Blockchain-Enabled Secure Communication for Unmanned Aerial Vehicle (UAV) Networks

Randhir Kumar  
Department of Electrical Engineering,  
Indian Institute of Technology,  
Hyderabad  
Telangna 502285, India  
randhir.honeywell@ieee.org

Ahamed Aljuhani  
Department of Computer Engineering, Faculty of Computers and Information Technology,  
University of Tabuk  
Tabuk 47512, Saudi Arabia  
A_aljuhani@ut.edu.sa

Prabhat Kumar  
Department of Software Engineering,  
LUT School of Engineering Science,  
LUT University  
Lappeenranta 53850, Finland  
prabhat.kumar@lut.fi

Abhinav Kumar  
Department of Electrical Engineering,  
Indian Institute of Technology,  
Hyderabad  
Telangna 502285, India  
abhinavkumar@ee.iith.ac.in

Antony Franklin  
Department of Computer Science Engineering, Indian Institute of Technology, Hyderabad  
Telangna 502285, India  
abhinavkumar@ee.iith.ac.in

Alireza Jolfaei  
College of Science and Engineering,  
Flinders University  
Adelaide, Australia  
alireza.jolfaei@flinders.edu.au

ABSTRACT

While 5G can provide high-speed Internet connectivity and over-the-horizon control for Unmanned Aerial Vehicles (UAVs), authentication becomes a key security component in 5G-enabled UAVs. This is due to the fact that the communicating entities in the network mostly use unsecured communication channel to exchange critical surveillance data. Authentication thus plays a crucial role in the 5G-enabled UAV network, providing a range of security services such as credential privacy, Session-Key (SK) security, and secure mutual authentication. However, transparency, anonymity, traceability, and centralized control are few major security requirements that cannot be fulfilled by the traditional authentication schemes. One of the upcoming technologies that can provide a solution for present centralized 5G-enabled UAV network is blockchain-based authentication scheme. Motivated from aforementioned discussion, this paper presents a Permissioned Blockchain empowered Secure Authentication and Key Agreement Framework in 5G-enabled UAVs. In this framework, first an authentication phase between UAV-to-UAV, UAV-to-Edge Server (ES) and Edge-to-Cloud Server (CS) supporting mutual authentication and key agreement is proposed. The authenticated surveillance data collected from UAV is used by the peer-to-peer CS for transaction verification, block creation and addition using smart contract-based consensus mechanism. The practical implementation of framework shows the effectiveness of the proposed approach.

CCS CONCEPTS

• Security and privacy → Symmetric cryptography and hash functions.

KEYWORDS

5G, Authentication and Key Agreement, Blockchain, Unmanned Aerial Vehicles

ACM Reference Format:


1 INTRODUCTION

Fifth generation (5G) networks resulted from the rapid growth of emerging technologies and applications, such as mobile edge computing, Internet of Things (IoT), and unmanned aerial vehicles (UAVs) [7]; such technologies require reliability, low latency, and high data rates. Compared to 4G networks, 5G networks significantly improve key features of sensing technologies. For example, they offer higher data rates, delivering more than 10 Gbps; they increase coverage area for wireless communications; and they provide low-latency operations [13]. The integration of 5G networks with innovative technologies, such as software-defined networking, network functions virtualization, fog computing, IoT, and UAVs, significantly improves end-user quality of service, and machine-to-machine and human-to-human communications [14].

As UAVs have grown and rapidly developed in the past decade to meet market growth, the 5G-enabled UAV can achieve superior performance in terms of latency, capacity, and communication coverage [10]. The 5G-enabled UAV can be deployed in a diverse range of industrial applications, including smart agriculture, smart health care, and smart transportation systems, to provide a cost-effective, flexible, and more efficient platform for end users. Because
of the nature of UAV operations, which rely on continuous data exchange with other sensing platforms, the security and privacy of the information exchanged between devices remains a significant challenge. UAV drones communicate with different sensing and smart devices, receiving and sending critical data to the ground station server (GSS). However, maintaining the security and privacy of the communication among smart devices, drones, and GSSs remains a significant issue [3]. Insecure communication among different sensing technologies, on the contrary, might be exploited by intruders and pose significant security risks. An attack, such as man-in-the-middle, intercepts communication between smart devices with the goal of capturing, modifying, and forwarding messages so that authentic participants believe the messages came from an authentic device. Another threat to 5G-enabled UAVs is distributed denial-of-service attacks, in which an attacker attempts to make smart devices unavailable or slow in responding to authentic participants [1].

