Computing and Informatics, Vol. 41, 2022, 424–442, doi: 10.31577/cai_2022_2_424

SECURE AND EFFICIENT BLOCKCHAIN SCHEME FOR THE INTERNET OF BIKES

Bacem Mbarek, Tomáš Pitner

Faculty of Informatics, Masaryk University
Brno, Czech Republic
e-mail: bacem.mbarek@mail.muni.cz, tomp@fi.muni.cz

Abstract. Blockchain has recently emerged as an auspicious technology for enabling vulnerable data to be exchanged anonymously and securely within Intelligent Transportation System (ITS). Furthermore, Blockchain can be used as an access control mechanism to present a decentralized solution to the distributed authentication problem in the Internet of Bikes (IoB). Although several Blockchain access control mechanisms have been proposed to address the security concerns in IoB, most of them are still vulnerable to some active attacks, especially the cloning attacks. Therefore, this paper proposes a new Trust-Based Access Control Blockchain System (TBACS) to address the cloning attack based on using a secure Trusted Digital Ticket (DGT). The simulations of our solution through the Hyperledger Fabric are showing relevant results in terms of communication overhead and the detection probability of cloning attacks.

Keywords: IoT, Blockchain, security, IoB, cloning attacks, trust

1 INTRODUCTION

With the rapid growth of the Internet of Things (IoT), the term "Blockchain" gained popularity with IoT applications. Blockchain has a great potential to overcome security and privacy challenges of most distributed systems by efficiently establishing trust among nodes, especially in emerging networks [1]. Such a fundamental technology to enable decentralization plays an important role in a wide spectrum of topics such as Internet of Things (IoT) [2], Cyber-Physical Systems (CPS) [3], edge computing [4], cloud computing [5], fog computing [6], social networks [7], vehicular networks [8], and many more. Currently, most information generated within the IoT ecosystem is likely to be stored in a distributed database.

The IoB (Internet of Bikes) is one of the widely spreading examples of distributed applications [9], urging for highly secure, independent and distributed platform, which Blockchain is capable of supporting. However, Blockchain is computationally expensive, it has limited scalability and incurs significant bandwidth overhead and delays and it all hinders its suitability for the IoT/IoB context. Moreover, Blockchain needs to be established in IoB applications in order to truly leverage the benefits provided by its distributed ledger to find solutions to problems in bike sharing such as bike deployment, redistribution, parking and maintenance. Due to the nature of the Blockchain, all bikes information in the edge can be tracked in a synchronized and distributed blocks.

While the IoB brings comfort and convenience to the public bicycles operating system, it is usually vulnerable and exposed to different attacks. For instance, one of the well-known attacks in public bicycles operating systems is to intercept the keys used between the bike and the station. An adversary could inject a clone attack inside the bike sharing system channel. This attack could insert false information about the cloned bike such as wrong location, false parking information to steal the bike, wrong declaration that the bike is stolen or broken, etc.

If the attacker created and implemented a cloned bike in the public bicycles network by duplicating data (ID and shared key) from an existing bike, the cloned bike cannot be detected and no alert could arise on the system's display as well. However, by using a mobile Digital Ticket, containing the historical transactions between a bike and a bike station, the bike station can discover and verify the legitimacy of bike profiles if they are recognized in the historical transactions. Yet, despite the availability of traditional access control systems with the verification of encrypted data, including those based on Blockchain, IoT networks are still being subject to the clone-nodes network attacks [10, 1, 2]. This is because the existing authentication approaches are still vulnerable to cloning attacks, since the adversary can easily learn the critical nodes to start specific attacks and protect replicas from being detected.

In this paper we address this gap by proposing a secure and efficient Blockchain scheme for the internet of bikes, named as *Trust-Based Access Control Blockchain System (TBACS)*, which ensures secure communication between the bikes and their network stations.

We use the IoB setting for demonstration and evaluation purposes, while TBACS is application agnostic and well-suited for diverse IoT applications. The main idea of our approach is to design and implement a secure and efficient model that is able to manage access control between bikes and their stations based on the Blockchain. In particular, we address the drawbacks of Blockchain access control protocols in terms of communication overhead and vulnerability to cloning attack, by using Trusted Digital Ticket (DGT) which is used as an authenticated key for detecting the illegible bikers.

The remainder of the paper is organized as follows. Section 2 discusses the state-of-the-art solutions that have been proposed to secure distributed IoT systems. Based on the related work overview, Section 3 proposes a new approach of integrating the Blockchain into our solution. In order to evaluate the proposed solution, Section 4 conducts a security analysis simulation by considering communication overhead and detection probability of cloning attacks. Finally, Section 5 concludes the paper and outlines future directions for this work.

2 RELATED WORK

Bicycling [9] is a transport type enjoying increasing popularity in modern cities. For that reason, many works have exploited bikes as a smart IoT object for improving the quality of life of citizens, such as bicycle parking systems [11], which has been designed to manage personal bicycles in a campus (i.e., universities) to check bike parking availability automatically.

Another interesting IoB work [12] has proposed a smart management framework for Bike Sharing Systems (BSSs) that allow rebalancing the reservation policies according to priority users. To do that, the IoB framework gathers real-time logistic data. However, the design does not ensure a flow of correct data throughout the system. In this case, IoB services could be disrupted, and the safety of bikers is not guaranteed. To encounter security issues, a variety of solutions have explored the security problems in IoB to identify the attacks and propose secure access control management mechanisms between bikes and their stations in the IoB network [13, 14, 15, 9]. These solutions could be classified in two categories: **Centralized Access Control** and **Distributed Access Control**.

