A Lightweight Blockchain based Two Factor Authentication Mechanism for LoRaWAN Join Procedure

Syed Muhammad Danish*, Marios Lestas†, Waqar Asif‡, Hassaan Khaliq Qureshi*, Muttukrishnan Rajarajan‡
*National University of Sciences & Technology (NUST), Islamabad, Pakistan
*{sdanish.msee16seecs, hassaan.khaliq}@seecs.nust.edu.pk
†Frederick University, Cyprus
† eng.lm@frederick.ac.cy
‡School of Engineering and Mathematical Sciences, City University, London, UK.
‡{r.muttukrishnan, waqar.asif}@city.ac.uk

***Abstract*—Recently, there has been increasing interest in employing blockchain in different applications, other than cryptocurrencies. Blockchains allow a peer to peer distributed network where different nodes communicate with each other, in a trustless manner. Long Range Wide Area Network (LoRaWAN) is an Internet of Things (IoT) technology, which enables long range communication. Although LoRaWAN networks are secure, the LoRaWAN join procedure is susceptible to replay and jamming attacks. Moreover, trust between network server and LoRa end device is the basic foundation of LoRaWAN network however, the centralized nature of network servers raise trust issues between network operators and customers. To solve this problem, we propose a lightweight two factor authentication mechanism for LoRaWAN join procedure, based on blockchain technology. The proposed blockchain based framework provides an extra layer of security for LoRaWAN join procedure and build trust among LoRaWAN network components. The proposed framework is validated using the Ethereum blockchain. The results demonstrate that the proposed framework provides efficient system performance in terms of throughput and latency. The proposed blockchain architecture is a cost effective solution, which can be utilized in the LoRaWAN network with few network servers and LoRa end device, having no strict requirement of throughput and latency.**

***Keywords*—Blockchain, LoRaWAN Join Procedure, LoRaWAN, Authentication, Internet of Things.**

I. Introduction

Blockchain technology has been one of the most revolutionary technological concept over the past few years. Blockchain technology has attracted significant attention from a wide range of industries: utilities, finance, medical services and the real estate [1]. By employing blockchain technology, applications that needed a central trusted authority for their execution, can now be executed in a decentralized and distributed environment without the need of a trusted third party or intermediary and attain the similar reliability and functionality, which was merely impossible before. Blockchain enables the network entities to operate in a trust-less environment even if the parties do not trust each other. The absence of central trusted authority leads to faster agreement among communicating parties. Cryptography, distributed consensus mechanism and self executing smart contract scripts makes blockchain more secure and allow distributed automated workflows thus, makes it alluring to developer and researchers working in IoT technology domain.

According to Gartner [2], there will be more than 20 billion Internet of Things (IoT) devices by 2020 and the number will continuously increase. IoT applications have significant impact on people's daily life nowadays. To compensate for long range, low power and losw cost requirements, Low Power Wide Area Network (LPWAN) has been introduced to connect IoT devices. LoRaWAN, a MAC layer protocol in the family of LPWAN IoT technology, is designed to support bidirectional long range, low power and low data rate communication between IoT devices. LoRaWAN fills the gap between the high power consumption long range networks and low power consumption short range networks. LoRaWAN network is designed to ensure confidentiality, authentication and integrity for secure communication between LoRaWAN network's entities. However, much work has yet to be done to make LoRaWAN network more secure.

LoRaWAN has been shown to be susceptible to wormhole attack [3], bit flipping attacks [4], replay attacks [5][6] and jamming attacks [7][8]. In [13], authors explained that LoRaWAN network server cannot be trusted for handling user's personal data and can modify the user's information. Authors in [7] demonstrate how a jammer can stop LoRa end device to make a connection with the LoRaWAN network server by generating constant Received Signal Strength (RSS) around LoRa end device. To detect jammer around LoRa end device, authors in [6], proposed intrusion detection mechanism. Authors in [4], explains the susceptibility of LoRaWAN join procedure to replay attacks by setting up an attack scenario. Recently, Blockchain has been employed within IoT networks to improve security. In [9], authors proposed an authentication framework for IoT networks, based blockchain technology. In [10], an identity framework, based on blockchain technology, is proposed for IoT networks. To authenticate smart meters, authors proposed [11] a blockchain based zero knowledge proof

