Private Blockchain-Envisioned Security Framework for AI-Enabled IoT-Based Drone-Aided Healthcare Services

by

Mohammad Wazid, Basudeb Bera, Ankush Mitra, Ashok Kumar Das, Rashid Ali

in

DroneCom '20: Proceedings of the 2nd ACM MobiCom Workshop on Drone Assisted Wireless Communications for 5G and Beyond Private blockchain-envisioned security framework for AI-
: 1
-6

Report No: IIIT/TR/2020/-1

Centre for Security, Theory and Algorithms
International Institute of Information Technology
Hyderabad - 500 032, INDIA
September 2020

Private Blockchain-Envisioned Security Framework for AI-Enabled IoT-Based Drone-Aided Healthcare Services

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

Basudeb Bera
Center for Security, Theory and Algorithmic Research,
International Institute of Information Technology, Hyderabad 500 032, India
basudeb.bera@research.iiit.ac.in

Ankush Mitra
Center for Security, Theory and Algorithmic Research,
International Institute of Information Technology, Hyderabad 500 032, India
ankush.mitra@students.iiit.ac.in

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

Rashid Ali
School of Intelligent Mechatronics Engineering, Sejong University,
Seoul, Republic of Korea
rashidali@sejong.ac.kr

ABSTRACT

Internet of Drones (IoD) architecture is designed to support a coordinated access for the airspace using the unmanned aerial vehicles (UAVs) known as drones. Recently, IoD communication environment is extremely useful for various applications in our daily activities. Artificial intelligence (AI)-enabled Internet of Things (IoT)-based drone-aided healthcare service is a specialized environment which can be used for different types of tasks, for instance, blood and urine samples collections, medicine delivery and for the delivery of other medical needs including the current pandemic of COVID-19. Due to wireless nature of communication among the deployed drones and their ground station server, several attacks (for example, replay, man-in-the-middle, impersonation and privileged-insider attacks) can be easily mounted by malicious attackers. To protect such attacks, the deployment of effective authentication, access control and key management schemes are extremely important in the IoD environment. Furthermore, combining the blockchain mechanism with deployed authentication make it more robust against various types of attacks. To mitigate such issues, we propose a private-blockchain based framework for secure communication in an IoT-enabled drone-aided healthcare environment. The blockchain-based simulation of the proposed framework has been carried out to measure its impact on various performance parameters.

CCS CONCEPTS

• **Networks** → **Security protocols**; • **Security and privacy** → **Authentication**.

DroneCom'20, September 25, 2020, London, United Kingdom

ACM ISBN 978-1-4503-8105-5/20/09…$15.00
https://doi.org/10.1145/3414045.3415941

KEYWORDS

Internet of Drones (IoD), healthcare, security, privacy, authentication, blockchain

ACM Reference Format:
Mohammad Wazid, Basudeb Bera, Ankush Mitra, Ashok Kumar Das, and Rashid Ali. 2020. Private Blockchain-Envisioned Security Framework for AI-Enabled IoT-Based Drone-Aided Healthcare Services. In *Workshop on Drone Assisted Wireless Communications for 5G and Beyond (DroneCom'20), September 25, 2020, London, United Kingdom.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3414045.3415941

1 INTRODUCTION

Internet of Drones (IoD) is a technology which drives its concept from the Internet of Things (IoT). IoD helps in providing coordinated access to a controlled airspace for the unmanned aerial vehicles (UAVs), also known as drones. With equipped smart sensors, actuators and other ubiquitous wireless connectivity, drones have now various amazing applications to facilitate our day-to-day life activities [14], [15]. Several applications of IoD include "package delivery", "traffic and wild life surveillance", "inspection of infrastructure", "rescue operations and inspection of agriculture fields", "battlefield scenario" and "cinematography" [3], [4], [13], [25].

Health informative (also known as healthcare informatics) is a kind of information engineering that is used healthcare domain for management and effective use of the patients' healthcare information (for example, a doctor can provide remote consultation to the patients on the basis of his/her medical records). In addition, it may not be essential for the patients to visit the doctor physically due to costs involved in visiting the hospitals and other recent outbreaks such as COVID-19. The health related records (blood test reports, medical history and family diseases history) can be then maintained over the healthcare server [24], [9], [27].

