IEEE INFOCOM 2022 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS) | 978-1-6654-0926-1/22/$31.00 ©2022 IEEE | DOI: 10.1109/INFOCOMWKSHPS54753.2022.9798114

BDESF-ITS: Blockchain-Based Secure Data Exchange and Storage Framework for Intelligent Transportation System

Naivedya Lath*, *Student Member, IEEE*, Kaustubh Thapliyal†, *Student Member, IEEE*,
Kartik Kandpal‡, *Student Member, IEEE*, Mohammad Wazid§, *Senior Member, IEEE*,
Ashok Kumar Das¶, *Senior Member, IEEE*, and D. P. Singh ‖, *Member, IEEE*

* Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun 248 002, India
naivedyalath@gmail.com

† Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun 248 002, India
kaustubhthapliyal611@gmail.com

‡ Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun 248 002, India
kartik78946@gmail.com

§ Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun 248 002, India
wazidkec2005@gmail.com

¶ Center for Security, Theory and Algorithmic Research,
International Institute of Information Technology, Hyderabad 500 032, India
ashok.das@iiit.ac.in, iitkgp.akdas@gmail.com

‖ Department of Computer Science and Engineering, Graphic Era Deemed to be University, Dehradun 248 002, India
devesh.geu@gmail.com

***Abstract*—The communication in Intelligent Transportation Systems (ITS) suffers from various security and privacy related issues as several attacks, like replay, man-in-the-middle (MiTM), impersonation, data leakage and unauthorised data update attacks can be mounted by an adversary. Therefore, we need a robust security mechanism to sort out such issues, which can be further enhanced through the use of mechanism of blockchain technology. In this paper, we propose a blockchain-based secure data exchange and storage framework for the ITS (in short, we call it as BDESF-ITS). We conduct the security analysis of the BDESF-ITS to prove its robustness against various possible attacks. The practical implementation of the BDESF-ITS is also carried out to observe its behaviour with the real world settings.**

***Index Terms*—Intelligent transportation system (ITS), authentication, privacy, security, blockchain simulation.**

I. Introduction

Intelligent transportation systems (ITS) is a combination of potential information and communication technologies (i.e., smart devices, smart vehicles) that can be used in transportation and traffic management systems. It improves the safety, efficiency and sustainability of transportation networks that further reduce the traffic congestion and enhance the drivers experiences. In the ITS, smart vehicles and other devices communicate through insecure (open) communication channels over the Internet. It is not secure in nature as various information security related attacks (for instance, "replay, man-in-the-middle (MiTM), impersonation, data leakage, unauthorised data update, etc.," attacks) are possible. Therefore, we need some emerging tools and technologies to resolve the security related issues of the ITS. Blockchain seems to be one of the emerging technologies and it can help us to sort out the issues.

Blockchain is a technology that can be used to store various types of data (i.e., ITS related data, healthcare data and industrial data). Data is stored in the blockchain in the form of blocks of chain. Blockchain is also known as a decentralized distributed network that can be used to store data in the form of blocks. Blockchain technology works on the basis of certain consensus algorithms (i.e., Proof of Work (PoW) algorithm). Each block in a blockchain can be added when it is verified and checked by the existing entities (i.e., miner nodes) that are present in the blockchain network. Each block in the chain contains information, like the "hash of the block, hash value of the previous block and signature of the block". Hashing is technique or a procedure in which the data or integrity of the block is protected. Every block in the blockchain has a unique digital signature that can be used for the verification purpose before its addition into the blockchain. The first block that is added int the chain which is known as the "genesis block" and it does not include the hash value of previous blocks. The blocks are connected through the cryptographic hash values. Thus, it is also called as hash chain. Each miner node competes based on their respective computing power to solve a mathematical puzzle, which is complicated to solve but easy to verify in case of PoW consensus algorithm. The first miner node that solves the puzzle is rewarded accordingly.

978-1-6654-0926-1/22/$31.00 ©2022 IEEE

A. Motivation

The improper management of a transportation system in the most of the countries causes the life or death situation for the people. As we know the communication of ITS suffers from various security and privacy related issues, we need some security mechanism to sort out these issues. The security and privacy related issues of ITS can be resolved through the inclusion of mechanism of blockchain. Hence, in this paper, we propose a blockchain based secure data exchange and storage framework for the ITS. The data of ITS may be "confidential and private". Therefore, if we put the confidential and private data of ITS on a "public blockchain" or on a "hybrid blockchain", this may raise privacy related issues. It is then recommended to consider such data to be put in encrypted form in the blockchin too.