978-1-7281-2373-8/19/$31.00 ©2019 IEEE

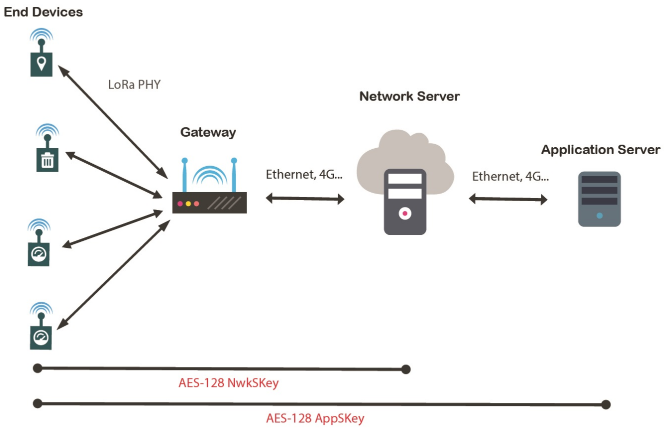

Fig. 1. LoRaWAN architecture

solution. Authors in [12] proposed a two factor authentication scheme for IoT networks based on blockchain technology. To the best of our knowledge, the only previous work which employ blockchain technology in the LoRaWAN network is [13], in which authors propose a blockchain based solution to ensure trust and data integrity in LoRaWAN networks. This is the first work to utilize blockchain technology in LoRaWAN network to assist the authentication of LoRa end devices in the LoRaWAN join procedure.

The main objective of this work is to propose a two factor authentication mechanism, based on blockchain, for LoRaWAN join procedure to add an additional layer of security in authentication mechanism and to build trust among LoRa end devices and network servers. The join request message in LoRaWAN join procedure is not encrypted and is susceptible to jamming and replay attacks. Also, the centralized nature of network servers raise the trust issues between network servers and LoRa end device since, the network server can modify the user's private data. Therefore, in this paper, we propose two factor authentication mechanism for LoRaWAN join procedure to enhance authentication security and to build trust among LoRa end devices and network server, by employing blockchain in LoRaWAN network. Unlike [13], we assume that there are few numbers of network servers in LoRaWAN network thus, network servers cannot be equipped with the functionality of blockchain. In our framework, blockchain is an independent network, working concurrently with the LoRaWAN network entities, to save the information of the LoRa end device for authentication purpose. With the help of smart contracts, the blockchain network save the LoRa end device information, which is triggered by the transactions from the gateways.

The proposed framework is simulated using the Ethereum blockchain and Python client and server implementation of LoRa end device and network server respectively. The framework is evaluated on the basis of different performance metrics i.e. throughput and latency. The simulations results demonstrate that the proposed framework provides efficient system performance in terms of throughput and latency. Although the network server fetch information from blockchain network on real time, the addition of another authentication check in LoRaWAN join procedure leads to the delay in LoRaWAN join procedure. To sum up, the proposed blockchain architecture is a cost effective solution, which can be utilized in the LoRaWAN network with few network servers and LoRa end device, having no strict requirement of throughput and latency. It is designed explicitly to enhance trust and security in LoRaWAN join procedure however, it comes at the cost of delay at LoRaWAN network server.

The rest of the paper is organized as follows. In section II, backgound information on the LoRaWAN and the blockchain technology is presented. The proposed blockchain based framework is described in Section III. Section IV provides details about the working of proposed framework while Section V presents the performance evaluation and results. The key conclusion and future work is summarized in section VI of our paper.

II. Background

In this section, the background information on blockchain technology and LoRaWAN technology is provided.

A. LoRaWAN

LoRaWAN network is organized in a star networking topology in which the the packets from LoRa end device reach the LoRaWAN network server via the gateway. LoRa end devices use a physical layer protocol, called LoRa, to communicate with the gateways while, gateways communicate with the network server over the standard TCP/IP connections. To offer low power and long range communication between the gateway and LoRa end device, Chirp Spread Spectrum (CSS) technique is used. Each LoRa end node has to go through a join procedure to start communication with the LoRaWAN network server. In LoRaWAN join procedure, the network server authenticates the LoRa end device based on the join request sent by it. This process is called Over The Air Activation (OTAA). The network server simply discard the join request message if the same DevNonce value is used in join request message. Also, based on the contents of join request, the session keys are generated by the join server and distributed to network and application servers. The LoRaWAN network architecture is shown in Fig. 1.