The first category focuses on the security of centralized access control management of bikes. For that reason, much effort has been made to achieve the security of **centralized station** and its bikes. In [13] the authors have used symmetric key encryption and digital signature algorithms for securing user information and bike sharing services. The proposed solution prevents an attacker from accessing the bike user information (i.e., Id user), BSS data (i.e., parking), and external services provided by IoT devices (i.e., location and weather data). As a result, it ensures a high quality of bike services (i.e., reservation) to the end-client in a secure way.

Similarly, the protection of bikers is discussed deeply in [16] to identify the risks that prevent the success of next BSS generation, such as security attacks and misbehaviour detection that could vary from biker to biker. Furthermore, the authors have highlighted the importance of building security services based on the current context of IoB to ensure the safety of bikers such as avoiding bike-vehicle collisions.

To further improve the security of centralized bike stations, different researchers proposed the integration of cloud computing in the centralized platforms to mange a large number of bikes. For that reason, many BSSs have started to release their own generated data to the public by excluding the user's sensitive information [14]. However, publishing of bike data without taking any precaution could disclose the biker's privacy with their in-depth movement patterns, recognizing the biker identity or its trajectories frequency with exact locations, which can be used unfavorably for inference attacks. That means an adversary can arrange published datasets based on the presence of location and timing bike information. To solve this issue, in [17], the authors have proposed an effective grouping method for avoiding the leakage of users' sensitive data. The proposed solution uses the anonymization method to minimize the probability of a successful linking attack by reducing the confidence that the adversary will have when breaching personal privacy. As a result, it protects users and bike sharing datasets from disclosure risks. However, an adversary may examine the intersection of anonymized datasets to re-identify user information even though they are preserved in each separate publication [1, 2, 7, 3]. Accordingly, independent data publishing presents new challenges for data privacy and security.

Another centralized security strategy based on space-time security protocol has been proposed in [18], where the authors have utilized the proposed protocol for monitoring public bicycle's real-time status. To do that, they have exploited the centralized cloud servers to control the BSS process and get the bicycle's real-time trajectory and riding status. Besides, they have proposed a smart lock that generates a dynamic password randomly based on location service and Bluetooth connection. Furthermore, they have designed a cooperative game model to rebalance bicycles in remote locations and areas with low traffic stream. As a result, the proposed model could manage the redistribution of bikes in urban places efficiently.

Similarly, in [19], the centralized platforms have been used for controlling the access to BSS services, where the authors have split a secret image into two parts based on visual cryptography. One stored in a cloud server and second posted on the bike. In this case, the identification of the legitimate users is done by constructing the original image based on two stored shadows. As a result, the security of the user information and BSS services are ensured. However, the unstable connection between cloud servers and IoB devices could cause communication delay as well as prevent the proposed model from achieving optimal performance and security scores.

The second category explores distributed systems in IoB, often based on the Blockchain technology, since these offer many advantages compared to centralized servers. For example, in [15], the authors have developed a bike sharing system based on a Blockchain framework that provides an innovative platform for a new distributed and transparent BSS transaction mechanism. Furthermore, the usage of Blockchain as an underlying trust mechanism prevents leakage of user privacy and unauthorized use of sharing bike services. However, the authors have applied the Blockchain technique directly without investigating the other Blockchain effects, such as Blockchain performance, anonymity, scalability, decentralization, and persistence [2].

For example, in [10], a Blockchain platform, named FairAccess, has been proposed to secure the IoT network by using smart contracts. In FairAccess a smart contract is basically a computerized transaction protocol that executes the terms of the agreement. In the simple definition, smart contracts are programs written by users to be uploaded and executed on the Blockchain to express fine-grained and contextual access control policies enveloped inside transactions. However, one of the drawbacks of using smart contracts is that it is relatively expensive, and needs large storage to be uploaded to the distributed blocks. Yet, this could minimize the performance of Blockchain process since it causes a problem for network scalability (i.e., delay issue). Another issue is regarding the storage of new data in the Blockchain, where it is necessary to download a full chain to all nodes [10].

Therefore, the development of a BSS architecture-based Blockchain system with scalable communication network is required for ensuring the safety of users as well as the transmission of aggregated bike data. Thus, in this paper, we tackle Blockchain authentication by considering the problem of cloning attack, which is a critical security problem in the IoB paradigm.

In the following, we describe in detail the main characteristics of Hyperledger Fabric based mechanisms that is of particular relevance to our work.

2.1 Hyperledger Fabric

Hyperledger Fabric is a Blockchain Framework used to create a Blockchain network from scratch and to define a large number of the network parameters, such as organizations or chaincodes.

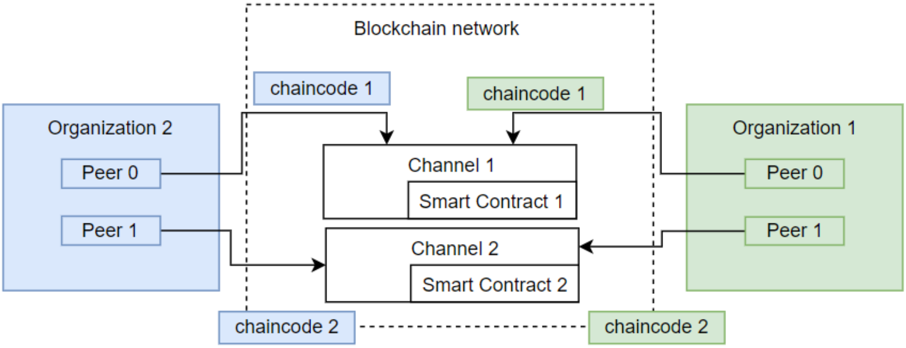

Figure 1. Hyperledger Fabric example network

An organization is composed of peer and authenticated by a couple private/public key, users are defined in the organizations and are authenticated like the peers. Organizations are connected to channels and can communicate through chaincodes on a smart contract. A chaincode is a set of functions that have to be used to interact with the smart contract related to it, a smart contract is a database model.