The drones in healthcare or drones-aided healthcare services is an emerging application involved in IoD environment. Consider the following recent scenario. Due to the pandemic of COVID-19, many countries have followed lock-down strategy in which they have partitioned the areas of a city/town into several zones: 1) "containment zone", 2) "red zone", 3) "orange zone" and 4) "green

zone". Among all these defined zones, the containment zone are particularly problematic because incoming and outgoing entries of the people containing in that area are restricted. Such a restriction is necessary to prevent the spreading of COVID-19 infections. It is also a kind of epicenter which has most of the positive cases of infections. The people who suffer from other severe diseases (i.e., cancer, cardiac, HIV and kidney) can not go outside or have to take permissions from the concerned authority to go outside of the containment zone. For such situations, the drones-aided healthcare services can be very effective and helpful. Using the drones-aided healthcare services, the tasks such as "blood and urine sample collection", "medicines delivery" and other medical equipment can be delivered to the patients in those areas. Apart from these services, the drone-aided healthcare services are also very useful for other scenarios such as rural areas, tribe areas, and curfew imposed areas. However, the communication in an IoT-enabled drone-aided healthcare communication environment may face several "security and privacy issues" as such an environment may be vulnerable to different attacks. Some potential attacks may be launched by an adversary include "replay", "man-in-the-middle attack (MiTM)", "impersonation attack", "sensitive information leakage attack", "unauthorised hijacking and controlling of drones", and "malware attacks on the system of drone" and also "denial-of-service (DoS) attack" [25], [3], [22]. In order to secure an IoD environment, authentication, access control and key management are the main security services. Moreover, the use of blockchain mechanism makes it more robust against various types of attacks including proving "immutability", "transparency" and "decentralization". In a blockchain, the distributed ledger technology helps in recording the provenance of digital assets. The mechanism of blockchain involves block creation, census process (mining of created blocks) and block addition in the blockchain. The information communicated among the drones and their ground station server in IoT-enabled drone-aided healthcare communication environment are stored in the distributed ledger of blockchain. Since the health-related information is strictly private and confidential, we consider the private blockchain in ths paper.

The main contributions towards this work are summarized below.

- A new private-blockchain based security framework for the secure communication in IoT-enabled drone-aided healthcare communication environment has been proposed.
- We present two important system related models (network model and attack model) that are mandatory to design the proposed security framework.
- The proposed framework is resilience against possible potential attacks needed in an IoD environment.
- Finally, a practical demonstration of the proposed framework using blockchain simulation shows its impact on performance parameters.

In the next section, a brief literature review of various existing techniques related to a healthcare domain is provided. The details of system models required to design the blockchain based framework for secure communication in IoT-enabled drone-aided healthcare environment is provided in Section 3. The detailed description of the proposed framework is explained in Section 4. A brief security analysis is also provided in Section 5. The blockchain-based practical demonstration of the proposed framework is given in Section 6. Finally, the paper is concluded in Section 7.

2 RELATED WORK

Kumar *et al.* [18] presented a multiverse optimizer (MVO) based 2-D path planning method to achieve quality of service (QoS) in UAV environment. Garg *et al.* [12] presented a data-driven transportation optimization scheme. In their scheme, a cyber-threat detection in smart vehicles was carried out via a data structure, called the "probabilistic data structure (PDS)". A triple bloom filter based scheduling scheme for load balancing was also applied to receive real-time data from various vehicles.

Garg *et al.* [11] also designed a tree-based attack-defense method for the security analysis of UAV environment. They implemented an attack-defense tree in order to predict each move of the defender as per an attacker's plan. A case study of denial-of-service (DoS) attack was also conducted by the authors to evaluate efficiency of their method. Kim *et al.* [17] addressed the drone-aided delivery and pickup planning of medication, and test kits for patients with chronic diseases who are required to visit clinics for their routine health examinations and for the refilling of medicine in the rural areas. Ullah *et al.* [23] investigated the benefits of uses of 5G in various domains by considering several use cases. Arteaga *et al.* [2] presented an exploitation of the "Global Positioning System (GPS)" vulnerability in commercial drones. Their identified vulnerability could help a malicious attacker to control autonomy and carry out other illegal tasks.

Chamola *et al.* [7] explored the uses of technologies (for example, Internet of Things (IoT), Unmanned Aerial Vehicles (UAVs), blockchain, Artificial Intelligence (AI) and 5G) to reduce the impact of COVID-19 outbreak. Wazid *et al.* [25] and Bera *et al.* [3] proposed blockchain based authentication and access control schemes for the IoT enabled drones communication to make secure communication among the drones and ground station server. Alladi *et al.* [1] discussed different applications of blockchain for drones communication.

Sharma *et al.* [21] provided a vulnerability assessment for drones-enabled industrial IoT (IIoT). They evaluated the drone's behavior for potential vulnerabilities by using security policies. Lin *et al.* [19] also presented a trend of IoD in both industry and research. Recently, Wazid *et al.* [26] also presented a blockchain based framework for the authentication and secure data exchange in an Internet of Intelligent Things (IoIT) environment by presenting a generalized authentication, key establishment and secure data exchange, and blockchain formation mechanism.