B. Research Contributions

The main research contributions of the paper are given below.

- We propose a blockchain based secure data exchange and storage framework for the ITS (in short, we call it as BDESF-ITS).
- We conduct the security analysis of the BDESF-ITS to prove its security against the potential attacks of the domain.
- The practical implementation of the BDESF-ITS is also carried out to observe its behaviour with the real world settings.

C. Paper Outline

The rest of the paper is outlined as follows. In Section II, we provide the related work study on the existing state of art solutions. In Section III, we discuss both the network and threat models. The threat model deals with all the possible capabilities of an adversary. The proposed scheme has been then described in Section IV. A brief security analysis has been provided in Section V. A detailed blockchain implementation of the proposed scheme is provided in Section VI. Finally, some concluding remarks have been drawn in Section VII.

II. Related Work

Herrera-Quintero *et al.* [1] proposed an ITS smart sensor prototype through the inclusion of Internet of Things (IoT) and the "serverless and microservice architecture" for the ITS (i.e., Bus Rapid Transit (BRT) systems). In their prototype, several Bluetooth signals of different devices, such as mobile phones, can be detected where people may use while travelling by the BRT system.

Kaffash *et al.* [2] provided a comprehensive survey of the applications of ITS. They also provided the survey of most of the recognized models in which Big data is applicable in the context of ITS.

Lian *et al.* [3] reviewed some mechanisms, which use the Big data to analyze the traffic safety in ITS. Their main focus was on discussing the important aspects, like crash prediction and detection and the factors, which contribute to the crash and driving behavior. Aujla *et al.* [4] also discussed the mechanisms for secure storage, verification as well as suditing of Big data in a cloud environment.

Srinivas *et al.* [5] presented a "three-factor user authentication scheme (UAP-BCIoT)" through the elliptic-curve cryptography (ECC). In UAP-BCIoT, the mutual authentication between a legitimate user and an IoT device is achieved through the cloud gateway node. In UAP-BCIoT, several functionality features, like "password/biometric update phase", "dynamic IoT device addition phase" and "user mobile device revocation phase if the mobile device of an authorized registered user is stolen/lost" are supported. Furthermore, UAP-BCIoT also offers IoT devices credential validation along with the Big data analytics.

Garg *et al.* [6] presented a "key management protocol for Internet of Medical Things, called BAKMP-IoMT". They provided the formal security verification of their scheme. Aujla *et al.* [7] presented a decoupled blockchain-based scheme for the edge-based ecosystem. This scheme leverages the edge nodes (devices) to create the decoupled blocks in blockchain. This securely transmits the healthcare data from the sensors to the edge devices.

Chaudhary *et al.* [8] presented a "BEST-blockchain-based secure energy trading scheme for electric vehicles (EVs)". In their scheme, the blockchain was used to validate the requests from EVs in a distributed manner. This ensures the resilience against the "single point of failure". Moreover, several other security protocols in IoT-enabled ITS environments as well as other IoT-based environments have been suggested in the literature [9], [10], [11], [12], [13], [14], [15].

In recent years, the blockchain technology has been applied in ITS in order to enhance the security of the system by incorporating with the access control and authentication techniques [16], [17], [18], [19].

III. System Models

In this section, we discuss the network and threat models that associated with the proposed BDESF-ITS. The detailed descriptions of these models are given below.

A. Network Model

The network model of BDESF-ITS is depicted in Fig. 1. In this model, we have three different layers. At the layer 1, we have different smart devices, smart vehicles and access points, which collect data from the smart appliances and then forward the data to the higher layer (i.e., the content routers of layer 2). The content routers perform the routing of the data to the servers of the data centers at the data center layer (layer 3). At the layer 3, the data of ITS is stored in the form of the blocks through the implemented blockchain. However, all steps of consensus algorithm (Practical Byzantine Fault Tolerance (PBFT) [20] in our case) should be executed successfully before the addition of the block in the blockchain. The authorised cloud servers act as the miner nodes and take participation in the consensus process.