Recent technologies, such as blockchain, attracted a great deal of attention recently owing to the numerous benefits that such a technologies offer. Blockchain technology follows decentralized, distributed, and peer-to-peer (P2P) communication networks, with data stored on each node to ensure the data integrity and confidentiality of all transactions [9]. Blockchain technology has been integrated with various emerging technologies and deployed in a variety of critical domains because it provides effective, robust, and more secure solutions against different types of cyberattacks [5, 12]. Precisely, blockchain-assisted authentication for 5G-enabled UAVs has been adopted to certify drone identities and ensure secure data-sharing communication in integrated environments, such as fog and cloud [2]. Although several studies on blockchain-enabled authentication for UAVs have been conducted to ensure the data integrity and confidentiality of all transactions in such integrated environments, some major challenges remain [8, 11]. Existing solutions, for example, lack cost-effective, efficient, and scalable blockchain-enabled authentication for UAV systems. Blockchain is deeply integrated with other sensing technologies and applications, such as IoT, fog, and cloud; however, it also lacks full integration with UAV systems.

Motivated by the aforementioned discussion, this article introduces a "UAV Communication", an architecture for secure authentication and key agreement using permissioned blockchain in 5G-enabled UAVs. Specifically, an authentication scheme is designed during the hop-by-hop device data relay between any two UAVs that are forwarding the data, other authentication scheme is designed when a UAV forwards its data to the associated edge server and final authentication scheme is designed when a edge server forwards its data to the cloud server. This is done specifically to ensure that the data exchanged between the components comes from the expected reliable source. The edge server encrypts the surveillance data before sending it to a cloud server using the cloud server’s public key. The edge server is also utilized to make the decision of which transactions in the received block should be encrypted and which can be kept unencrypted in order to create the hybrid blockchain. A distributed cloud centre with smart contract facility makes up the cloud server. The cloud servers initially employ smart contracts to validate the received transaction. The cloud server generates the block once it has been verified, works with other cloud servers to run a Proof-of-Authority (round-based aura algorithm) consensus method, and finally adds the entire block to the blockchain.

2 SYSTEM MODELS

In this section, we present the network and a threat model that is used to design proposed framework. Both models are explained below:

2.1 Network Model

The network model for the proposed framework is illustrated in Fig. 1. The framework demonstrates the 5G-enabled UAV network where UAVs are responsible to collect data from IoT smart devices placed in various location of smart cities. The proposed framework has a Trusted Authority (TA), that is considered as a fully trusted entity and is responsible for registering all UAVs, edge servers and cloud servers prior to their deployment. In this strategy, the UAV gathers surveillance data and securely transmits it to edge servers after establishing a session key between them. The encrypted data is relayed to cloud server on a hop-by-hop forwarding basis from edge servers. The cloud server has distributed data centers forming peer-to-peer cloud server network. The cloud data center uses its private key to decrypt the received data. The smart contract-based consensus algorithm is used by data centers to construct, verify and then will add transaction to blockchain ledger. The authenticated
data stored in blockchain is temper proof and is rescued from data poisoning attacks.

2.2 Threat Model

The "Dolev-Yao", often known as the DY model, is the first threat model that we employ in this paper [6]. According to this model, an adversary known as A can not only intercept, alter, or delete communication messages between any two participants, but can also add harmful messages to the channel. It is assumed that Trusted Authority (TA) is a perfectly reliable entity. Unmanned Aerial Vehicles (UAV) is regarded as untrusted entity, whereas edge and cloud servers (CS) are regarded as semi-trusted entities. The Canetti and Krawczyk adversary model (often referred to as CK-adversary) is also used as a further threat model [4]. In this instance, an adversary A has the ability to hijack a live session between two network users by stealing their secret credentials and the session key/state.