3 SYSTEM MODELS

In the following, we discuss the following models that are utilized in the proposed security framework design.

3.1 Network model

The network model of the proposed framework provided in Figure 1 depicts the connection and communication among different network entities, such as patients, relative and friends of patients,

drones, doctors and other healthcare staffs in the hospitals, pharmacy staff at the medicine refilling center, etc. There is a ground station server (*GSS*) acts with a fully trusted control room (*CR*) controls all the activities happen in such an environment. Drones are responsible for the samples collection (i.e., blood and urine), and also for the delivery of medicine and other medical needs. Each drone communicates with its neighbor other drones in its own flying zone as well with the *GSS*. The *GSS* executes the commands for the drones and then the drones act accordingly. Drones also send the data related to their activities to the *GSS*. Thus, the *GSS* records the received data in the form of transactions and then makes them available to the Peer-to-Peer (P2P) cloud servers networks. Cloud servers are resource rich nodes having high computation, communication and storage capabilities, act like the miner nodes. The healthcare data is very sensitive therefore, its not a good strategy to put this over the public blockchain. Hence, we consider a private blockchain model in the proposed framework. The P2P cloud servers network is also capable to execute big data analysis on the received healthcare data using the Artificial Intelligence (AI)/Machine Learning (ML) techniques. The big data analytic process is needed to draw some useful predictions from the received and analysed data (for example, prediction related to the medical requirements of the patients inside a COVID-19 containment zone) using the authenticated data available inside the blocks in the private blockchain.

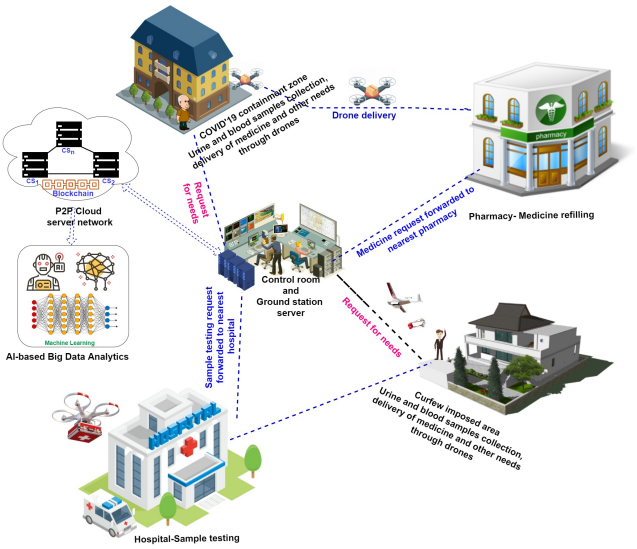

Figure 1: Network model (Adapted from [17]).

3.2 Threat model

The Dolev-Yao (DY) threat model [10] is followed along with the current *de facto* Canetti and Krawczyk (CK) adversary model [5]. The DY model permits an adversary $\mathcal{A}$ not only to intercept the communicated messages between entities in the IoD environment, but also can modify, delete or insert fake contents in between the communication. Under the CK-adversary model, beyond $\mathcal{A}$'s capabilities of the DY threat model, $\mathcal{A}$ can also compromise session states, session keys and secret keys if a session is hijacked. Hence, it is a desirable requirement that the construction of session keys must be based on both short term (temporal) secrets and long term secrets so that compromised of a session key between two entities does not affect in compromising the session keys established in other sessions between those entities in the IoD environment. Some drones can be physically captured by $\mathcal{A}$ as they can not monitored in 24×7. $\mathcal{A}$ can then easily extract the sensitive information from their memory using the power analysis attacks [20]. This malicious act of $\mathcal{A}$ may lead to other attacks, such as impersonate attacks. The control room (*CR*) and *GSS* are assumed to be the fully trusted entities, whereas cloud servers are semi-trusted entities in the network.

4 THE PROPOSED FRAMEWORK

The proposed blockchain-envisioned security framework for AI-enabled IoT-based drone-aided healthcare services is explained below. The proposed framework contains the following phases. Various notations used in the proposed framework are provided in Table 1. In addition, to protect replay attack, it is also assumed that all the entities in the IoD environment are synchronized with their clocks [4].