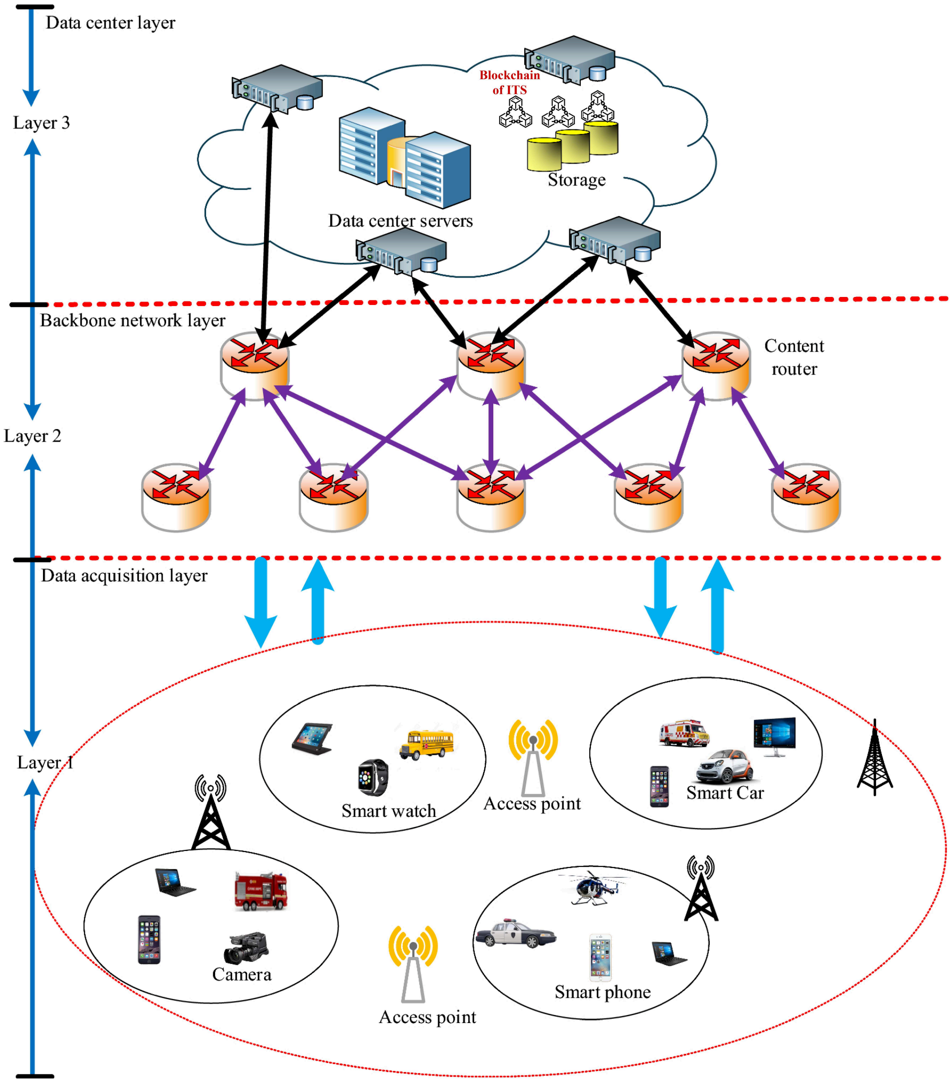


Fig. 1. Architecture (network model) of the proposed BDESF-ITS

B. Threat Model

The widely used "Dolev-Yao (DY) model" [21] has been applied in the designing of the proposed BDESF-ITS. As per the DY model, the communicating entities (i.e., smart devices and smart vehicles) communicate over an open (public, i.e., Internet) channel. Therefore, a potential attacker (online hacker) $\mathcal{A}$ may get a chance to perform some malicious tasks with the exchanged data. The exchanged messages may be revealed, changed, delayed or deleted under the DY model. Furthermore, $\mathcal{A}$ may physically steal some smart devices and extract the sensitive data from the memory of these devices with the application of "sophisticated power analysis attacks" [22]. The extracted information can be then used in other malicious attacks, like "man-in-the-middle (MiTM) attack", "impersonation attack", "credentials guessing and illegal session key computation attacks". In addition, $\mathcal{A}$ can also launch some malware (i.e., virus, backdoor, hardware trojan, ransomware) to further compromise the security of the ITS.

IV. The Proposed Scheme: BDESF-ITS

In this section, we provide the details of the proposed BDESF-ITS. The BDESF-ITS can be explained with the help of following phases.