3 THE PROPOSED FRAMEWORK

3.1 Proposed Authentication and Key Agreement Module

3.1.1 Initialization Phase. This phase explores, how Trusted Authority (TA) chooses the parameters to register the entities in proposed framework. The detailed process is discussed below. First, non singular elliptic curve is selected by the TA i.e., \( E(\beta, y) \), \( S^2 = \beta^3 + \alpha \beta + y \mod W_n \), where \( W_n \) is a large prime value and \( \beta, y \in \mathbb{F}^* \). Further, the TA chooses a base point \( \mathcal{P} \in E(\beta, y) \) of order \( \mathcal{N} \) as \( W_n \). Furthermore, the TA chooses a cryptographic hash function i.e.; \( H(\cdot) \) using SHA-256. In addition, TA chooses an identifier \( \text{ID}_{TA} \) and picks a private key \( \text{SK}_{TA} \in \mathbb{F}^* \) and evaluates a public key \( \text{PK}_{TA} = \text{SK}_{TA} \mod (W_n) \). Finally, the TA preserves a private key \( \text{SK}_{TA} \) secret and disseminates public parameters \((E(\beta, y), \mathcal{P}, H(\cdot), \text{ID}_{TA})\).

3.1.2 Registration Phase. This phase describes a registration process of each entities and shares the communication parameters.

(a) UAV Registration: The TA registers a UAV node \( \text{UAV} \), where \( \text{UAV} \in \{1, 2, \ldots, \text{UAV}_n\} \).

**Step-1:** The TA chooses an unique identity \( \text{ID}_{\text{UAV}} \) for registration of UAV devices. Further, TA evaluates a pseudo identity \( \text{ID}_{\text{UAV}} = H(\text{ID}_{\text{UAV}} \mod (W_n)) \) where \( \text{ID}_{\text{UAV}} \) is a registration time of \( \text{UAV} \) and generates a certificate \( \text{CRT}_{\text{UAV}} = H(\text{ID}_{\text{UAV}} \mod (W_n)) \) for each \( \text{UAV} \) and preserves registration information \( \text{ID}_{\text{UAV}} \) on board units \( \text{OBU}_j \) of UAV devices \( \text{UAV} \).

**Step-2:** TA chooses a random number \( R_{\text{EN}}, R_{\text{ES}} \in \mathbb{F}^* \), and evaluates a partial private key \( \text{PPR}_{\text{EN}} = \text{PPR}_{\text{ES}} \mod (W_n) \) for each \( \text{UAV} \). Further, \( \text{TA} \) chooses a base point \( \mathcal{P} = \mathcal{P} \mod (W_n) \) and generates temporary identity \( \text{ID}_{\text{UAV}} = H(\text{ID}_{\text{UAV}} \mod (W_n)) \) for each \( \text{UAV} \) and evaluates a partial private key \( \text{PPR}_{\text{EN}} = \text{PPR}_{\text{ES}} \mod (W_n) \) on board units \( \text{OBU}_j \) of UAV devices \( \text{UAV} \).

(b) ES Registration: The TA registers a ES \( \text{ES}_j \), where \( \text{ES}_j \in \{1, 2, \ldots, \text{ES}_n\} \).

**Step-1:** The TA chooses an unique identity \( \text{ID}_{\text{ES}} \) for registration of ES. Further, TA evaluates a pseudo identity \( \text{ID}_{\text{ES}} = H(\text{ID}_{\text{ES}} \mod (W_n)) \) where \( \text{ID}_{\text{ES}} \) is a registration time \( \text{ES}_j \) and produces certificate \( \text{CRT}_{\text{ES}_j} = \text{CRT}_{\text{ES}_j} * H(\text{ID}_{\text{ES}} \mod (W_n)) \).