Figure 1 sums up the main characteristics about Hyperledger Fabric, the figure shows two organizations with two peers each connected to one channel and using on chaincode related to one smart contract.

The couchDB database is a database model that can be used in Hyperledger Fabric. Figure 2 presents how the ledger database is implemented in Hyperledger Fabric. This database is created in the peer and all the query or invoke operation are done in the peer. The couchdb database is different as it exists on its own through a docker. When data is query with a chaincode through one peer, a http request is sent to the couchDB docker. Then the database sends back a http response to the peer and the peer sends the information to the client. Figure 3 presents a scheme to explain how the peer is connected to the couchdb and how it communicates with it.

The advantages of the couchDB database are that queries are easier to make. Indeed, we can query data using column tagname of the table such as in an SQL query.

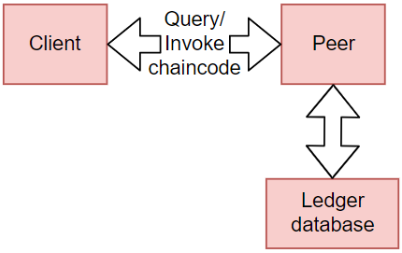

Figure 2. Ledger database

3 TBACS: TRUST-BASED ACCESS CONTROL BLOCKCHAIN SYSTEM

To address the cloning attacks in IoB environments, we propose a new Blockchain access control scheme based on the trusted Digital Ticket (DGT), which is used as an authenticated key for detecting the illegible bikers. Furthermore, we propose DGT not just for ensuring secure communication between bikes and stations, but also for reducing the overhead communication between the two entities. Moreover, for each bike-station interaction, the DGT is stored in smart contract and encrypted/decrypted with the asymmetric authentication technique.

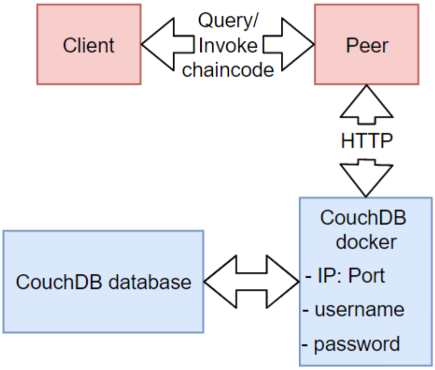

Figure 3. CouchDB database

There are two fundamental components in the IoB, which are the IoT devices plugged in bikes, and distributed platform installed in the bike stations. As shown in Figure 4, bike is a transmitter/receiver that sends requests/information to the bike station. Each bike has several embedded sensors that periodically generate data packets and store them in their buffers.

3.1 Overview of Our Layered Design

The implemented platform consists of four parts, as shown in Figure 5: bikes, ordering service, endorsing peers and committing peers.

Bikes: The data sensed by the bikes have to be transmitted to private Blockchain distributed ledgers.

Endorsing peers: A predefined number of bike stations. During the commissioning and configuration of the Blockchain network, the developers should select a number of bike stations defined as the endorsing peers.

Ordering service: It creates the block of transactions and sends it to all the peers. The ordering service collects transactions for a channel into proposed blocks for distribution to peers. Blocks are delivered on a channel basis. The ordering service accepts endorsed transactions, orders them into a block, and delivers the blocks to the committing peers. The main responsibility of ordering service is to receive transactions from the bikes and fit into a Block.

Committing peers: Usually endorsing peers are also committing, but a peer can be only committing and not endorsing. Committing peers (including endorsing peers) run validation and update their copy of the Blockchain and world state. Each peer receiving the block, now in the role of a committing peer, appends the whole block to its Blockchain copy. Committing peers are responsible for adding blocks of transactions to the shared ledger and updating the world state.

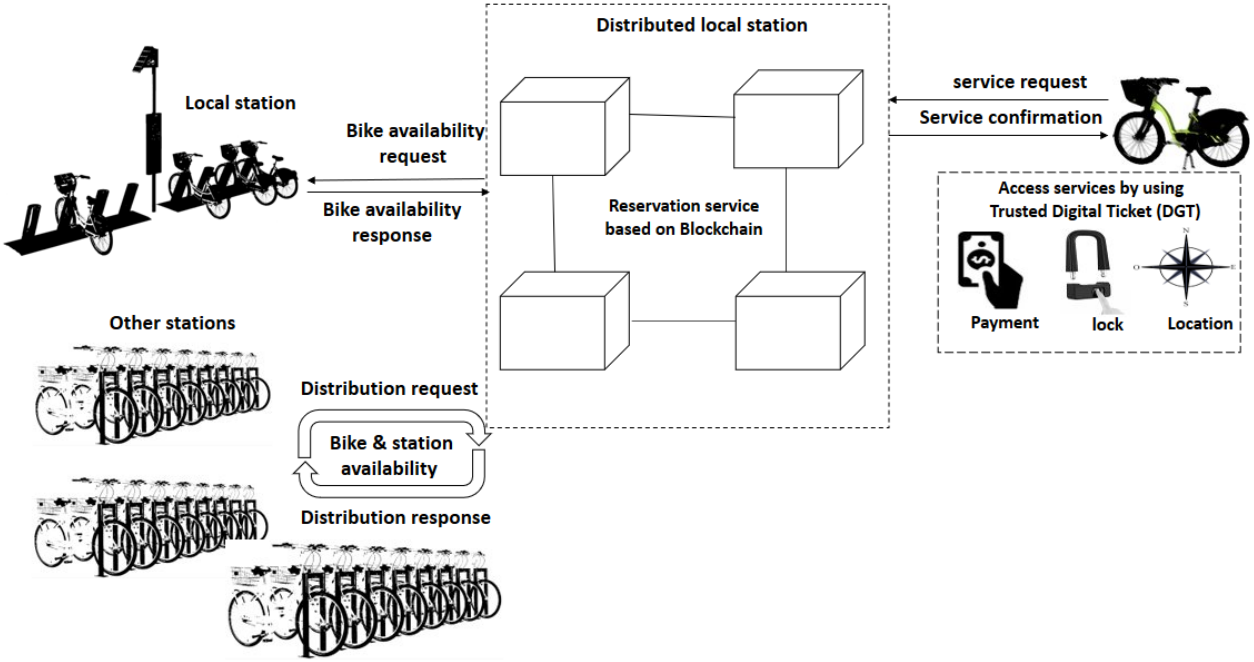
Local station
Bike availability request
Bike availability response
Distributed local station
Reservation service based on Blockchain
service request
Service confirmation
Access services by using Trusted Digital Ticket (DGT)
Payment
lock
Location
Other stations
Distribution request
Bike & station availability
Distribution response