Table 1: Notations and their meanings

Symbol	Meaning
$\mathcal{A}$	An adversary
DR_i	i^{th} drone
GSS, CR	Ground station server and control room
CS_k	k^{th} cloud server in blockchain center
U_l	l^{th} user
SK_{p_i,p_j}	Established session key between entities p_i and p_j
(KU_X, KR_X)	Elliptic curve cryptography (ECC) based public and private keys pair of an entity p_i
Cmd_{GSS,DR_i}	Command issued by *GSS* to a drone DR_i
$ECDSA.Sig_{KR_{GSS}}(Cmd_{GSS,DR_i})$	ECDSA signature of *GSS* on command Cmd_{GSS,DR_i}
$Data_{KR_i,GSS}$	Data sent by DR_i to *GSS*
$ECDSA.Sig_{KR_{DR_i}}(Data_{DR_i,GSS})$	ECDSA signature of DR_i on data $Data_{DR_i,GSS}$
$Req_{U_l,GSS}$	Request sent by U_l to *GSS*
TS_x	Current timestamp of an entity X
BC	Blockchain center
BLK_x	New block to be added in the blockchain

4.1 Pre deployment and registration phase

In this phase, the selection of various cryptographic primitives including "one-way cryptographic hash function", a non-singular elliptic curve over a finite field of large prime order, ECC encryption/decryption and elliptic curve digital signature algorithm (ECDSA) [16]. After this process, the registration of various entities, such as drones (DR_i), ground station server (*GSS*), cloud servers (CS_k) and users (U_l) are performed the trusted control room (*CR*). After the completion of registration process, the essential credentials are stored in the memory of the devices as well in the smart phones (mobile devices) of registered users (i.e., doctor, patients and their relatives, other healthcare staff, etc.). In addition, all the entities X will generate their own ECC-based private and public keys pairs (KU_X, KR_X). All these entities are then deployed in different areas, such as COVID-19 containment zones, curfew imposed areas, rural and tribe areas, hospitals and pharmacies.

4.2 Authentication, key establishment, access control and data collection phase

This phase can be executed as follows.

Step 1. To avail the services of the network, different users can login into the system with the help of their mobile devices and preloaded secret credentials in their mobile devices. If the users are genuine, they will be able to login into the system and at the same through user authentication mechanism they can establish session keys with the *GSS*. We can apply a similar user authentication and key establishment process between a registered user U_l and the *GSS* as done in the existing user authentication scheme between a user and a drone [25]. In this way, assume that the session key $SK_{U_l,GSS}$ is established between U_l and the *GSS* for secure communication.

Step 2. A registered user U_l can now send a request $Req_{U_l,GSS}$ for healthcare services to the *GSS* securely to the *GSS* using the established session key $SK_{U_l,GSS}$. In this way, U_l can send the encrypted request $E_{Req_{U_l,GSS}}$ to the *GSS* and the *GSS* can also decrypt it using the same session key $SK_{U_l,GSS}$ to get $Req_{U_l,GSS}$ which forms a transaction $TX_{U_l,GSS}$ for the user U_l for adding in the blockchain later.

Step 3. In the access control process, each drone (DR_i) needs to mutually authenticate with the *GSS*. After successful mutual authentication, they will establish a secret key $SK_{DR_i,GSS}$ among them for secure communication. It is worth noticing that the *GSS* will communicate with the cloud servers CS_k in the blockchain using the public key KU_{CS_k}. We apply a recently proposed existing robust access control mechanism [3] for establishing $SK_{DR_i,GSS}$ between DR_i and its associated *GSS*.

Step 4. Consider a drone (DR_i) in its assigned flying zone is responsible for specific tasks, such as blood and urine samples collection and delivery of medicine, and other medical needs are assigned to that drone from the *CR/GSS*. Upon receiving an authenticate request $Req_{U_l,GSS}$ securely from a legal user U_l to the *GSS* (as explained in Step 2), the *GSS* will issue a command by generating current timestamp TS_1 and sending the encrypted command message, say $MSG_1 = \{E_{SK_{DR_i,GSS}}[Cmd_{GSS,DR_i}, ECDSA.Sig_{KR_{GSS}}(Cmd_{GSS,DR_i}, TS_1)], TS_1\}$ to the concerned DR_i via public channel, where $ECDSA.Sig_{KR_{GSS}}(\cdot)$ represents the ECDSA signature using the *GSS*'s private key KR_{GSS}. After receiving the message from DR_i, the *GSS* checks the validity of timestamp TS_1 by $|TS_1 - TS_1^*| \leq \Delta T$, where the maximum transmission delay is represented by ΔT and TS_1^* is reception time of the message MSG_1, and decrypts the message using the same session key $SK_{DR_i,GSS}$ to have Cmd_{GSS,DR_i} and its signature. If the signature verification using the public key KU_{GSS} of the *GSS* is valid, the command is treated as authentic. DR_i then reads the information (available in Cmd_{GSS,DR_i}) requested by *GSS* and prepares an encrypted response data message as $MSG_2 = \{E_{SK_{DR_i,GSS}}[Data_{DR_i,GSS}, ECDSA.Sig_{KR_{DR_i}}(Data_{DR_i,GSS}, TS_2)], TS_2\}$. DR_i then sends the response message MSG_2 to *GSS* via public channel.