B. Blockchain Technology

Blockchain is a type of distributed ledger which use independent nodes to share, record and synchronize data in their respective database instead of keeping the data in traditional central server. Blockchain technology is managed by a peer-to-peer network without the involvement of any trusted third party. The two operations associated with the blockchain are read operation and write operation. The transactions are stored on the blockchain network in the form of blocks. Cryptographic hash is used to identify each block and each next block on the blockchain data structure contains the hash of the previous block. Thus, a link is established between blocks

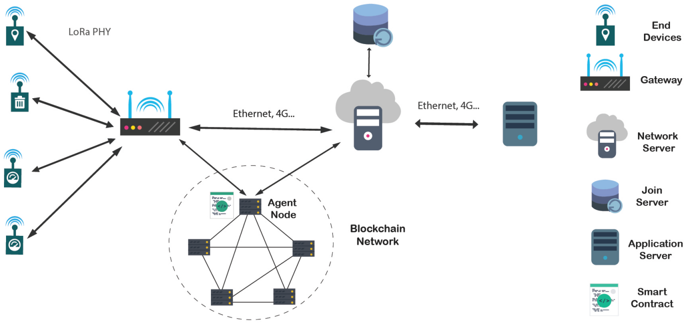

Fig. 2. Blockchain based framework for LoRaWAN two factor authentication

and a chain of blocks is created, called blockchain. Miners mine the blocks by following the consensus algorithm. This consensus mechanism guarantees the security of information, making it difficult to tamper with. Smart contracts can also be deployed on blockchain network. Smart contract is a piece of code which is executed automatically when a node trigger it by sending transaction [1]. Blockchain technology can be beneficial in following ways:

- the information stored in the blockchain network is immutable and tamper-proof.
- multiple nodes on the blockchain network validates transactions and blocks instead of a traditional central server.
- a decentralized peer-to-peer network i.e. network is not managed by a central entity.
- every node in the blockchain network saves a copy of the ledger instead of keeping the data in traditional central server.
- once deployed, smart contracts cannot be deleted from the blockchain network by a single node.

Thus, the blockchain network enables secure and tamper-proof communication between the individual nodes on the blockchain network.

III. Proposed Architecture

In this section, blockchain based framework for two factor authentication in LoRaWAN join procedure is explained. The presented blockchain based framework for LoRaWAN join procedure propose a new authentication system which combines the current LoRaWAN join procedure protocol with blockchain based authentication of LoRa end device to enhance the security of LoRaWAN join procedure.

In our proposed framework, blockchain is an independent network, working in parallel with the LoRaWAN network. Blockchain functionality has not been added in the LoRa end device and gateways because these devices are normally resource constrained as well as deployed outdoor and cannot perform complex blockchain tasks. Furthermore, in the blockchain network, a smart contract is deployed on agent node and gateways in addition to network servers, are connected to this agent node to interact with the smart contract. The distinctive feature of smart contract is that it is unique and cannot be removed from the blockchain network. Fig. 2 shows the proposed architecture for two factor authentication system for LoRaWAN network.

The system architecture consist of the following components: Blockchain network, smart contract, network server, join server, agent node, gateways and LoRa end devices.

A. LoRa end device

These are battery operated, resource constrained and low power IoT devices to perform a range of automated task. They have limited storage and computational and capabilities and are susceptible to attack because they are not designed to have effective security measures. LoRa end devices are connected to the network server through the gateways and the LoRaWAN network servers identify each LoRa end device with a 128 bit AppKey (NwkKey in LoRaWAN specification v1.1).

B. Gateway

Gateways act as a bridge between the LoRaWAN network servers and LoRa end device. LoRa end devices use LoRa modulation and LoRaWAN protocol to connect to the gateway, whereas the gateway utilize the high bandwidth network like Cellular, Ethernet or WIFI to connect to the network server. Gateways receive the LoRa end device packets by scanning the spectrum. All gateways in the vicinity of LoRa end device receive packets since LoRa end node is not associated with single gateway.