Figure 4. Proposed internet of bikes network architecture

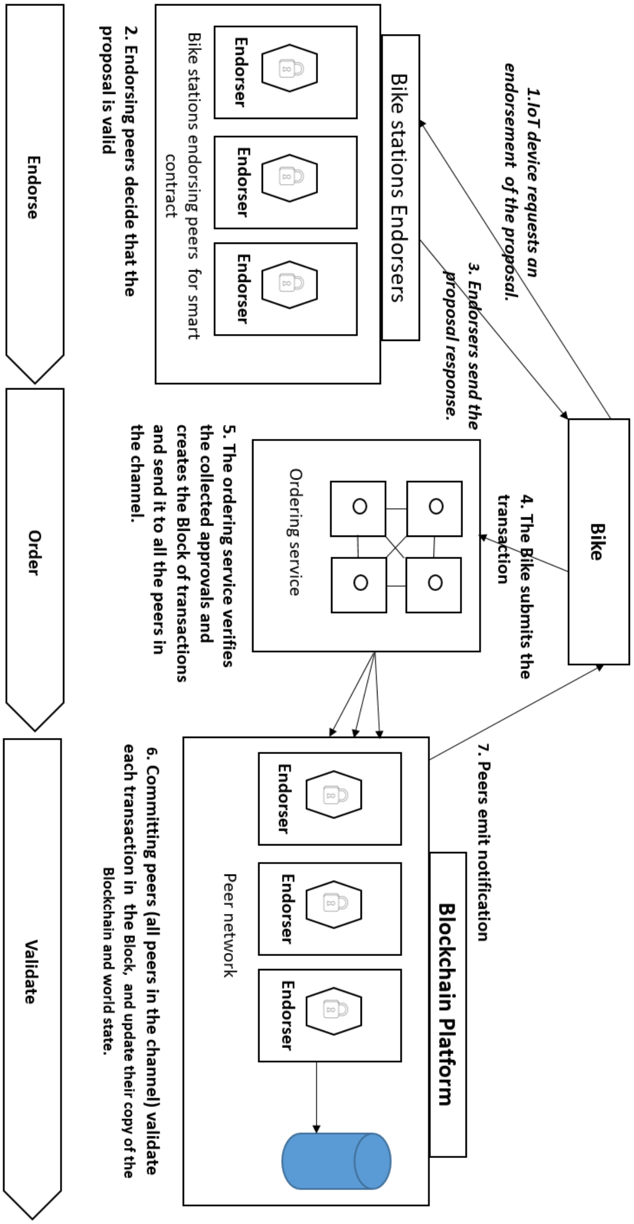
1.IoT device requests an endorsement of the proposal.
Bike stations Endorsers
Endorser
Endorser
Endorser
Bike stations endorsing peers for smart contract
2. Endorsing peers decide that the proposal is valid
Endorse
3. Endorsers send the proposal response.
Bike
4. The Bike submits the transaction
Ordering service
5. The ordering service verifies the collected approvals and creates the Block of transactions and send it to all the peers in the channel.
Order
7. Peers emit notification
Blockchain Platform
Endorser
Endorser
Endorser
Peer network
6. Committing peers (all peers in the channel) validate each transaction in the Block, and update their copy of the Blockchain and world state.
Validate

Figure 5. Order-execute architecture to storage data in TBACS Blockchain platform

3.1.1 Order-Execute Architecture in TBACS Blockchain Platform

Figure 5 shows the order-execute architecture to data storage in the IoB Blockchain platform. This architecture can be summarized as follows.

1. The bike submits endorsement requests to endorsing peers.
2. Endorsing peers decide that the proposal is valid or not after checking for consistency to the bike applicant. Each execution captures the set of read and written data (also called the RW set), which is flowing in the Hyperledger fabric. Moreover, the Endorsement System Chaincode (ESCC) signs the proposal response on the endorsing peer. The RW sets are signed by each endorser.
3. The endorsing peers send the proposal response to the bike.
4. The bike submits the transaction to the ordering service.
5. The ordering service verifies the collected endorsements and creates the Block of transactions and sends it to all the peers in the channel.
6. The committing peers validate each transaction in the Block, and update their copy of the Blockchain and world state.
7. The peers emit notification to the bike and send a DGT to the applicant bike.