Step 5. *GSS* receives the message MSG_2, checks the validity of received timestamp TS_2, and then decrypts it using $SK_{DR_i,GSS}$. After that *GSS* verifies the decrypted signature using the public key KU_{DR_i} of DR_i. If it verifies successfully, the *GSS* reads the information $Data_{DR_i,GSS}$. After that the *GSS* prepares transactions $TX_{DR_i,GSS}$ and TX_{GSS,DR_i} for the command and response messages, respectively. In this way, the *GSS* will have a number of transactions, say TX_i, where $i = 1, 2 \cdots t_n$. Finally, the *GSS* sends encrypted transactions $\{E_{KU_{GSS}}[TX_i]|i = 1, 2, \cdots, t_n\}$ securely to a cloud server, say CS_k using the public key KU_{CS_k} of the CS_k.

Block Header	
Block Sequence number (version)	SNB_{BLK_x}
Last block hash	$LBH_{BLK_{x-1}}$
Merkle tree root	MTR_{BLK_x}
Timestamp	TS_{BLK_x}
Public key of owner (proposer)	KU_{CS_k}
Block Payload (Encrypted Transactions)	
List of t_n encrypted transactions #i (TX_i)	$\{E_{KU_{GSS}}(TX_i)\|i = 1, 2, \cdots, t_n\}$
Current block hash	$CBHash_{BLK_x}$
Signature on $CBHash$	ECDSA signature on $CBHash_{BLK_x}$ as $Sig_{BLK_x} = ECDSA.Sig_{KR_{CS_k}}(CBHash_{BLK_x})$

Figure 2: Structure of a block BLK_x

4.3 Blockchain implementation phase

In this phase, a cloud server CS_k in the P2P cloud servers network will collect securely a pool of transactions. The blocks creation, verification and addition into the blockchain are done using the following steps:

Step 1. CS_k will then create a block, say BLK_x in order to add into blockchain. The structure of BLK_x presented in Figure 2 contains the following: 1) a block header having the block sequence number/version (SNB_{BLK_x}), previous/last block hash ($LBH_{BLK_{x-1}}$), Merkle tree root (MTR_{BLK_x}) on all t_n encrypted transactions $\{E_{KU_{GSS}}[TX_i]|i = 1, 2, \cdots, t_n\}$, block creation timestamp (TS_{BLK_x}); 2) block payload having t_n encrypted transactions; 3) current block hash $CBHash_{BLK_x}$; and 4) signature on block $Sig_{BLK_x} = ECDSA.Sig_{KR_{CS_k}}(CBHash_{BLK_x})$.

Step 2. CK_k then adds the created block using the consensus algorithm via voting request with the steps explained in Algorithm 1. It is worth noticing that we have applied the "Practical Byzantine Fault Tolerance (PBFT) consensus algorithm" [6].

4.4 AI-enabled secure Big data anlytics phase

We now discuss how an AI-enabled secure Big data analytics can be done using the formed blockchain in the previous section.

We consider a data poisoning attack, which becomes a significant threat in AI/ML. This is mainly due to the fact that the fake data may be injected by malicious users which may lead to delude the "training data sets for puzzling AI/ML algorithms" [8]. This results in incorrect predication on data sets. Such an attack is fatal because it may have a crucial factor for businesses as well as organizations from both the "financial terms" and "damaging their reputations" points of view.

With the help of the proposed blockchain-based security framework, the transactional data (e.g., Cmd_{GSS,DR_i}, $Data_{KR_i,GSS}$ and $Req_{U_l,GSS}$) stored in private blockchain are authentic as well as genuine too. It helps in avoiding data poisoning attacks by a malicious user being an adversary. As a result, it leads to run the AI/ML

Algorithm 1 Consensus for block verification and addition

Input: A pool of transactions and N, where N is the nodes in the P2P network with $N = 3F + 1$ and F is the number of faulty nodes
Output: Commitment and addition of a block BLK_x into BC after its successful validation

1: Assume a proposer (called a leader), say CS_l is elected in a round-robin fashion
2: The proposer CS_l collects transactions securely from the transaction pool and creates a block BLK_x
3: CS_l broadcasts the block BLK_x to each follower cloud server node CS_j in the network
4: The validators CS_j receive BLK_x from CS_l and validates it with transaction pool
5: **for** each validator node **do**
6: Verify timestamp, Merkle tree root, current block hash, and signature on BLK_x
7: If all checks are verified successfully, broadcast the validated status
8: **end for**
9: Let Val denotes the valid responses. Initialize $Val \leftarrow 0$
10: **for** each commit message in the global commit message pool **do**
11: CS_l calculates Val values
12: **if** commit message status is valid **then**
13: Set $Val = Val + 1$
14: **end if**
15: **end for**
16: **if** $(Val > 2F + 1)$ **then**
17: Broadcast block committed message to other followers
18: Add block BLK_x into blockchain BC
19: **end if**

algorithms as per their expectations to make the correct predictions for the Big data analytics purpose. This is possible because the blocks are verified in the blockchain before taking into account for Big data analytics on the decrypted transactions.