C. Network & Join Server

The network server forwards the packets of LoRa end device to application server. Main functionality of networks server is scheduling and managing the utilization of gateways, keep track of each LoRa end device to map the packets to correct application server and to keep track of security keys and frame counters. Join server is directly connected to network server and is responsible for Over The Air Activation (OTAA) LoRaWAN join procedure. It provides the network and application session keys to the network and application server respectively.

D. Agent Server

The smart contract in our framework is deployed by the agent node in the blockchain network. The agent node owns the smart contract and after deployment in the blockchain

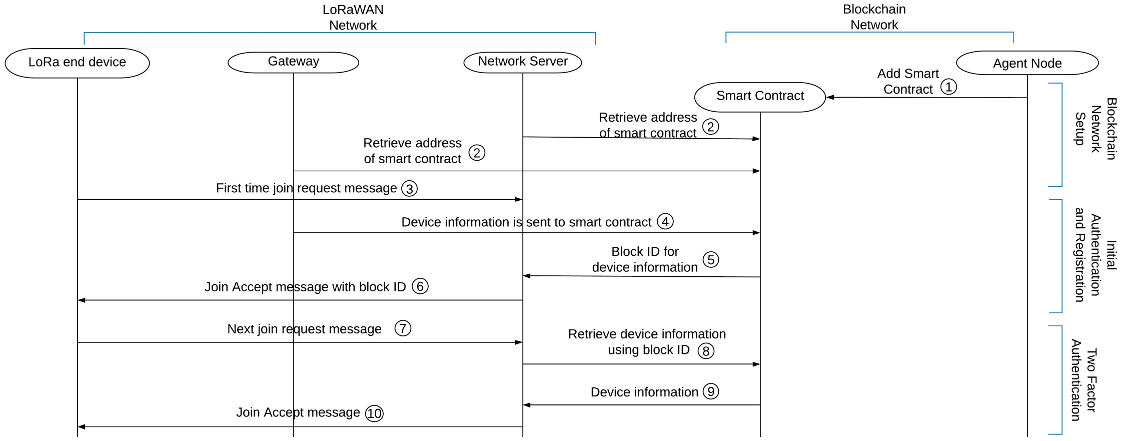
LoRaWAN Network
Blockchain Network
LoRa end device
Gateway
Network Server
Agent Node
Smart Contract
Add Smart Contract ①
Retrieve address of smart contract ②
Retrieve address of smart contract ②
First time join request message ③
Device information is sent to smart contract ④
Block ID for device information ⑤
Join Accept message with block ID ⑥
Next join request message ⑦
Retrieve device information using block ID ⑧
Device information ⑨
Join Accept message ⑩
Blockchain Network Setup
Initial Authentication and Registration
Two Factor Authentication

Fig. 3. Interaction among different components of proposed framework for two factor authentication

network, it retrieves the address of the smart contract. Gateway interact with the smart contract through its address and the authentication information of LoRa end device is saved in the blockchain network based on the join request's block id field. LoRaWAN network server uses call function, along with the block id, to retrieve this saved information from blockchain network to authenticate LoRa end device.

E. Blockchain Network

In our framework, private blockchain has been used as a blockchain network for the sake of simplicity. Private blockchain has been chosen to evaluate the system since it provides better and reliable result than public blockchains. However, public blockchain should be utilized in our proposed framework. In the private blockchains, only private nodes can write data however, anyone in the network can read the data. The data, stored in the blockchain network, is fully tamper-proof and decentralized.

IV. System Interaction

This section explains the interaction between different components of the proposed framework. These interactions can be classified into three stages: Setting up the blockchain network, Initial authentication and registration of LoRa end device in blockchain network, and finally the two factor authentication of LoRa end device using blockchain, in LoRaWAN network.

A. Setting up Blockchain Network

In this phase, the smart contract is deployed in the blockchain network by the agent node. After the smart contract has been deployed, the address of smart contract is replied by the blockchain network. The LoRaWAN network server uses this address of the smart contract to read the device information from the blockchain network, while the device information is written on the blockchain network when the gateway sends the transaction to smart contract. Gateway will only forward the join request message to blockchain network if the join request's block id field is empty.