A. Parameters Selection

In the BDESF-ITS, we store the different information (credentials) of the ITS entities, like vehicle identification number, vehicle speed, vehicle model, traffic light and outside temperature, traffic status and vehicle accidents related data, the form of blocks, which are further added in the blockchain.

B. Computation of Security Parameters and Block Formation

Blockchain is a immutable in nature, which works on the back-end of any application and stores all the information in the form of certain blocks, which contain hash values (i.e., hash of this block, hash of previous block). Blocks in the blockchain are chained together, which use hashing algorithm (i.e., Secure Hash Algorithm (SHA-256) [23]). SHA256 is a hashing algorithm, which takes any arbitrary-length readable data as input and converts it into 256-bit hash value. Only the desired person who has the same input value can get the same hash value from that. Blockchain can be assumed as a never ending stream of blocks, which are connected to one another. The data be to stored in the blockchain should be first converted in the form of some transactions and then the transactions need to be encrypted with the public key of the owner (i.e., a smart vehicle, gateway node, access point), if the transactions are private and confidential. It is very important for the security reasons as the authority (i.e., owner), who has the corresponding private key can only decrypt the encrypted transactions in case confidential transactions are put into the blockchain. Thus, a block contains various fields, like block identification number, owner's information, public key of owner, random nonce, timestamp value, Merkle tree root, transactions in encrypted/plain text forms, hash of the block, hash of the previous block and the "ellliptic curve digital signature" of this block created with the private key of the owner.

C. Execution of Consensus Procedure

In the proposed BDESF-ITS, we do the implementation of the blockchain with the help of the "Practical Byzantine Fault Tolerance (PBFT) algorithm". The PBFT works on the distributed network when more than 50% of the peer nodes in a Peer-to-Peer (P2P) network approve the addition of the blocks into the blockchain. The main objective of the PBFT is to protect the system against failures from both correct and faulty nodes. PBFT works on the creation of primary and secondary nodes. It has four main steps:

1) In the first step, a client sends a request to the primary node to mine the block.
2) When the primary node receives the request from the client, the primary node sends the request to all the secondary nodes or backup nodes. This phase is called *pre-prepare phase*.
3) The backup nodes or secondary nodes send the requests to all the remaining backup nodes and the primary node. This phase is called *prepare phase*.
4) The primary node and all backup nodes then send the messages to all the nodes in the *commit phase*. After that the request is sent successfully back to the client and the block is added into the blockchain if and only if the client receives more replies than the number n_f of the faulty nodes in the P2P network $(2n_f + 1)$.

D. Implementation of Blockchain

For storing data in the blockchain, we have created both the unecncrypted transactions and encrypted transactions in case of confidential transactions, which are stored in some blocks. For validating the transactions, we check whether the sender's address is legal or not, and we have used public key cryptographic operations for that. All valid transactions are added in the transaction pool and each block with certain numbe of transactions is created. To add a block in a blockchain, we have to first mine the block through PBFT consensus algorithm. When it is successfully mined, it is finally added in the blockchain of ITS.

V. Security Analysis of BDESF-ITS

In the proposed BDESF-ITS, different freshly generated timestamp values and random nonces should be used for all the exchanged messages among the entities. The timestamp should be also verified at the receiver's end once the message reaches there. Moreover, the messages should be generated with the help of different secrets of the ITS users and smart devices. Furthermore, the secret key, which is computed between two communicating parties should be computed with the help of "short term secrets (i.e., various timestamp values and random nonce values)" and "long term secrets (i.e., various identities and secret keys)". All these recommendations will provide security against "replay attack", "MiTM attack", "impersonation attack", "unauthorised session key computation attack" and "credential leakage attack". In addition, various attacks are also possible on the blockchain algorithms, especially traditional algorithms i.e., Proof-of-Work (PoW). In the BDESF-ITS, we suggest to use PBFT as it is secure against the potential attacks, which can be performed on the blockchain based system. Therefore, BDESF-ITS is resilient against potential attacks of the domain, and seems to be safe and secure.

VI. Practical Implementation

We have done the implementation of BDESF-ITS through simulation study. The details of the practical implementation are given below.

A. Creation of Primary Node

The creation of primary nodes is done when a client first sends the request to the primary node. The primary node transmits the request to the all the backup nodes, this is why the primary node is also known as the leader node, and also receives request from backup nodes. The snippets of code for the primary node is given in Fig. 2.