3.2 Operation of DGT Ticket

The Digital Ticket (DGT) contains all previous transactions ID (ID is a special set of numbers that defines each transaction) made by a bike during the customer journey, where the bike station collects all ID transactions data into a DGT that is encrypted by the asymmetric authentication technique and stored inside a smart contract. Moreover, all transactions made by a bike are stored in the Blockchain platform and their IDs are stored in the DGT ticket.

Once the payment is made, the bike station charges the booked bike with an encrypted DGT. Moreover, our contribution includes the use of Digital Ticket to shorten the authentication process while offering the possibility to identify malicious nodes. Our Digital Ticket also enables reduction of the energy consumption as well as the communication overhead.

In order to implement our idea, the bike station creates a DGT dedicated to every new external peer requesting access to the IoB environment.

The DGT is used to ensure the authentication process by migrating to the bike with which its corresponding peer needs to be authenticated. To this end, it records the IDs of the current and previous transactions which enrolled between the bike and the bike station. It will also save and use various information, including the time of when it reached the current bike, the path leading to the current bike from the bike station, and the sensed data/message. Then, the DGT contains the different ID transactions made between the bike and the bike stations.

The DGT will migrate from the bike station to the bike. It will then be used by the bike for the next authentication to the network stations. It also updates their recorded IDs transactions and could be used to enforce security by identifying potential malicious nodes. The DGT is presented as follows.

$$DGT = ID_{T_1}, ID_{T_2}, ID_{T_3}, \ldots, ID_{T_N}, \tag{1}$$

$$Transaction_i = BikeID, Time, StationId, Path, Message. \tag{2}$$

Algorithm 1 describes a secure booking transaction requested by the user between the selected bike and its station.

When the user needs to reserve a bike from a bike station, he must use the platform of the selected bike to start the booking procedures. The user employs its bank card to make the payment. If the payment is made and the reservation is confirmed, the station creates a Digital Ticket (DGT) containing various information about the bike and the user.

Before sending the DGT, the station encrypts the ticket using a smart contract and asymmetric authenticated encryption algorithm [20]. Then, the station sends the DGT to the bike. After the reception of the bike, the receiver decrypts the DGT and verifies the ID transactions with their copies stored in the blockchain database. If the verification is correct, then the padlock of the bike is unlocked, and the user can use the bike for any new communication with any station in our defined network. The bike should use its DGT and execute Algorithm 2 for the access control management.

Algorithm 1: Bike reservation

```
Input: S: Station; B: Bike; BC: Blockchain; T: Transaction
Output: DGT : Digital ticket;
Data:
if payment is done then
    S create a DGT;
    encrypt(DGT);
    S send (encrypt(DGT)) to B;
    B decrypt(DGT);
else
    booking is denied;
```

3.3 Authentication Algorithm

Algorithm 2 gives a description of the access control management of a reserved bike.

First, the bike is enabled to access the station using its DGT given by the initial phase (bike reservation) described in Algorithm 1.

Second, the bike should encrypt the ticket and send it to the bike station.

Next, the bike station verifies the ticket by the decryption of the DGT. If the verification is correct, then the bike station randomly selects a number of IDs transactions from the DGT to verify and compare them by their copies in the Blockchain. If the selected IDs transactions are correct, then the ticket is considered to be valid.

Following this, the bike station grants access to the bike. During the communication with the bike, the station should record all of the new transactions inside both the DGT and the Blockchain. Finally, at the end of the session, the bike station encrypts the ticket and sends it to the bike. Algorithm 2 is executed for each new request session between the bike and the bike station by using the updated DGT.

Algorithm 2: Bike access control

```
Input:  DGT : Digital ticket; S: Station; B: Bike; BC: Blockchain; T:
        Transaction
Output: session access/deny;
if The user has a DGT =1 then
    B encrypts (DGT)
    B sends (encrypts (DGT)) to S.
if decryption(DGT)= true then
    S Select a randomly ID Transactions:$ID_{T_1}, ID_{T_2}, \ldots, ID_{T_N}$
for $i \leftarrow 1$ to $N$ do
    if $Blockchain[] = ID_{T_i}$ then
        access is granted;
        S records the new ID transactions both in DGT and the distributed
        Blockchain ;
    else
        access is denied;
```

3.3.1 Smart Contracts for Monetizing IoT Data

The concept of smart contracts can be used to automate negotiations between service providers and users along with required monetary transactions without a trusted intermediary. A Smart Contract is fundamentally a code that validates a negotiation and immediately brings a contract into effect, without the involvement of any intermediaries [21]. The smart contract code resides on a blockchain as multiple functions with unique addresses that can be called by any user of the Blockchain.

All entities interacting with a Blockchain (including users and Things) must own at least one public-private key pair. First of all the sender encrypts a smart contract with the public key. The receiver then receives the encrypted smart contract and decrypts it with the private key.

4 EVALUATION

In order to implement the Trust-Based Access Control Blockchain System (TBACS) for the IoB, we used Hyperledger Caliper software [22], which is a benchmark tool developed within the Hyperledger project [23]. We assess the performance of our scheme compared to up-to-date FairAccess [10] scheme, where FairAccess is a typical Blockchain access control scheme in IoB. We evaluate the two schemes in terms of detection probability and communication overhead. We run our simulations on a large-scale network of 500 bikes and 100 bikes station that initiate the communication in every iteration with all the settings given in Table 1.