**Step-2:** TA chooses a random number \( R_{\text{EN}}, R_{\text{ES}} \in \mathbb{F}^* \), and evaluates a partial private key \( \text{PPR}_{\text{ES}} = \text{PPR}_{\text{ES}} \mod (W_n) \) for each \( \text{ES}_j \). Further, \( \text{TA} \) chooses a base point \( \mathcal{P} = \mathcal{P} \mod (W_n) \) and generates a partial private key \( \text{PPR}_{\text{ES}} \) and evaluates a public key \( \text{PK}_{\text{ES}} = \text{PK}_{\text{ES}} \mod (W_n) \) for each \( \text{ES}_j \), further, \( \text{ES}_j \) chooses an unique identity \( \text{ID}_{\text{ES}} \) for individual \( \text{CSV}_j \) registration. Further, TA evaluates a pseudo identity \( \text{PPR}_{\text{ES}} \mod (W_n) \) and preserves a registration information \( \text{PPR}_{\text{ES}} \) on its board unit \( \text{OBU}_j \) of ES \( \text{ES}_j \). Finally, \( \text{ES}_j \) deletes a partial private key \( \text{PPR}_{\text{ES}} \) and disseminates a public key \( \text{PK}_{\text{ES}} \).

3.1.3 Key Agreement and Authentication Phase. We have discussed various steps used in key agreement and authentication. i) UAV to UAV Authentication

**Step-1:** UAV\text{ }1\text{ } picks an unique random value \( d_t \in \mathbb{F}_t \) and its current timestamp \( \text{TSTP}_1 \), and evaluates \( L_1 = h(\text{ID}_{\text{UAV}_1} \mod (W_n)) \) for each \( \text{UAV}_1 \). Further, \( \text{UAV}_1 \) applies encryption as \( L_2 = E_{\text{PPR}_{\text{UAV}_1}}(L_1) \). Furthermore, \( \text{UAV}_1 \) evaluates the \( L_3 = H(L_2) \) for each \( \text{UAV}_1 \) and preserves a registration information \( \text{PPR}_{\text{UAV}_1} \) and transmits request message as \( M_1 = H(\text{ID}_{\text{UAV}_1}, \text{PPR}_{\text{UAV}_1}, \text{TSTP}_1, L_2) \) and transmits to \( \text{UAV}_2 \) through open channel.

**Step-2:** after message retrieval \( M_1 \) by \( \text{UAV}_2 \) timestamp gets validated i.e., \( \text{TSTP}_2 \) using \( \text{TSTP}_1, | \text{TSTP}_2 - \text{TSTP}_1 | < \Delta T \). If it is valid, UAV\text{ }2 checks for certificates \( \text{CRT}_{\text{UAV}_1} \), \( \text{PK}_{\text{UAV}_1} \) and if validated successfully, then UAV\text{ }1 receives a timestamp \( \text{TSTP}_2 \) with respect of \( \text{PPR}_{\text{UAV}_1} \) from the databases and evaluates \( L_3 = h(L_2) \) for each \( \text{UAV}_2 \) and preserves registration information \( \text{PPR}_{\text{UAV}_1} \) to verify whether \( L_3 = L_1 \). If validated successfully, then UAV\text{ }2 applies decryption \( L_2 = L_2 - E_{\text{PPR}_{\text{UAV}_1}}(L_1) \).

**Step-3:** UAV\text{ }2 chooses unique random number \( \text{UAV}_2 \in \mathbb{F}_b \) and maintains the timestamp \( \text{TSTP}_2 \) and generates temporary identity \( \text{ID}_{\text{UAV}_2} = H(\text{ID}_{\text{UAV}_2} \mod (W_n)) \), and \( \text{PPR}_{\text{UAV}_2} \), and applies encryption \( \text{UAV}_2 = E_{\text{PPR}_{\text{UAV}_2}}(\text{ID}_{\text{UAV}_1}) \). Next, UAV\text{ }2 (UAV\text{ }1) creates session key \( \text{SES}_{\text{UAV}_1} = H(\text{ID}_{\text{UAV}_1} \mod (W_n)) \) and evaluates a partial private key \( \text{PPR}_{\text{UAV}_2} = \text{PPR}_{\text{UAV}_2} \mod (W_n) \) and encrypts the message \( M_2 = H(\text{ID}_{\text{UAV}_1}, \text{PPR}_{\text{UAV}_2}, \text{TSTP}_2, \text{TSTP}_1) \) and sends a reply message \( M_2 = H(\text{ID}_{\text{UAV}_1}, \text{PPR}_{\text{UAV}_2}, \text{TSTP}_2, \text{TSTP}_1) \) and transmits to \( \text{UAV}_1 \) through open channel.