B. Initial Authentication and Registration

In order to connect to the LoRaWAN network server, a join request message is sent from the LoRa end device to the gateway. LoRa end device is performing the join procedure for the first time so, the join request's block id field is empty. Also, the join request message is unencrypted according to LoRaWAN specification v1.1. The gateway forward this request to the network server as well as to the smart contract, using smart contract address. The validity of join request message will be checked by the LoRaWAN network server. Meanwhile, the blockchain network will mine the device information, sent to smart contract. After mining, the block id will be sent to network server and the join accept message will be sent by the network server to LoRa end device along with the block id. At this point, the information of LoRa end device is registered in the blockchain network and LoRa end device is also connected to the LoRaWAN network server for the first time.

C. Two Factor Authentication

After registering the LoRa end device information in the blockchain network, the information will be authenticated through normal LoRaWAN join procedure as well as by the information stored in the blockchain network. For the second time, when the LoRa end device wants to join LoRaWAN network, it send the join request message along with the block id. At this point, 128 bit NwkKey will be used to encrypt the join request message. After receiving the join request message, LoRaWAN network server will use the given block id to retrieve the data from the blockchain network. If the LoRa end device's information, saved in the blockchain network, matches with the current join request message information, LoRaWAN network server will check the authenticity of join request message using the current LoRaWAN join procedure protocol, defined in LoRaWAN specification v1.1. If the join request message passes both the authentication checks, the network server will reply with a join accept message and the LoRa end device will be connected to the LoRaWAN network server.

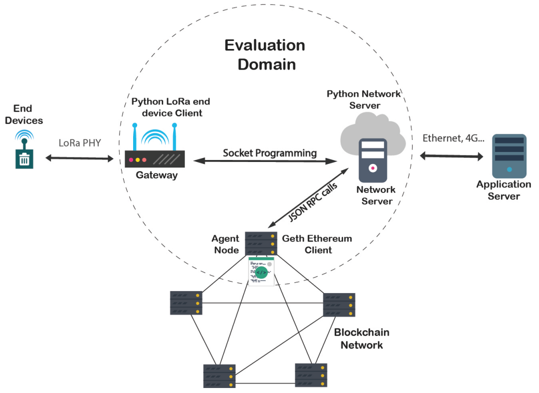

Fig. 4. Evaluation Domain

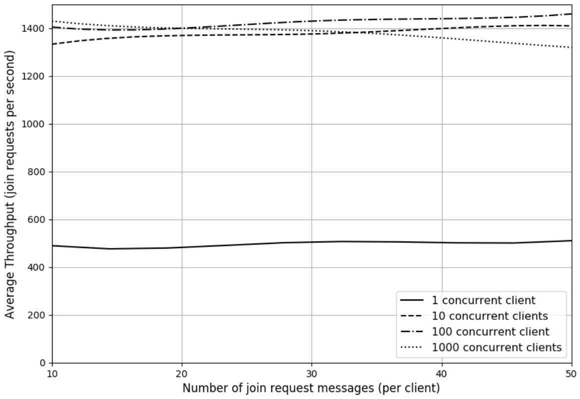

Fig. 5. Average Throughput

The proposed blockchain based LoRaWAN join procedure architecture is designed explicitly to enhance the trust and security in LoRaWAN join procedure. The join request message will be encrypted and the block id will be unique for each LoRa end device. Thus, two way authentication will enhance security and trust among LoRaWAN network entities. However, the main limitation of our system is that the first join request message from LoRa end device will experience significant delay since the authentication information of LoRa end device is mined in the blockchain network to get the block id.

V. Results

A. Implementation

UBUNTU 16.04 desktop with Intel(R) Core(TM) i7-6700 @ 3.40 Ghz specifications was used to perform the experiments. The simulation scenario for two factor authentication in LoRaWAN join procedure is shown in Fig. 4. To simulate the proposed framework, a private blockchain was implemented using geth Ethereum client. Ethereum is one of the most popular blockchain platform and has been extensively examined by the developers and researchers, in terms of performance [14][15]. Thus, the evaluation of Ethereum blockchain is ignored intentionally and the performance of the components, outside the blockchain network i.e. network server and LoRa end device, is evaluated. Moreover, in the simulations, we assumed that join request message from LoRa end device is already at the gateway since the physical layer delay parameters for LoRa relies on the Spreading Factor (SF) [16]. It is also assumed that blockchain network contains the LoRa end device information. LoRa end device client is implemented using the Python programming language, to generate the concurrent join request messages and the LoRaWAN network server is implemented with a server written in Python, which communicates wth LoRa end device Python client using socket programming. A smart contract is deployed on Ethereum private blockchain to save LoRa end device information. The LoRa end device information is retrieved from the blockchain network using JSON RPC calls on real time and a join accept message is sent back to Python LoRa end device client using socket programming. Each experiment is repeated 5 times to calculate the average values of throughput and latency for different concurrent clients, in the range from 1 to 1000.