This choice was motivated by the fact that both solutions are integrating the use of Blockchain-based authentication scheme for the IoB. The setup of our experiments is as follows:

1. Bike Nodes run on Fabric version v1.1.0-preview2 instrumented for performance evaluation through local logging;
2. All nodes are 2.0 GHz 16-vCPU VMs running Ubuntu with 8 GB of RAM and SSDs as local disks;
3. There are 50 bike station endorsers;
4. Signatures use the default SHA-1 scheme; and
5. We adopt 2 MB as Data block sizes.

During our experiments, we analysed the size mint and spend transactions. In particular, the 2 MB Data blocks contained 473 mint or 670 spend transactions. In other words, the average transaction size is 3.06 kB for spend and 4.33 kB for mint.

In general, transactions in Fabric are large because they carry certificate information. The results have been obtained by a confidence interval of 95 %.

Parameter	**Value**
Simulation time	100 s
Run times	50 times
Number of Bikes station	100
Number of Bikes	500

Table 1. Simulation parameters

4.1 Detection Probability of Cloned Nodes

Figure 6 shows the results for the replica detection probability of the TBACS protocol compared to the FairAccess protocol. In particular, it demonstrates that the probability of detecting a replica node is significantly lower when FairAccess is used.

By using TBACS, a cloning attack can be detected if the subjective trust is not verified. For instance, when the number of the replica nodes is 30, the replica detection probability is around 80 %. This can be explained by the fact that each bike station with TBACS in the network is able to verify the historical transactions of each bike; while the FairAccess protocol is not effective in detecting the cloning attacks. Therefore, the replica detection with FairAccess protocol is under 50 %, when the number of replica nodes is more than 30. Furthermore, it can be seen that when the number of replica nodes is more the 15, the decreasing rate of the FairAccess replica detection probability is significantly faster than the decreasing rate of TBACS. One possible reason is that when the number of the replica nodes is higher, the bike station with FairAccess will verify bike by only checking the authentication of the smart contract and is not effective in detecting cloned bikes.

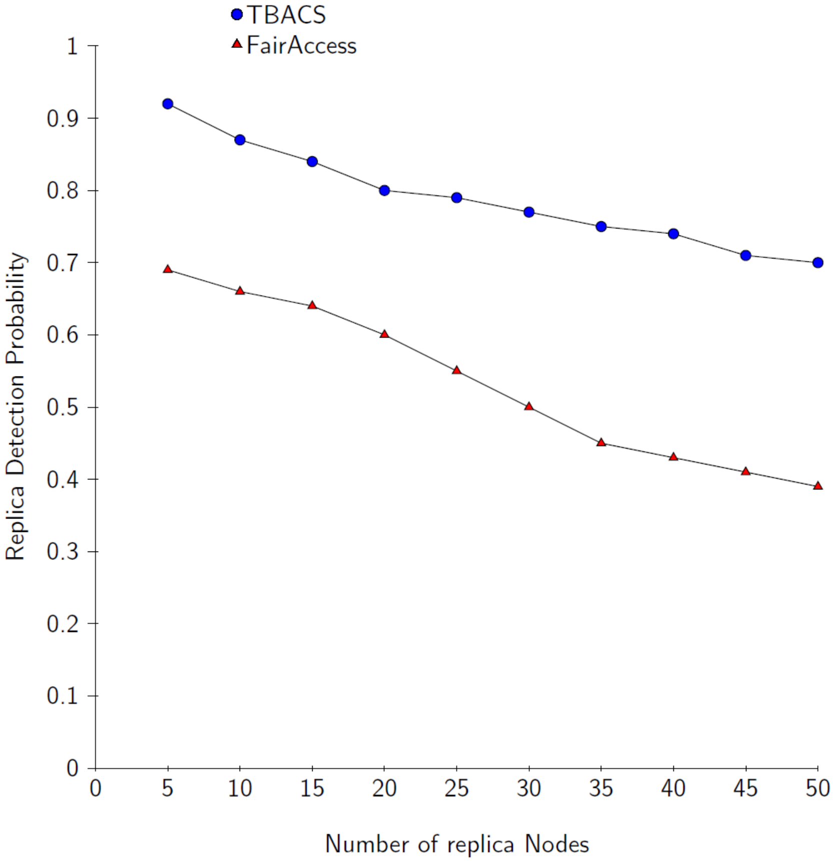

Figure 6. Evaluation of detection probability of replica nodes

4.2 Communication Overhead

Figure 7 illustrates the maximum communication overhead for the two protocols (TBACS and FairAccess), with varying time of simulation. For convenience, the time is expressed as a percentage with respect to the total duration of the simulation (i.e., 100 seconds).

We notice that TBACS has a significantly lower communication overhead than the FairAccess protocol. For example, when the simulation duration is 40, the percentage of communication overhead for TBACS is around 20 %; while it is around 42 % for FairAccess. In fact, TBACS uses historical transaction trust recorded in the DGT; while with FairAccess, the bike station should verify through all the distributed Blockchain by uploading and executing a contract. Smart contract storage is relatively expensive, with large storage to be uploaded to the Blockchain.

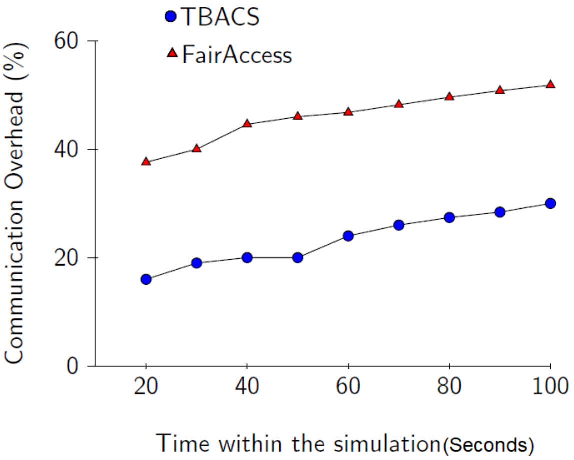

Figure 7. Communication overhead as a function of time

4.3 Discussions

The resistance of our protocol to the cloning attacks relies on the fact that the bike station can succeed in discovering the cloned bike by using the historical transaction IDs recorded in the DGT.