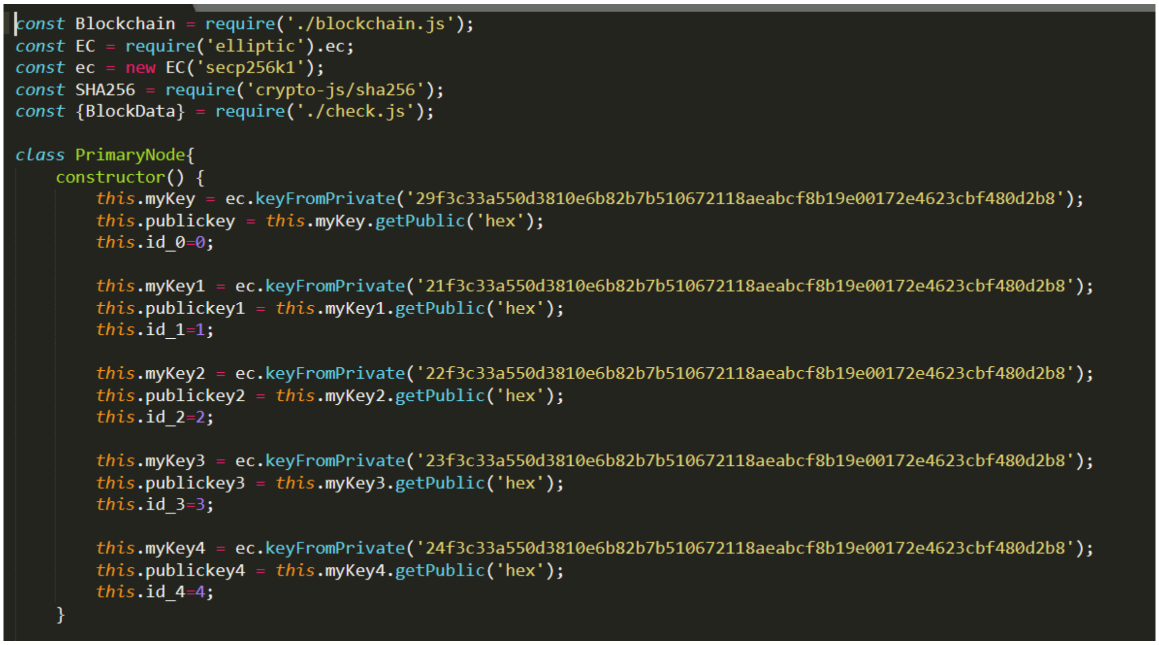
B. Creation of Backup Nodes

The backup nodes are created for taking the valuable requests and need to send them to the leader for their votes to determine which node should be added or not. The snippet of code for the backup nodes is given in Fig. 3.

C. Simulation Environment

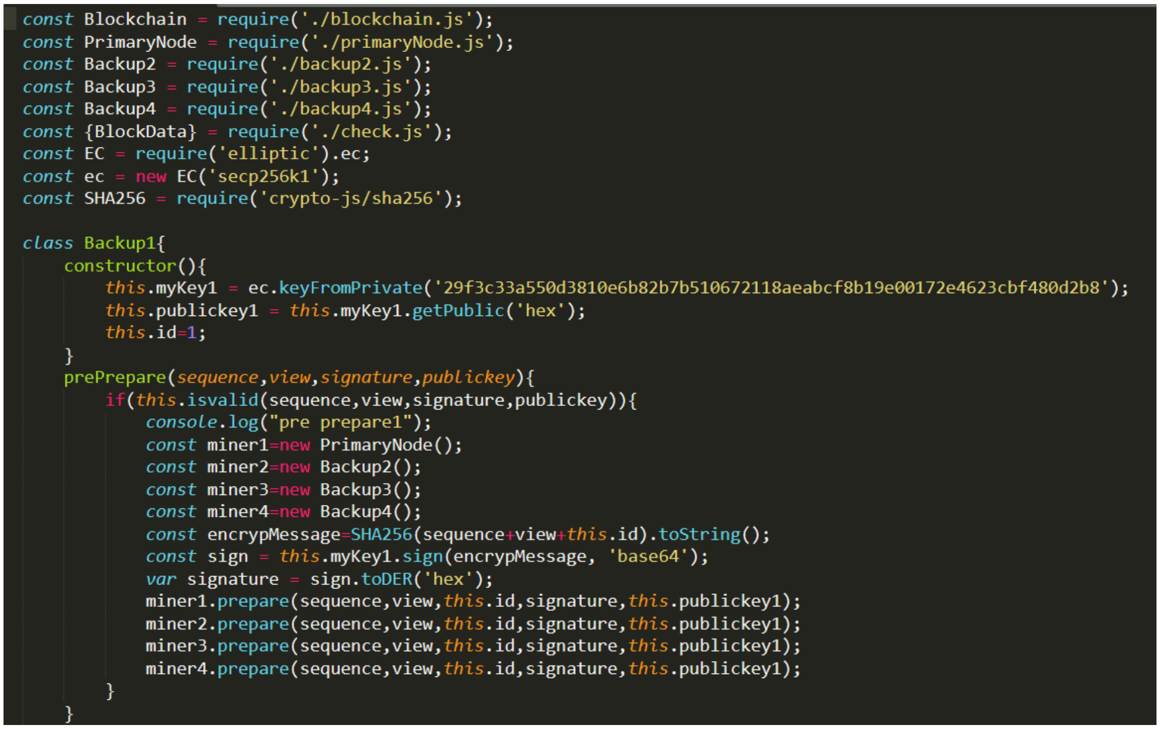
The simulations were performed with the setting: "Intel(R) Core(TM) version i3-5005U CPU with 2.00 GHz and 6.00 GB of size of RAM". The following three scenarios were considered in the simulations:

