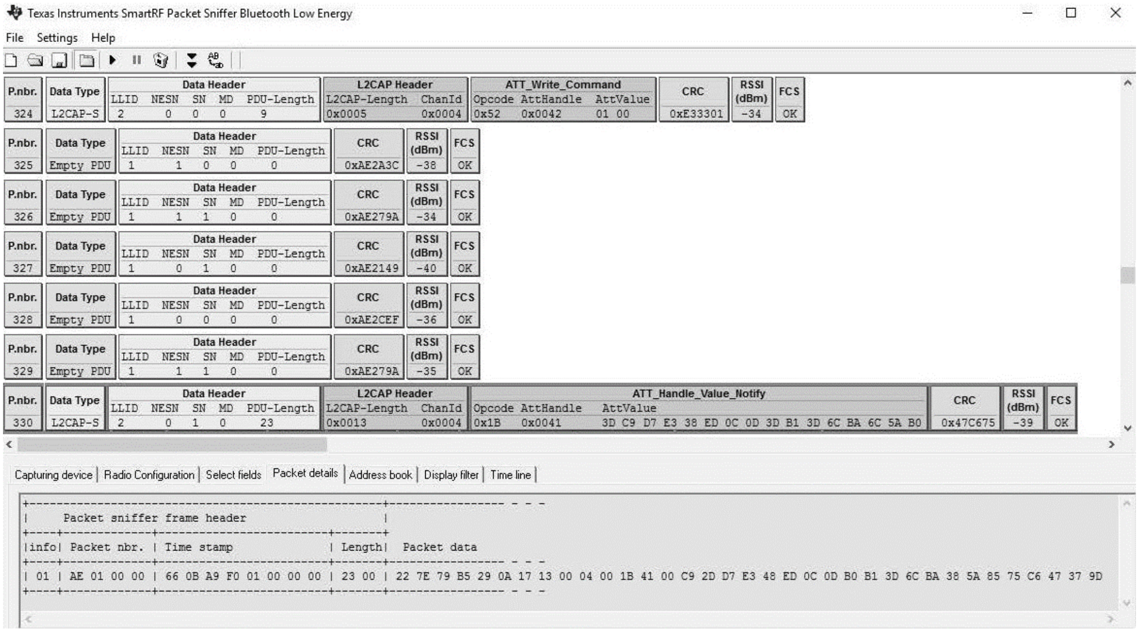
In this structure, the Hyperledger Fabric system used for the implementation of the operations of the blockchain platform. The Hyperledger Composer tool used to facilitate the process of prototyping of blockchain applications. This tool uses the prepared scripts to create a virtual Hyperledger Fabric blockchain system. The docker builds initial containers Peer, Dev-Peer, CouchDB, CA, and Orderer. The Peer container performs the processes of blockchain operations and consensus mechanisms. The Dev-Peer container performs blockchain code operations that are validated by the Peer container by using the consensus protocol. A copy of the blockchain general ledger stored in CouchDB containers. The CouchDB database stores data status information and blockchain records. This solution ensures system performance by performing the queries and read operations during the circuit code execution. The data state database acts as a cache to perform read operations on the blockchain. The Peer type servers do not have to search for information recursively each time they traverse the blockchain transaction history when performing queries or read operations. The database status acts as a cache for reading operations on blockchains, and Peer type servers do not have to search for information recursively each time they traverse the blockchain transaction history, when performing queries or read operations. The CA container performs a certificate authority management function, issues private key infrastructure-based certificates to network organizations, one root, and registration certificate for each authorized system user. The objects are not classified as system users because their data transmitted to the blockchain system only through messaging servers. The distribution servers are replaced by Orderer containers that divide transactions into blocks. This distribution service operates independently of the execution servers. The message processing servers located at a short distance from the IoT objects because these servers freely access block circuit platforms using API requests, depending on the message type and function. The REST API works on processing servers with blockchain servers. The data aggregation servers perform aggregation and processing functions, while terminals access the proxy servers. The RabbitMQ message broker works only on proxy servers whose purpose is to forward messages to other servers running message handlers. The IoT objects can be mobile devices, so data from them can be sent to the geographically closest proxy servers. This functionality provided by load balancers or specialized canonical name records.