5 SECURITY ANALYSIS

In the proposed framework, the following attacks are resisted against an adversary who is either a passive or an active, in nature.

1) *Replay attack.* The use of current timestamps in the messages $MSG_1 = \{E_{SK_{DR_i,GSS}}[Cmd_{GSS,DR_i}, ECDSA.Sig_{KR_{GSS}}(Cmd_{GSS,DR_i}, TS_1)], TS_1\}$ and $MSG_2 = \{E_{SK_{DR_i,GSS}}[Data_{DR_i,GSS}, ECDSA.Sig_{KR_{DR_i}}(Data_{DR_i,GSS}, TS_2)], TS_2\}$ ensures that the recipient will validate the timestamp before further processing the messages. Also, the timestamps are included in the message signature and the signature is encrypted. Hence, the proposed framework is secured against replay attack.

2) *Man-in-the-middle(MiTM) attack.* Even if an adversary can make fake message content (request, command and response), he/she can not send it to the appropriate receiver (GSS, DR_i, U_l) because the secret (session) keys are unknown. Also, the fake signatures can not be created by the adversary for the messages MSG_1 and SG_2 because the private keys of DR_i and GSS are unknown. Thus, MiTM attack is resisted in the proposed framework.

3) *Impersonation attacks.* Such attacks can not be successfully launched by an adversary because he/she does not possess the private keys of DR_i and GSS. Hence, even if the adversary can generate timestamps and fake message contents (request, command and response) on behalf of U_l, DR_i and GSS, he/she can not succeed for user/drone/GSSS impersonate attacks.

4) *Other potential attacks.* The cloud servers CS_k and the GSS may store the secret information in the secured region in their databases in order to thwart against hacking attempts. The proposed mechanism of blockchain makes it more secure and tamper proof against the Denial-of-Service (DoS), data modification and leakage attacks.

5) *Block verification.* In the proposed framework, three-level block verifications take place. First, the Merkle tree root is constructed using the available t_n encrypted transactions $\{E_{KU_{GSS}}[TX_i]|i = 1, 2, \cdots, t_n\}$ and then checked against the stored MTR_{BLK_x} on the verified block BLK_x. Second, the current hash block $CBHash_{BLK_x}$ is verified. Third, the available signature Sig_{BLK_x} is validated using the public key KR_{CS_k} of the owner CS_k. Thus, if all the verifications pass successfully, the block BLK_x is then only treated as a genuine block for AI-enabled secure Big data analytics purpose.

6 PRACTICAL DEMONSTRATION

In this section, we provide the details of practical demonstration of our proposed framework to measure its impact on the performance parameters. The simulation was conducted on a platform having "Ubuntu 20.04 64-bit OS with Intel(R) Celeron(R) CPU 3855U @ 1.60GHz". The size of the random-access memory (RAM) size was 4 GB. The considered programming platform was VS CODE 2019 with Node.js language. We assumed the block version, proposer ECC-based public key, timestamp (epoch time), Merkle tree root, current block hash (using SHA-256 hashing algorithm), and ECDSA signature are of sizes 32, 320, 42, 256, 256 and 320 bits, respectively. In addition, an encrypted transaction using the ECC encryption produces two elliptic curve points, and as a result, it requires (320 + 320) = 640 bits.

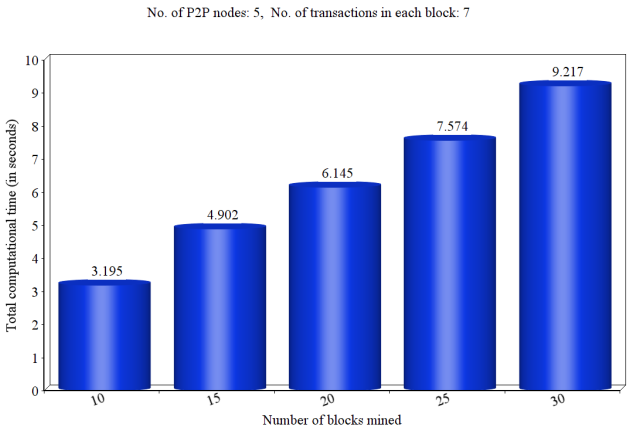

Figure 3: Simulation results for Case 1.