- **Scenario 1:** In this case, the total number of transactions were 20 and the number of blocks mined were 5. It took a total of 0.02 seconds for the assigned task.



```
const Blockchain = require('./blockchain.js');
const EC = require('elliptic').ec;
const ec = new EC('secp256k1');
const SHA256 = require('crypto-js/sha256');
const {BlockData} = require('./check.js');

class PrimaryNode{
    constructor() {
        this.myKey = ec.keyFromPrivate('29f3c33a550d3810e6b82b7b510672118aeabcf8b19e00172e4623cbf480d2b8');
        this.publickey = this.myKey.getPublic('hex');
        this.id_0=0;

        this.myKey1 = ec.keyFromPrivate('21f3c33a550d3810e6b82b7b510672118aeabcf8b19e00172e4623cbf480d2b8');
        this.publickey1 = this.myKey1.getPublic('hex');
        this.id_1=1;

        this.myKey2 = ec.keyFromPrivate('22f3c33a550d3810e6b82b7b510672118aeabcf8b19e00172e4623cbf480d2b8');
        this.publickey2 = this.myKey2.getPublic('hex');
        this.id_2=2;

        this.myKey3 = ec.keyFromPrivate('23f3c33a550d3810e6b82b7b510672118aeabcf8b19e00172e4623cbf480d2b8');
        this.publickey3 = this.myKey3.getPublic('hex');
        this.id_3=3;

        this.myKey4 = ec.keyFromPrivate('24f3c33a550d3810e6b82b7b510672118aeabcf8b19e00172e4623cbf480d2b8');
        this.publickey4 = this.myKey4.getPublic('hex');
        this.id_4=4;
    }
```

Fig. 2. Snippet of code for the primary node



```
const Blockchain = require('./blockchain.js');
const PrimaryNode = require('./primaryNode.js');
const Backup2 = require('./backup2.js');
const Backup3 = require('./backup3.js');
const Backup4 = require('./backup4.js');
const {BlockData} = require('./check.js');
const EC = require('elliptic').ec;
const ec = new EC('secp256k1');
const SHA256 = require('crypto-js/sha256');

class Backup1{
    constructor(){
        this.myKey1 = ec.keyFromPrivate('29f3c33a550d3810e6b82b7b510672118aeabcf8b19e00172e4623cbf480d2b8');
        this.publickey1 = this.myKey1.getPublic('hex');
        this.id=1;
    }
    prePrepare(sequence,view,signature,publickey){
        if(this.isvalid(sequence,view,signature,publickey)){
            console.log("pre prepare1");
            const miner1=new PrimaryNode();
            const miner2=new Backup2();
            const miner3=new Backup3();
            const miner4=new Backup4();
            const encrypMessage=SHA256(sequence+view+this.id).toString();
            const sign = this.myKey1.sign(encrypMessage, 'base64');
            var signature = sign.toDER('hex');
            miner1.prepare(sequence,view,this.id,signature,this.publickey1);
            miner2.prepare(sequence,view,this.id,signature,this.publickey1);
            miner3.prepare(sequence,view,this.id,signature,this.publickey1);
            miner4.prepare(sequence,view,this.id,signature,this.publickey1);
        }
    }
```

Fig. 3. Snippet of code for the backup nodes

- **Scenario 2:** In this case, the total number of transactions were 50 and the number of blocks mined were 11. A total of 0.05 seconds for the assigned task was needed.
- **Scenario 3:** In this case, the total number of transactions were 100, whereas the number of blocks mined were 21. A total of 0.09 seconds for the assigned task was needed in this scenario.