The simulation of data of eavesdropping attack was performed on a computer using SmartRF Protocol Packet Sniffer software. The safety requirements of the IoT information system are implemented, data of the smart objects read from the control unit, and the data listening system on the computer is activated. The main commands performed and the results obtained on the control unit of the IoT information system are shown in Table 2.

Table 2. Commands for performing on the control unit

```
administrator@smartobjectserver:~ $ gatttool -a A0:A2:28:AE:2E:06 -I
[A0:A25:28:AE:2E:06][LE]> connect
Attempting to connect to A0:A25:28:AE:2E:06
Connection successful
[A0:A25:28:AE:2E:06][LE]> char-write-cmd 0x44 01
[A0:A25:28:AE:2E:06][LE]> char-write-cmd 0x42 01:00
Notification = 0x0041 value: 3d c9 d7 e3 38 ed 0c 0d 3d b1 3d 6c ba 6c 5a b0
Notification = 0x0041 value: 67 8e 81 5d 22 12 79 12 5b 0e 6e a6 c7 6a 32 a6
[A0:A25:28:AE:2E:06][LE]> char-write-cmd 0x42 00:00
```

All data packets captured on the computer control unit, smart objects, and data listening SmartRF Protocol Packet Sniffer window is presented in Figure 8.



```
P.nbr. | Data Type | Data Header: LLID NESN SN MD PDU-Length | L2CAP Header: L2CAP-Length ChanId | ATT_Write_Command: Opcode AttHandle AttValue | CRC | RSSI (dBm) | FCS
324    | L2CAP-S   | 2 0 0 0 9                               | 0x0005 0x0004                     | 0x52 0x0042 01 00                            | 0xE33301 | -34 | OK

P.nbr. | Data Type | Data Header: LLID NESN SN MD PDU-Length | CRC | RSSI (dBm) | FCS
325    | Empty PDU | 1 1 0 0 0                               | 0xAE2A3C | -38 | OK
326    | Empty PDU | 1 1 1 0 0                               | 0xAE279A | -34 | OK
327    | Empty PDU | 1 0 1 0 0                               | 0xAE2149 | -40 | OK
328    | Empty PDU | 1 0 0 0 0                               | 0xAE2CEF | -36 | OK
329    | Empty PDU | 1 1 1 0 0                               | 0xAE279A | -35 | OK

P.nbr. | Data Type | Data Header: LLID NESN SN MD PDU-Length | L2CAP Header: L2CAP-Length ChanId | ATT_Handle_Value_Notify: Opcode AttHandle AttValue | CRC | RSSI (dBm) | FCS
330    | L2CAP-S   | 2 0 1 0 23                              | 0x0013 0x0004                     | 0x1B 0x0041 3D C9 D7 E3 38 ED 0C 0D 3D B1 3D 6C BA 6C 5A B0 | 0x47C675 | -39 | OK
```

```
+-----------------------------------------------+---------------- - - -
|     Packet sniffer frame header               |
+----+------------+----------------------+-------+
|info| Packet nbr. | Time stamp           | Length|  Packet data
+----+------------+----------------------+-------+---------------- - - -
| 01 | AE 01 00 00 | 66 0B A9 F0 01 00 00 00 | 23 00 | 22 7E 79 B5 29 0A 17 13 00 04 00 1B 41 00 C9 2D D7 E3 48 ED 0C 0D B0 B1 3D 6C BA 38 5A 85 75 C6 47 37 9D
+----+------------+----------------------+-------+---------------- - - -
```

Figure 8. SmartRF Protocol Packet Sniffer window for a finding of the data packets

The data message activation command 01 00 is used to easily find the data packets in the SmartRF Protocol Packet Sniffer. The packet number of the found data message activation command is 324, and the traffic packet is 330. The read data 3d c9 d7 e3 38 ed 0c 0d 3d b1 3d 6c ba 6c 5a be encrypted, which means that the IoT information system wholly protected from the threats of the eavesdropping, tampering, and possible attacks.