**Step-4:** once reply message is received (\( M_2 \)) from UAV then timestamp gets validated \( \text{TSTP}_2 \) and checks whether \( | \text{TSTP}_2 - \text{TSTP}_1 | < \Delta T \). if validated successfully, \( \text{UAV}_1 \) checks certificates
using \( C_{TK_{UAV}} \). \( B = PBZ + HF(PB_{UAV}) \mid PB_{RT} \). Further, \( UAV_1 \) applies decryption \( UAV_2 \) to receive \( UAV_2 = D_{PPR_{UAV}}(UAV_2) \). Furthermore, \( UAV_1 \) computes \( UAV_1^{new} = HF(PPR_{UAV}^{new} \mid \text{timestamp}) \) and computes \( UAV_2^{new} = UAV_2 \), then \( UAV_1 \) evaluates \( PPR_{UAV}^{new} = PPR_{UAV}^{new} \oplus HF(PS_{UAV}^{new} \mid PPR_{UAV}^{new} \mid \text{timestamp}) \) and creates session key \( SES_{UAV}^{new} = HF(PSS_{UAV}^{new} \mid L_1 \mid UAV_2^{new} \mid UAV_2 \mid PPR_{UAV}^{new} \mid \text{timestamp}) \) and share to \( UAV_2 \). Further, \( UAV_1 \) picks a timestamp \( T_{STP} \), and checks for session key verification \( T_{STP} \), through \( SES_{UAV}^{new} = HF(PSS_{UAV}^{new} \mid \text{timestamp}) \) and goes for updation of \( PPR_{UAV}^{new} \) and \( PPR_{UAV}^{new} \) into the database. Furthermore, \( UAV_1 \) generates acknowledgement receipt \( M_2 = \{ SES_{UAV}^{new} \mid T_{STP} \} \) and transmit to \( UAV_2 \) through open channel.

Step-5: once acknowledgement receipt is received by \( UAV_2 \), \( M_2 \) checks for timestamp \( T_{STP} \) and evaluates \( L_1 \mid UAV_2 \mid PPR_{UAV}^{new} \mid \text{timestamp} \). Further, \( UAV_2 \) applies decryption \( PPR_{UAV}^{new} \mid \text{timestamp} \) and its timestamp \( \text{timestamp} \) and transmits to \( ES \) through open channel.

**Step-1:** \( UAV \) picks an unique random value \( dr_1 \in Z_q \) and its current timestamp \( T_{STP} \), and evaluates \( L_1 \mid UAV_2 \mid PPR_{UAV}^{new} \mid \text{timestamp} \). If \( L_1 \mid UAV_2 \mid PPR_{UAV}^{new} \mid \text{timestamp} \) is validated successfully, then \( UAV_2 \) gets the session key \( SES_{UAV}^{new} \) and its timestamp and transmits to \( ES \) through open channel.

**Step-2:** after successful receiving of message \( M_2 \), \( UAV_2 \) checks for timestamp \( T_{STP} \), and evaluates \( L_1 \mid UAV_2 \mid PPR_{UAV}^{new} \mid \text{timestamp} \). If \( L_1 \mid UAV_2 \mid PPR_{UAV}^{new} \mid \text{timestamp} \) is validated successfully, then \( ES \) sends the acknowledgement receipt \( M_2 = \{ SES_{UAV}^{new} \mid T_{STP} \} \) to \( UAV \) through open channel.

**Step-3:** Further, \( UAV \) picks for unique random number \( ES_{dr_1} \in Z_q \) and its timestamp \( T_{STP} \), and generates temporary identity \( PPR_{UAV}^{new} \) and evaluates \( ES_{dr_1} = HF(PSS_{UAV}^{new} \mid PPR_{UAV}^{new} \mid \text{timestamp}) \) and applies encryption \( ES_{dr_2} = E_{PB_{UAV}}(ES_{dr_1}) \). Further, ES (ES) evaluates session key \( SES_{ES} = HF(PSS_{ES}^{new} \mid PPR_{ES}^{new} \mid \text{timestamp}) \), and \( ES_{dr_1} = HF(PSS_{UAV}^{new} \mid PPR_{UAV}^{new} \mid \text{timestamp}) \) and generates reply message \( M_2 = \{ PPR_{UAV}^{new}, ES_{dr_1}, ES_{dr_2}, CR_{ES}, PSID_{ES}, T_{STP} \} \) and transmit to \( ES \) through open channel.