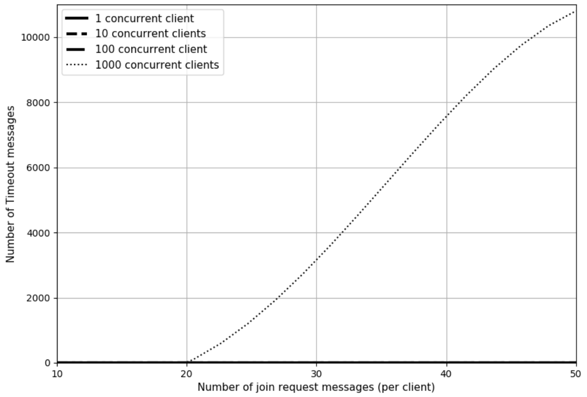

Fig. 6. Timeout messages

B. Evaluation

First, we evaluate the performance of network server in terms of throughput. Throughput is defined as the number of join request messages, a network server processes, in a second. In this scenario, the LoRa end device Python client sends the join request message to Python network server using socket programming. Once the request is received, the Python network server use JSON RPC call to fetches the device information from smart contract using the block id field in join request message and if the device information matches, it then checks the validity of other fields in the join request message i.e. DevNonce and reply with a join accept message to LoRa end device Python client. Fig. 5 shows the average throughput at the network server. It can be seen that for the average throughput for all the clients remains almost unchanged for different number of join request messages.

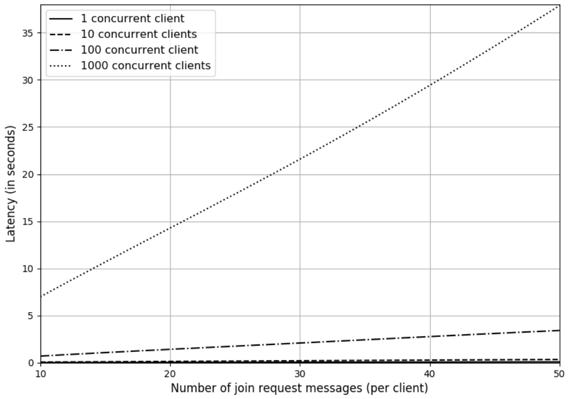

Fig. 7. Latency

However, increasing the number of concurrent clients from 1 to 100 increases the throughput at the LoRaWAN network server. However, when the concurrent clients are increased to 1000, the throughput decrease slightly with the increase in per client's join request message and the behavior is related to timeout messages as shown in Fig. 6. Secondly, we evaluate the performance of network server in terms of latency using the same aforementioned scenario. Latency is defined as the amount of time required by the network server in retrieving the device information from blockchain network and replying back the join accept message to LoRa end device. Fig. 7 shows the average latency for fetching the device information from blockchain network. What stands out from the graph is that the latency increases with the increasing number of join request messages per client. It can also be seen that increasing the number of concurrent clients from 1 to 1000 results in an increases in the average latency at network server.

It can be seen from the above results that as the number of concurrent clients increase, the throughput at the network server increases. However, increasing the number of concurrent clients and join requests, the latency increases significantly. This increase in latency is because of the addition of blockchain authentication check in LoRaWAN join procedure. However, keeping in mind the fact that LoRa end device normally performs the authentication mechanism one time in a day, our proposed system provides efficient system performance with enhanced security.