6. CONCLUSIONS

The implementation of safeguard methods on the first stages of identification and authentication of objects before the permission stage for launching them into the working area of the IoT is very important. The research works need more careful investigations. We propose some algorithms for a more secure connection of objects to the functionality of IoT infrastructure. Very prospective initiatives of blockchain development can help in the identification and authentication stages of objects by the integration of their functionality to the IoT infrastructure for more safety integrity. The requirements for the safety of the multi-layered infrastructure of objects by linking to the IoT proposed in this article. Such infrastructure became more complex according to the risks of unsafe possibilities. This research is forwarded for evaluation of some kinds of safety means related to identification and authentications stages of objects by integrating them with the functionality of blockchain in the infrastructure of IoT. The objectives are related to the development of model and working algorithms of stages of checking by integrating means for establishing and managing operational rules of the IoT objects. In future works, we plan to strengthen the IoT information safety model for the identification and authentication of objects.

REFERENCES

[1] Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F., (2017) "Internet of Things Security: A Survey," Journal of Network and Computer Applications, Vol. 88, No. 1, pp10-28.

[2] Andziulis, A., Dzemydienė, D., Steponavičius, R., & Jakovlev, S., (2011) "Comparison of two heuristic approaches for solving the production scheduling problem," International Journal of Information Technology and Control, Vol.40, No. 2, pp118-122.

[3] Atzei, N., Bartoletti, M., & Cimoli, T., (2017) "A survey of attacks on Ethereum smart contracts, Proceedings of the 6th Conference on Principles of Security and Trust (ETAPS), pp164-186.

[4] Atzori, M., (2017) "Blockchain Technology and Decentralized Governance: Is the State Still Necessary," International Journal of Governance and Regulation, Vol. 6, No. 1, pp1-37.

[5] Baghli, R. B., Najm, E., & Traverson, B., (2016) "Towards a Multi-Leveled Architecture for the Internet of Things," Proceedings of the 20th IEEE International Enterprise Distributed Object Computing Workshop (EDOCW), pp182-187.

[6] Benabdessalem, R., Hamdi, M., & Kim, T. H., (2014) "A Survey on Security Models, Techniques, and Tools for the Internet of Things," Proceedings of the 7th International Conference on Advanced Software Engineering and Its Applications (ASEA), pp44-48.

[7] Dwork, C., & Naor, M., (1992) "Pricing via Processing or Combatting Junk Mail," Proceedings of the Advances in Cryptology, pp139-147.

[8] Fakhri, D., & Mutijarsa, K., (2018) "Secure IoT Communication using Blockchain Technology," Proceedings of the Symposium on Electronics and Smart Devices, pp1-6.

[9] Ferrag, M. A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L., & Janicke, H., (2018) "Blockchain Technologies for the Internet of Things: Research Issues and Challenges," IEEE Internet of Things Journal, Vol. 6, No. 2, pp2188-2204.

[10] Fersi, G., (2015) "A Distributed and Flexible Architecture for Internet of Things," Proceedings of the International Conference on Advanced Wireless, Information, and Communication Technologies (AWICT), pp. 130-137.

[11] Fink, G. A., Zarhitsky, D. V., Carroll, T. E., & Farquhar, E. D., (2015) "Security and Privacy Grand Challenges for the Internet of Things," Proceedings of the Conference on Collaboration Technologies and Systems (CTS), pp27-34.

[12] Gomba, M., & Nlwya, B., (2017) "Architecture and Security Considerations for Internet of Things," Proceedings of the 7th IEEE Conference on Global Wireless Summit (GWS), pp252-256.