The following cases were considered during the simulations.

Case 1. In this case, we considered that the number of peer nodes is 5. In each block, there were 7 transactions. The simulation results are shown on the varied number of blocks mined into the blockchain versus the total computational time (in seconds) in Figure 3.

Case 2. Under this case, we also assumed that the peer nodes is 5 and a blockchain contained 20 blocks. The simulation results shown in Figure 4 depend on the number of transactions varied per block versus the total computational time (in seconds).

It was noticed that the computational time varied linearly in both the cases. For instance, the implemented framework took 9.217 seconds for adding 30 blocks in the blockchain, and it took 7.093 seconds for executing 20 transactions in a block.

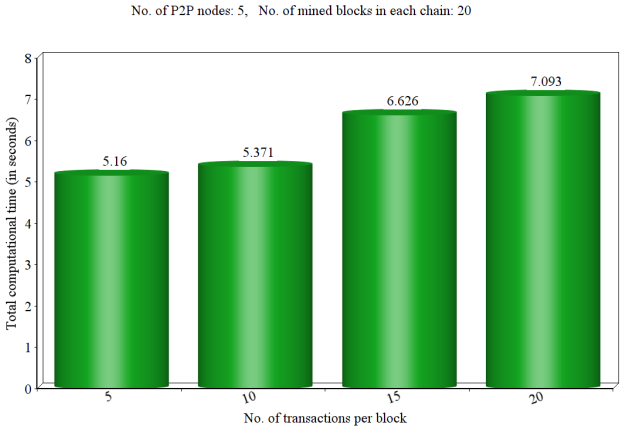

Figure 4: Simulation results for Case 2.

7 CONCLUSION

This paper provides a security framework for an AI-enabled IoT-based drone-aided healthcare communication environment. A private blockchain has been considered in the proposed framework due to highly sensitive and confidential healthcare data. The created blocks by the cloud servers in the P2P network are mined, verified and then added based on the PBFT consensus algorithm with the voting mechanism. The conducted security analysis of the proposed framework proves its resilience against various potential attacks. Moreover, the proposed framework is also implemented practically using the blockchain simulation.

ACKNOWLEDGMENTS

This work was supported by the Ripple Centre of Excellence Scheme, CoE in Blockchain (Sanction No. IIIT/R&D Office/Internal Projects/001/2019), IIIT Hyderabad, India.

REFERENCES

[1] T. Alladi, V. Chamola, N. Sahu, and M. Guizani. 2020. Applications of blockchain in unmanned aerial vehicles: A review. *Vehicular Communications* 23 (2020), 100249.

[2] S. P. Arteaga, L. A. M. Hernandez, G. S. Perez, A. L. S. Orozco, and L. J. G. Villalba. 2019. Analysis of the GPS Spoofing Vulnerability in the Drone 3DR Solo. *IEEE Access* 7 (2019), 51782–51789.

[3] B. Bera, D. Chattaraj, and A. K. Das. 2020. Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment. *Computer Communications* 153 (2020), 229 – 249.

[4] B. Bera, S. Saha, A. K. Das, N. Kumar, P. Lorenz, and M. Alazab. 2020. Blockchain-Envisioned Secure Data Delivery and Collection Scheme for 5G-Based IoT-Enabled Internet of Drones Environment. *IEEE Transactions on Vehicular Technology* (2020). DOI: 10.1109/TVT.2020.3000576.

[5] R. Canetti and H. Krawczyk. 2002. Universally Composable Notions of Key Exchange and Secure Channels. In *Advances in Cryptology — EUROCRYPT*, Lars R. Knudsen (Ed.). Springer Berlin Heidelberg, Amsterdam, The Netherlands, 337–351.

[6] M. Castro and B. Liskov. 2002. Practical Byzantine fault tolerance and proactive recovery. *ACM Transactions on Computer Systems* 20, 4 (2002), 398–461.

[7] V. Chamola, V. Hassija, V. Gupta, and M. Guizani. 2020. A Comprehensive Review of the COVID-19 Pandemic and the Role of IoT, Drones, AI, Blockchain, and 5G in Managing its Impact. *IEEE Access* 8 (2020), 90225–90265.

[8] X. Chen, C. Liu, B. Li, K. Lu, and D. Song. 2017. Targeted Backdoor Attacks on Deep Learning Systems Using Data Poisoning. *CoRR* abs/1712.05526 (2017). http://arxiv.org/abs/1712.05526

[9] M. Wazid A. K. Das, S. Kumari, X. Li, and F. Wu. 2016. Design of an efficient and provably secure anonymity preserving three-factor user authentication and key agreement scheme for TMIS. *Security and Communication Networks* 9, 13 (2016), 1983–2001.