The obtained results for the considered scenarios are depicted in Fig. 4 and Fig. 5, respectively. We can see that "computational time (seconds)" increases with the increasing number of users as that causes the creation of more number of blocks that are mined and added into the blockchain. Similarly, "transactions per second (TPS)" increases with a increasing number of users and associated number of mined blocks.

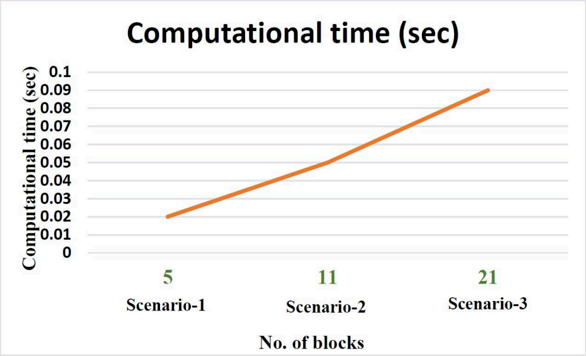


Fig. 4. Obtained results: Computational time (seconds)

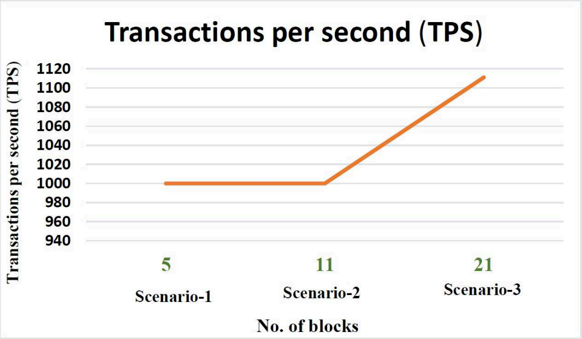


Fig. 5. Obtained results: Transactions per second

VII. Conclusion

ITS can be used in various applications, like smart traffic management, accident controlling and prediction and security and surveillance. The communication of ITS suffers from various security and privacy related issues. To resolve these issues, we presented a blockchain based secure data exchange and storage framework for the ITS. The practical demonstration of the proposed BDESF-ITS was also provided to measure its impact on the performance parameters.

In future, we would like to add more features in the presented framework.

References

[1] L. F. Herrera-Quintero, J. C. Vega-Alfonso, K. B. A. Banse, and E. Carrillo Zambrano, "Smart ITS Sensor for the Transportation Planning Based on IoT Approaches Using Serverless and Microservices Architecture," *IEEE Intelligent Transportation Systems Magazine*, vol. 10, no. 2, pp. 17–27, 2018.

[2] S. Kaffash, A. T. Nguyen, and J. Zhu, "Big data algorithms and applications in intelligent transportation system: A review and bibliometric analysis," *International Journal of Production Economics-Elsevier*, vol. 231, p. 107868, 2021.

[3] Y. Lian, G. Zhang, J. Lee, and H. Huang, "Review on big data applications in safety research of intelligent transportation systems and connected/automated vehicles," *Accident Analysis & Prevention-Elsevier*, vol. 146, p. 105711, 2020.

[4] G. S. Aujla, R. Chaudhary, N. Kumar, A. K. Das, and J. J. P. C. Rodrigues, "SecSVA: Secure Storage, Verification, and Auditing of Big Data in the Cloud Environment," *IEEE Communications Magazine*, vol. 56, no. 1, pp. 78–85, 2018.

[5] J. Srinivas, A. K. Das, M. Wazid, and A. V. Vasilakos, "Designing Secure User Authentication Protocol for Big Data Collection in IoT-Based Intelligent Transportation System," *IEEE Internet of Things Journal*, vol. 8, no. 9, pp. 7727–7744, 2021.