[13] Hinai, S. A., & Singh, A, V., (2017) "Internet of Things: Architecture, Security Challenges and Solutions," Proceedings of the International Conference on Infocom Technologies and Unmanned Systems (ICTUS), pp197-201.

[14] Hossain, M. M., Fotouhi, M., & Hasan, R., (2015) “Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things,” Proceedings of the 11th IEEE World Congress on Services, pp21-28.

[15] Khalid, U., Asim, M., Baker, T., Hung, P., Tariq, M., & Rafferty, L., (2020) “A decentralized lightweight blockchain-based authentication mechanism for IoT systems,” International Journal of Cluster Computing, Vol. 23, No. 1, pp1-21.

[16] Khan, R., Khan, S. U., Zaheer, R., & Khan, S., (2012) “Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges” Proceedings of the 10th International Conference on Frontiers of Information Technology, pp257-260.

[17] Kim, H., Wasicek, A., Mehne, B., & Lee, E. A., (2016) “A Secure Network Architecture for the Internet of Things Based on Local Authorization Entities,” Proceedings of the 4th IEEE Conference on Future Internet of Things and Cloud (FiCloud), pp114-122.

[18] Kraijak, S., & Tuwanut, P., (2015) “A Survey on Internet of Things Architecture, Protocols, Possible Applications, Security, Privacy, Real-World Implementation and Future Trends,” Proceedings of the 16th IEEE Conference on Communication Technology (ICCT), pp26-31.

[19] Kurmis, M., Andziulis, A., Dzemydienė, D., Jakovlev, S., Voznak, M., & Gricius, G., (2015) “Cooperative context data acquisition and dissemination for situation identification in vehicular communication networks,” Journal of Wireless Personal Communications, Vol. 85, No. 1, pp49-62.

[20] Li, W., Meng, W., Liu, Z., & Au, M., (2020) “Towards Blockchain-Based Software-Defined Networking: Security Challenges and Solutions,” International Journal of Ieice Transactions on Information and Systems, vol. E103.D(2), pp196-203.

[21] Lin, I. C., & Liao, T. C., (2017) “A Survey of Blockchain Security Issues and Challenges,” International Journal of Network Security, Vol. 19, No. 5, pp653-659.

[22] Liu, C., Zhang, Y., Li, Z., Zhang, J., Qin, H., & Zeng, J., (2015) “Dynamic Defense Architecture for the Security of the Internet of Things,” Proceedings of the 11th International Conference on Computational Intelligence and Security (CIS), pp390-393.

[23] Madakam, S., Ramaswamy, R., & Tripathi, S., (2015) “Internet of Things (IoT): A Literature Review,” Journal of Future Computer and Communication, Vol. 3, No. 5, pp164-173.

[24] Mahmoud, R., Yousuf, T., Aloul, F., & Zualkernan, I., (2015) “Internet of Things Security: Current Status, Challenges and Prospective Measures,” Proceedings of the 10th Conference for Internet Technology and Secured Transactions (ICITST), pp336-341.

[25] Matharu, G. S., Upadhyay, P., & Chaudhary, L., (2014)” The Internet of Things: Challenges and Security Issues,” Proceedings of the Conference on Emerging Technologies (ICET), pp54-59.

[26] Matulevičius, R., & Savukynas, R., (2019) “Application of the Reference Model for Security Risk Management in the Internet of Things Systems,” in Lupeikienė, A., Vasilecas, O., Dzemyda, G. (Ed). Databases and Information Systems X. IOSPress, pp 65-78.

[27] Meidan, Y., Bohadana, M., Shabtai, A., Guarnizo, J., Ochoa, M., Tippenhauer, N., & Elovici, Y., (2017), “ProfilIoT: A Machine Learning Approach for IoT Device Identification Based on Network Traffic Analysis,” Proceedings of the 32nd ACM SIGAPP Symposium on Applied Computing (SAC), pp. 506-509.