[10] D. Dolev and A. Yao. 1983. On the security of public key protocols. *IEEE Transactions on Information Theory* 29, 2 (1983), 198–208.

[11] S. Garg, G. S. Aujla, N. Kumar, and S. Batra. 2019. Tree-Based Attack–Defense Model for Risk Assessment in Multi-UAV Networks. *IEEE Consumer Electronics Magazine* 8, 6 (2019), 35–41.

[12] S. Garg, A. Singh, S. Batra, N. Kumar, and L. T. Yang. 2018. UAV-Empowered Edge Computing Environment for Cyber-Threat Detection in Smart Vehicles. *IEEE Network* 32, 3 (2018), 42–51.

[13] M. Gharibi, R. Boutaba, and S. L. Waslander. 2016. Internet of Drones. *IEEE Access* 4 (2016), 1148–1162.

[14] V. Hassija, V. Chamola, D. N. G. Krishna, and M. Guizani. 2020. A Distributed Framework for Energy Trading Between UAVs and Charging Stations for Critical Applications. *IEEE Transactions on Vehicular Technology* 69, 5 (2020), 5391–5402.

[15] V. Hassija, V. Saxena, and V. Chamola. 2020. Scheduling drone charging for multi-drone network based on consensus time-stamp and game theory. *Computer Communications* 149 (2020), 51–61.

[16] D. Johnson, A. Menezes, and S. Vanstone. 2001. The Elliptic Curve Digital Signature Algorithm (ECDSA). *International Journal of Information Security* 1, 1 (2001), 36–63.

[17] S. J. Kim, G. J. Lim, J. Cho, and M. J. Cote. 2017. Drone-Aided Healthcare Services for Patients with Chronic Diseases in Rural Areas. *Journal of Intelligent & Robotic Systems* 88 (2017), 163–180.

[18] P. Kumar, S. Garg, A. Singh, S. Batra, N. Kumar, and I. You. 2018. MVO-Based 2-D Path Planning Scheme for Providing Quality of Service in UAV Environment. *IEEE Internet of Things Journal* 5, 3 (2018), 1698–1707.

[19] C. Lin, D. He, N. Kumar, K. R. Choo, A. Vinel, and X. Huang. 2018. Security and Privacy for the Internet of Drones: Challenges and Solutions. *IEEE Communications Magazine* 56, 1 (2018), 64–69.

[20] T. S. Messerges, E. A. Dabbish, and R. H. Sloan. 2002. Examining smart-card security under the threat of power analysis attacks. *IEEE Trans. Comput.* 51, 5 (2002), 541–552.

[21] V. Sharma, G. Choudhary, Y. Ko, and I. You. 2018. Behavior and Vulnerability Assessment of Drones-Enabled Industrial Internet of Things (IIoT). *IEEE Access* 6 (2018), 43368–43383.

[22] J. Srinivas, A. K. Das, N. Kumar, and J. J. P. C. Rodrigues. 2019. TCALAS: Temporal Credential-Based Anonymous Lightweight Authentication Scheme for Internet of Drones Environment. *IEEE Transactions on Vehicular Technology* 68, 7 (2019), 6903–6916.

[23] H. Ullah, N. Gopalakrishnan Nair, A. Moore, C. Nugent, P. Muschamp, and M. Cuevas. 2019. 5G Communication: An Overview of Vehicle-to-Everything, Drones, and Healthcare Use-Cases. *IEEE Access* 7 (2019), 37251–37268.

[24] M. Wazid, A. K. Das, N. Kumar, M. Conti, and A. V. Vasilakos. 2018. A Novel Authentication and Key Agreement Scheme for Implantable Medical Devices Deployment. *IEEE Journal of Biomedical and Health Informatics* 22, 4 (2018), 1299–1309.

[25] M. Wazid, A. K. Das, N. Kumar, A. V. Vasilakos, and J. J. P. C. Rodrigues. 2019. Design and Analysis of Secure Lightweight Remote User Authentication and Key Agreement Scheme in Internet of Drones Deployment. *IEEE Internet of Things Journal* 6, 2 (2019), 3572–3584.

[26] M. Wazid, A. K. Das, S. Shetty, and M. Jo. 2020. A Tutorial and Future Research for Building a Blockchain-Based Secure Communication Scheme for Internet of Intelligent Things. *IEEE Access* 8 (2020), 88700–88716.

[27] M. Wazid, S. Zeadally, A. K. Das, and V. Odelu. 2016. Analysis of Security Protocols for Mobile Healthcare. *Journal of Medical Systems* 40, 11 (2016), 1–10.