The adversary can discover the key and state the false identity of a bike to create a cloned bike to disturb the functions of the IoB network. To solve this issue, we introduce a new trust-based access control Blockchain system based on the recording trust historical transaction IDs on the Digital Ticket. Hence, our new trust authentication technique defeats the drawbacks of the previous FairAccess protocols in terms of cloning attacks. However, an attacker may try to access the internet of bikes environment without authorization with the aim to falsify the bikes network.

In order to prevent such threats, we are proposing to send encrypted bike information based on symmetric cryptographic key sharing. In addition, to guarantee confidentiality, our proposed security scheme allows for encrypting and generating illegible messages.

It has been proven (e.g., [20]) that these messages are only accessible by authenticated parties. For additional confidentiality, smart contract is used alongside with cryptography. Therefore, we propose a Blockchain-based system to enforce the privacy and security matters related to collecting, sharing, and managing vulnerable data. Moreover, we encounter the Blockchain overhead communication issues by deploying a Digital Ticket that collects relevant historical data into an image, creates encrypted data, reduces response time delays, and solves synchronization and scalability problems in IoB environment.

5 CONCLUSION

In this paper, we have proposed a new access control mechanism in the internet of bikes network called TBACS. Our solution is based on a secure Digital Ticket (DGT) in Blockahin that is capable of authenticating bikes to their stations by comparing the transaction IDs recorded into the DGT to their transaction IDs stored in the Blockchain platform which is installed and distributed to the stations. Moreover, we have proposed an asymmetric authenticated algorithm to aggregate and hide private bike data into selected images (DGT). Afterwards, we have studied the security issues in public bicycles operating systems, especially tackling the cloning attack.

Our simulation results have shown that the proposed TBACS significantly outperforms FairAccess as the state-of-the-art distributed security protocol, in both effectiveness and efficiency. From the effectiveness perspective, TBACS increases the detection probability of replica nodes in cloning attacks. It indicates that once the TBACS is applied in the internet of bikes, it can secure the information exchanges in bike sharing systems and protect the bike privacy in the internet of bikes environments. Considering the efficiency, the proposed TBACS indicates high performance enhancement comparing to FairAccess. For communication overhead evaluation, the FairAccess protocol consumes more time in the verification of the authenticity of the received transaction.

As for future works, we plan to conduct further real-world experiments in the internet of bikes by considering different security issues in the IoB environment. Also, as the convenience in IoB systems is combined with security and privacy issues, another future work is to increase the bike's awareness of IoB security vulnerability and privacy disclosure possibility in IoB networks. Further, the social and economic concerns can be raised due to security issues in IoB information systems.

REFERENCES

[1] Zhang, Y.—Wen, J.: The IoT Electric Business Model: Using Blockchain Technology for the Internet of Things. Peer-to-Peer Networking and Applications, Vol. 10, 2017, No. 4, pp. 983–994, doi: 10.1007/s12083-016-0456-1.

[2] Banerjee, M.—Lee, J.—Choo, K. K. R.: A Blockchain Future for Internet of Things Security: A Position Paper. Digital Communications and Networks, Vol. 4, 2018, No. 3, pp. 149–160, doi: 10.1016/j.dcan.2017.10.006.

[3] Zhao, Y.—Li, Y.—Mu, Q.—Yang, B.—Yu, Y.: Secure Pub-Sub: Blockchain-Based Fair Payment with Reputation for Reliable Cyber Physical Systems. IEEE Access, Vol. 6, 2018, pp. 12295–12303, doi: 10.1109/ACCESS.2018.2799205.

[4] Stanciu, A.: Blockchain Based Distributed Control System for Edge Computing. 2017 21st International Conference on Control Systems and Computer Science (CSCS), 2017, pp. 667–671, doi: 10.1109/CSCS.2017.102.

[5] Park, J. H.—Park, J. H.: Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions. Symmetry, Vol. 9, 2017, No. 8, Art. No. 164, doi: 10.3390/sym9080164.

[6] Liu, H.—Zhang, Y.—Yang, T.: Blockchain-Enabled Security in Electric Vehicles Cloud and Edge Computing. IEEE Network, Vol. 32, 2018, No. 3, pp. 78–83, doi: 10.1109/MNET.2018.1700344.

[7] Fu, D.—Fang, L.: Blockchain-Based Trusted Computing in Social Network. 2016 2nd IEEE International Conference on Computer and Communications (ICCC), 2016, pp. 19–22, doi: 10.1109/CompComm.2016.7924656.

[8] Yang, Z.—Yang, K.—Lei, L.—Zheng, K.—Leung, V. C. M.: Blockchain-Based Decentralized Trust Management in Vehicular Networks. IEEE Internet of Things Journal, Vol. 6, 2019, No. 2, pp. 1495–1505, doi: 10.1109/JIOT.2018.2836144.

[9] Behrendt, F.: Why Cycling Matters for Smart Cities. Internet of Bicycles for Intelligent Transport. Journal of Transport Geography, Vol. 56, 2016, pp. 157–164, doi: 10.1016/j.jtrangeo.2016.08.018.