[28] Meng, W., Wang, J., Wang, X., Liu, J., Yu, Z., Li, J., Zhao, Y., & Chow, S. M., (2018) “Position Paper on Blockchain Technology: Smart Contract and Applications,” Proceedings of the 12th International Conference on Network and System Security, pp474-483.

[29] Miraz, M. H., & Ali, M., (2018) “Blockchain Enabled Enhanced IoT Ecosystem Security,” Proceedings of the Conference on Emerging Technologies in Computing (iCETiC), pp1-9.

[30] Mynzhasova, A., Radojicic, C., Heinz, C., Kölsch, J., Grimm, C., Rico, J., Keith, D., Castro, R. G., & Oravec, V., (2017) “Drivers, Standards and Platforms for the IoT: Towards a Digital VICINITY,” Proceedings of the Conference on Intelligent Systems (IntelliSys), pp1-7.

[31] Nakamoto, S., (2009) “Bitcoin: A Peer-to-Peer Electronic Cash System,” Bitcoin Project, pp. 1-9.

[32] Nastase, L., (2017) “Security in the Internet of Things: A Survey on Application Layer Protocols,” Proceedings of the 21st Conference on Control Systems and Computer Science (CSCS), pp659-666.

[33] Neumann, A. J., Statland, N., & Webb, R. D., (1977) “Post-processing audit tools and techniques,” Proceedings of the NBS Workshop, pp36-341.

[34] Ning, H., Liu, H., & Yang, L. T., (2013) “Cyberentity Security in the Internet of Things,” Journal of Innovative Technology for Computer Professionals, Vol. 46, No. 4, pp46-53.

[35] Pal, S., Hitchens, M., & Varadharajan, V., (2017) "Towards A Secure Access Control Architecture for the Internet of Things," Proceedings of the 42nd IEEE International Conference on Local Computer Networks (LCN), pp219-222.

[36] Panarello, A., Tapas, N., Merlino, G., Longo, F., & Puliafito, A., (2018) "Blockchain and IoT Integration: A Systematic Survey," International Journal of Sensors, Vol. 18, No. 8, pp1-38.

[37] Patra, L., & Rao, U. P., (2016) "Internet of Things - Architecture, Applications, Security and Other Major Challenges," Proceedings of the 3rd International Conference on Computing for Sustainable Development (INDIACom), pp1201-1206.

[38] Paulavičius, R., Grigaitis, S., Igumenov, A., & Filatovas, E., (2019) "A Decade of Blockchain: Review of the Current Status, Challenges, and Future Directions," International Journal of Informatica, Vol. 30, No. 4, pp729-748.

[39] Rathore, H., Mohamed, A., & Guizani, M., (2020) "A Survey of Blockchain Enabled Cyber-Physical Systems," International Journal of Sensors, Vol. 20, No. 1, pp1-28.

[40] Ren, Z., Liu, X., Ye, R., & Zhang, T., (2017) "Security and Privacy on Internet of Things," Proceedings of the 7th IEEE Conference on Electronics Information and Emergency Communication (ICEIEC), pp140-144.

[41] Roman, R., Alcaraz, C., Lopez, J., & Sklavos, N., (2011) "Key Management Systems for Sensor Networks in the Context of the Internet of Things," International Journal of Computers and Electrical Engineering, Vol. 37, No. 2, pp147-159.

[42] Salman, M. A., (2014) "On Identification of Internet of Things," International Journal of Sciences: Basic and Applied Research, Vol. 18, No. 1, pp59-62.

[43] Savukynas, R., & Dzemydienė, D., (2018) "Security Means in Multi-layered Architecture of Internet of Things for Secure Communication and Data Transmission," Proceedings of Baltic DB&IS 2018 Conference Forum and Doctoral Consortium co-located with the 13th International Baltic Conference on Databases and Information Systems, pp127-134.

[44] Shah, S. H., & Yaqoob, I. (2016) "A Survey: Internet of Things (IoT) Technologies, Applications and Challenges," Proceedings of the 4th IEEE International Conference on Smart Energy Grid Engineering (SEGE), pp381-385.