[6] N. Garg, M. Wazid, A. K. Das, D. P. Singh, J. J. P. C. Rodrigues, and Y. Park, "BAKMP-IoMT: Design of Blockchain Enabled Authenticated Key Management Protocol for Internet of Medical Things Deployment," *IEEE Access*, vol. 8, no. 1, pp. 95 956–95 977, 2020.

[7] G. S. Aujla and A. Jindal, "A Decoupled Blockchain Approach for Edge-Envisioned IoT-Based Healthcare Monitoring," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 2, pp. 491–499, 2021.

[8] R. Chaudhary, A. Jindal, G. S. Aujla, S. Aggarwal, N. Kumar, and K.-K. R. Choo, "BEST: Blockchain-based secure energy trading in SDN-enabled intelligent transportation system," *Computers & Security*, vol. 85, pp. 288–299, 2019.

[9] H. Grover, T. Alladi, V. Chamola, D. Singh, and K.-K. R. Choo, "Edge Computing and Deep Learning Enabled Secure Multitier Network for Internet of Vehicles," *IEEE Internet of Things Journal*, vol. 8, no. 19, pp. 14 787–14 796, 2021.

[10] T. Alladi, V. Kohli, V. Chamola, F. R. Yu, and M. Guizani, "Artificial Intelligence (AI)-Empowered Intrusion Detection Architecture for the Internet of Vehicles," *IEEE Wireless Communications*, vol. 28, no. 3, pp. 144–149, 2021.

[11] T.-Y. Wu, Z. Lee, L. Yang, and C.-M. Chen, "A Provably Secure Authentication and Key Exchange Protocol in Vehicular Ad Hoc Networks," *Security and Communication Networks*, vol. 2021, p. 9944460, 2021. [Online]. Available: https://doi.org/10.1155/2021/9944460

[12] D. Mishra, A. K. Das, and S. Mukhopadhyay, "A secure and efficient ECC-based user anonymity-preserving session initiation authentication protocol using smart card," *Peer-to-Peer Networking and Applications*, vol. 9, no. 1, pp. 171–192, Jan 2016.

[13] P. Wang, C.-M. Chen, S. Kumari, M. Shojafar, R. Tafazolli, and Y.-N. Liu, "HDMA: Hybrid D2D Message Authentication Scheme for 5G-Enabled VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 8, pp. 5071–5080, 2021.

[14] A. K. Das, "A random key establishment scheme for multi-phase deployment in large-scale distributed sensor networks," *International Journal of Information Security*, vol. 11, no. 3, pp. 189–211, 2012.

[15] A. K. Das, M. Wazid, A. R. Yannam, J. J. P. C. Rodrigues, and Y. Park, "Provably secure ecc-based device access control and key agreement protocol for iot environment," *IEEE Access*, vol. 7, pp. 55 382–55 397, 2019.

[16] M. Wazid, B. Bera, A. K. Das, S. P. Mohanty, and M. Jo, "Fortifying Smart Transportation Security through Public Blockchain," 2022, doi: 10.1109/JIOT.2022.3150842.

[17] S. Son, J. Lee, Y. Park, Y. Park, and A. K. Das, "Design of Blockchain-Based Lightweight V2I Handover Authentication Protocol for VANET," *IEEE Transactions on Network Science and Engineering*, 2022, doi: 10.1109/TNSE.2022.3142287.

[18] D. Chattaraj, B. Bera, A. K. Das, S. Saha, P. Lorenz, and Y. Park, "Block-CLAP: Blockchain-Assisted Certificateless Key Agreement Protocol for Internet of Vehicles in Smart Transportation," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 8, pp. 8092–8107, 2021.

[19] A. Vangala, B. Bera, S. Saha, A. K. Das, N. Kumar, and Y. Park, "Blockchain-Enabled Certificate-Based Authentication for Vehicle Accident Detection and Notification in Intelligent Transportation Systems," *IEEE Sensors Journal*, vol. 21, no. 14, pp. 15 824–15 838, 2021.

[20] M. Castro and B. Liskov, "Practical Byzantine fault tolerance and proactive recovery," *ACM Transactions on Computer Systems*, vol. 20, no. 4, pp. 398–461, 2002.

[21] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[22] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks," *IEEE Transactions on Computers*, vol. 51, no. 5, pp. 541–552, 2002.

[23] W. E. May, "Secure Hash Standard," 2015, FIPS PUB 180-1, National Institute of Standards and Technology (NIST), U.S. Department of Commerce, April 1995. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf. Accessed on May 2021.