[10] Ouaddah, A.—Abou Elkalam, A.—Ait Ouahman, A.: FairAccess: A New Blockchain-Based Access Control Framework for the Internet of Things. Security and Communication Networks, Vol. 9, 2016, No. 18, pp. 5943–5964, doi: 10.1002/sec.1748.

[11] Angulo-Esguerra, D.—Villate-Barrera, C.—Giral, W.—Florez, H. C.—Zona-Ortiz, A. T.—Díaz-Sánchez, F.: Parkurbike: An IoT-Based System for Bike Parking Occupation Checking. 2017 IEEE Colombian Conference on Communications and Computing (COLCOM), 2017, pp. 1–5, doi: 10.1109/ColComCon.2017.8088201.

[12] Razzaque, M. A.—Clarke, S.: Smart Management of Next Generation Bike Sharing Systems Using Internet of Things. International Smart Cities Conference (ISC2), 2015, pp. 1–8.

[13] Rahman, M. S.—Kiyomoto, S.: Secure Bike Sharing System for Multi-Modal Journey. 2016 IEEE International Conferences on Big Data and Cloud Computing (BDCloud), Social Computing and Networking (SocialCom), Sustainable Comput-

ing and Communications (SustainCom), 2016, pp. 437–444, doi: 10.1109/BDCloud-SocialCom-SustainCom.2016.71.

[14] Shen, S.—Wei, Z. Q.—Sun, L. J.—Su, Y. Q.—Wang, R. C.—Jiang, H. M.: The Shared Bicycle and Its Network – Internet of Shared Bicycle (IoSB): A Review and Survey. Sensors, Vol. 18, 2018, No. 8, Art. No. 2581, doi: 10.3390/s18082581.

[15] Guo, H.—Zhou, J.—Wang, J.—Wang, X.: A Bike Sharing System Based on Blockchain Platform. MATEC Web of Conferences, Vol. 232, 2018, doi: 10.1051/matecconf/201823201027.

[16] Razzaque, M. A.—Clarke, S.: A Security-Aware Safety Management Framework for IoT-Integrated Bikes. 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), 2015, pp. 92–97, doi: 10.1109/WF-IoT.2015.7389033.

[17] Hasan, A. S. M. T.—Jiang, Q.—Li, C.: An Effective Grouping Method for Privacy-Preserving Bike Sharing Data Publishing. Future Internet, Vol. 9, 2017, No. 4, Art. No. 65, doi: 10.3390/fi9040065.

[18] Peng, R.—Zhang, M.—Guo, C.—Cui, J.—Song, J.: Public Bicycle Operating System Based on Space-Time Security and the Internet of Things. Wuhan University Journal of Natural Sciences, Vol. 23, 2018, No. 6, pp. 541–548, doi: 10.1007/s11859-018-1360-8.

[19] Li, L.—Yu, J.—Wang, B.—Zhou, Q.—Zhang, S.—Lu, J.—Chang, C. C.: Multiple Schemes for Bike-Share Service Authentication Using QR Code and Visual Cryptography. In: Sun, X., Pan, Z., Bertino, E. (Eds.): Cloud Computing and Security (ICCCS 2018). Springer, Cham, Lecture Notes in Computer Science, Vol. 11065, 2018, pp. 629–640, doi: 10.1007/978-3-030-00012-7_57.

[20] Hamid, N.—Yahya, A.—Ahmad, R. B.—Al-Qershi, O. M.: Image Steganography Techniques: An Overview. International Journal of Computer Science and Security (IJCSS), Vol. 6, 2012, No. 3, pp. 168–187.

[21] Di Pierro, M.: What Is the Blockchain? Computing in Science and Engineering, Vol. 19, 2017, No. 5, pp. 92–95, doi: 10.1109/MCSE.2017.3421554.

[22] Sukhwani, H.—Wang, N.—Trivedi, K. S.—Rindos, A.: Performance Modeling of Hyperledger Fabric (Permissioned Blockchain Network). 2018 IEEE 17th International Symposium on Network Computing and Applications (NCA), 2018, pp. 1–8, doi: 10.1109/NCA.2018.8548070.

[23] Hyperledger Fabric. `https://github.com/hyperledger/fabric`.

Bacem Mbarek is Senior Researcher at the Faculty of Informatics, Masaryk University in Brno, Czech Republic. In 2017, he received his Ph.D. degree from the National Engineering School of Tunis, Tunisia. He was Assistant Researcher at the German University of Technology in Oman (GUtech), in 2017–2018. He was Visiting Researcher at the University of Bordeaux (2014–2015). His main research interest is in the area of Blockchain, network security, and IoT. He is involved in different European and international projects as well as standardization efforts. He published several scientific papers in high ranked conferences and journals in his field of research. He served on many programs and organization committees of international conferences and workshops.

Tomáš Pitner received his Ph.D. from Masaryk University in Brno, Czech Republic, in 1998. Since 2008, he has been Associate Professor, Academic Director at Center for Research and Education in IT (CERIT), and Head of the Lasaris Research Laboratory at Masaryk University. Since 2007 he has worked as an external Professor at the Faculty of Computer Science at the University of Vienna. His research focuses primarily on cybersecurity, critical infrastructures, namely for power grids, e-health applications, enterprise software architectures and technologies. He also deals with the communication aspects of academic and industrial cooperation. He leads large-scale applied and contractual research projects in the field of smart grids. He acts as Secretary of International Advisory Board at National Competence Centre for Cybersecurity (NC3) since 2019, and he led the Research Program at the Czech CyberCrime and Critical Information Infrastructure Protection Center of Excellence (C4e).