VI. Conclusion

The join request message in LoRaWAN join procedure is not encrypted and is susceptible to jamming and replay attacks. Also, the centralized nature of network servers raise the trust issues between network servers and LoRa end device since, the network server can modify the user's private data. In this paper, we propose two factor authentication mechanism for LoRaWAN join procedure to enhance authentication security and to build trust among LoRa end devices and network server, by employing blockchain in LoRaWAN network. A smart contract is employed to read and write information in the blockchain network. Also, the blockchain technology is not combined with the gateways and LoRa end device because of their low computational complexities. The proposed framework is simulated using the Ethereum blockchain and Python client and server implementation of LoRa end device and network server respectively. The simulation results demonstrate that the proposed framework provides efficient system performance in terms of throughput and latency. The proposed blockchain architecture is a cost effective solution, which can be utilized in the LoRaWAN network with few LoRa end devices and network servers, having no strict requirement of latency and throughput. In future, we are planning the hardware implementation of the proposed framework.

References

[1] Christidis, Konstantinos, and Michael Devetsikiotis, *Blockchains and smart contracts for the internet of things.*: IEEE Access: 2292-2303, 2016.

[2] "Gartner Says 20.4 Billion Connected Things" Will Be in Use in 2020", 2017. [Online]. Available: https://www.gartner.com/newsroom/id/3598917

[3] Emekcan Aras, Gowri Sankar Ramachandran, Piers Lawrence and Danny Hughes,, *Exploring The Security Vulnerabilities of LoRa*: International Conference on Cybernetics (CYBCONF), 2017.

[4] JungWoon Lee, DongYeop Hwang, JiHong Park, and Ki-Hyung Kim, *Risk Analysis and Countermeasure for Bit-Flipping Attack in LoRaWAN*: International Conference on Information Networking (ICOIN), 2017.

[5] Emekcan Aras, Gowri Sankar Ramachandran, Piers Lawrence and Danny Hughes, *Exploring The Security Vulnerabilities of LoRa*: International Conference on Cybernetics (CYBCONF), 2017.

[6] SeungJae Na, DongYeop Hwang, WoonSeob Shin, and Ki-Hyung Kim, *Scenario and Countermeasure for Replay Attack Using join request Messages in LoRaWAN*: International Conference on Information Networking (ICOIN), 2017.

[7] Stefano Tomasin, Simone Zulian and Lorenzo Vangelista, *Security Analysis of LoRaWANTM Join Procedure for Internet of Things Networks*: IEEE Wireless Communications and Networking Conference Workshops (WCNCW), 2017.

[8] S. M. Danish, A. Nasir, H. K. Qureshi, A. B. Ashfaq, S. Mumtaz, J. Rodriguez, *Network Intrusion Detection System for Jamming Attack in LoRaWAN Join Procedure*: Proceedings of the 54th IEEE International Conference on Communications (ICC), pp. , May, 2018

[9] Hammi, Mohamed Tahar, Patrick Bellot, and Ahmed Serhrouchni, *BC-Trust: A decentralized authentication blockchain-based mechanism*: In IEEE Wireless Communications and Networking Conference (WCNC), pp. 1-6. IEEE, 2018.

[10] Lee, Chan Hyeok, and Ki-Hyung Kim, *Implementation of IoT system using block chain with authentication and data protection.*: In IEEE International Conference on Information Networking (ICOIN), pp. 936-940, 2018.

[11] Zhu, Xiaoyang, Youakim Badr, Jesus Pacheco, and Salim Hariri, *Autonomic Identity Framework for the Internet of Things.*: In IEEE International Conference on Cloud and Autonomic Computing (ICCAC), pp. 69-79, 2017.

[12] Wu, Longfei, Xiaojiang Du, Wei Wang, and Bin Lin, *An out-of-band authentication scheme for internet of things using blockchain technology.*: In IEEE International Conference on Computing, Networking and Communications (ICNC), pp. 769-773. 2018.

[13] Jun Lin, Zhiqi Shen, and Chunyan Miao, *Using Blockchain Technology to Build Trust in Sharing LoRaWAN IoT*: In Proceedings of the ACM 2nd International Conference on Crowd Science and Engineering (ICCSE'17) pp. 38-43, 2017.

[14] https://github.com/ethereum/tests

[15] https://blog.ethcore.io/performance-analysis/

[16] https://www.semtech.com/images/datasheet/LoraDesignGuide_STD.pdf