[45] Showkat, S., & Qureshi, S. (2020) "Securing the internet of things using blockchain," Proceedings of the 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence), pp540-545.

[46] Sicari, S., Rizzardi, A., Miorandi, D., Cappiello, C., & Coen-Porisini, A., (2016) "A Secure and Quality-Aware Prototypical Architecture for the Internet of Things," International Journal of Information Systems, Vol. 58, No. 1, pp43-55.

[47] Simsek, I., & Rathgeb, E. P., (2019) "Zero-Knowledge and Identity-Based Authentication and Key Exchange for Internet of Things," Proceedings of the 5th IEEE World Forum on Internet of Things (WF-IoT), pp283-288.

[48] Solapure, S. S., & Kenchannavar, H., (2016) "Internet of Things: Internet of Things: A Survey Related to Various Recent Architectures and Platforms Available," Proceedings of the 5th IEEE Conference on Advances in Computing, Communications and Informatics (ICACCI), pp2296-2301.

[49] Stammberger, K., Semp, M., Anand, M. B., & Culler, D., (2010) "Introduction to security for smart Object Networks," [White paper], Internet Protocol for Smart Objects Alliance, pp1-28.

[50] Suo, H., Wan, J., Zou, C., & Liu, J., (2012) "Security in the IoT: A Review," Proceedings of the Conference on Computer Science and Electronics Engineering (ICCSEE), pp648-651.

[51] Tan, J., & Koo, S. G. M., (2014) "A Survey of Technologies in Internet of Things," Proceedings of the 10th IEEE International Conference on Distributed Computing in Sensor Systems, pp269-274.

[52] Vasilomanolakis, E., Daubert, J., Luthra, M., Gazis, V., Wiesmaier, A., & Kikiras, P., (2015) "On the Security and Privacy of Internet of Things Architectures and Systems," Proceedings of the International Workshop on Secure Internet of Things (SIoT)," pp49-57.

[53] Wang, H., Wang, L., Zhou, Z., Tao, X., Pau, G., & Arena, F., (2019) "Blockchain-Based Resource Allocation Model in Fog Computing," Journal of Applied Sciences, Vol. 9, No. 24, pp1-18.

[54] Weber, R. H., (2010) "Internet of Things – New Security and Privacy Challenges," International Journal of Computer Law and Security Review, Vol. 26, No. 1, pp23-30.

[55] Wen, Y., Jinlong, W., & Gianchuan, Z., (2016) "Physical Objects Registration and Management for Internet of Things," Proceedings of the 35th Chinese Control Conference (CCC), pp8335-8339.

[56] Weyrich, M., & Ebert, C., (2016) “Reference Architectures for the Internet of Things,” International Journal of IEEE Software, Vol. 33, No. 1, pp112-116.

[57] Xie, S., Zheng, Z., Chen, W., Wu, J., Dai, H. N., & Imran, M., (2020) “Blockchain for cloud exchange: A survey,” Journal of Computers and Electrical Engineering, Vol. 81, No. 1, pp. 1-12.

[58] Zhao, K., & Ge, L., (2013) “A Survey on the Internet of Things Security,” Proceedings of the 9th Conference on Computational Intelligence and Security (CIS), pp. 663-667.

[59] Zhu, T., Dhelim, S., Zhou, Z., Yang, S., & Ning, H., (2017) ”An Architecture for Aggregating Information from Distributed Data Nodes for Industrial Internet of Things,” International Journal of Computers and Electrical Engineering, Vol. 58, No. 1, pp337-349.

AUTHOR

The Ph.D. student of the Group of Intelligent Technologies Research at the Institute of Data Science and Digital Technologies, Faculty of Mathematics and Informatics, which is part of Vilnius University. The junior lecturer on Software Engineering, Systems Theory, and Information Security at Vilnius Gediminas Technical University. The research interests include advanced database systems, business process engineering, intelligent information systems, social computing technologies, software systems engineering, information security.