**Step-4:** once reply message is successfully received from \( ES \), \( ES \) then timestamp gets validated \( T_{STP} \) by \( ES \), \( T_{STP} \mid T_{STP} \), \( \text{timestamp} \). If validated successfully, then \( ES \) checks certificates \( CR_{ES} \), \( B = PB_{ES} + HF(PB_{ES} \mid PB_{RT}) \). Further, \( ES \) applies decryption \( ES_{dr_2} \) to receive \( ES_{dr_2} = D_{PPR_{ES}}(ES_{dr_2}) \). Further, \( UAV_1 \) evaluates \( ES_{dr_1} = HF(PSS_{UAV}^{new} \mid PPR_{UAV}^{new} \mid \text{timestamp}) \), and \( ES_{dr_1} = HF(PSS_{UAV}^{new} \mid PPR_{UAV}^{new} \mid \text{timestamp}) \) and finds \( ES_{dr_1} = ES_{dr_2} \) when \( UAV \). Furthermore, partial private key gets validated \( PPR_{UAV}^{new} = PPR_{UAV}^{new} \oplus HF(PSS_{UAV}^{new} \mid PPR_{UAV}^{new} \mid \text{timestamp}) \) and evaluates a session key \( SES_{UAV}^{new} = HF(PSS_{UAV}^{new} \mid L_1 \mid ES_{dr_1} \mid T_{STP} \mid T_{STP} \) and share to \( ES \). Furthermore, \( UAV \) picks a current timestamp \( T_{STP} \) and generates acknowledgement message \( M_3 = \{ SES_{UAV}^{new} \mid T_{STP} \} \) and transmit to \( ES \) through open channel.

**Step-5:** once acknowledgement reply received successfully, then \( ES \) checks for timestamp \( T_{STP} \), and evaluates \( L_1 \mid ES \). Further, \( ES \) verifies session key \( SES_{UAV}^{new} = HF(PSS_{UAV}^{new} \mid T_{STP}) \) if matches successfully, then \( ES \) establishes session key \( SES_{UAV}^{new} = HF(PSS_{UAV}^{new} \mid T_{STP}) \) and \( ES \) goes for updation of \( PPR_{UAV}^{new} \) and \( PPR_{UAV}^{new} \) into the database securely.
3.2 Proposed Permissioned Blockchain-based Transaction Writing Module

This phase describes the block verification and addition. The authorized UAVs are responsible to create the transactions in the network. Next, the transactions gets verified by the authorized ES denoted as miner. Further, block gets created and added into the blockchain. The block consists of two parameters namely \( V_i \leftarrow (W_i, X_i) \), where \( W_i \) denotes local blockchain ledger of peers where \( X_i \) denotes block pointer. The algorithm consists of four different functions like PROPOSE(), SCORE(), DELIVER(), and ISDECIDED(). The PROPOSE() function is responsible to propose a block with an index in blockchain network. The consensus executed successfully, once block gets decided which is explained in ISDECIDED() function (line number 33). The PROPOSE function uses time-duration (consecutive period) where each miners executes infinite loop and checks CTS, in order to propose a block(line number 10). When it gets chance to propose a block (line number 12), a miner sets the parent of block (last block) and does signature (line number 16). Each disseminates() by PROPOSE() function delivered to participating nodes (honest nodes). The DELIVER() functions gets executed (line number 27) and invoked by the honest nodes with correct view of blockchain network. The correct view of the blockchain is made using SCORE() function (line number 23), where the highest blockchain gets highest score. The score is computed where many blockchain, with similar height with last block consists of lowest index wins. This is performed using two different functions i.e.; height and step-num that denotes blockchain height and number of block in the blockchain network. Finally, ISDECIDED() function (line number 33) gets executed when block \( b \) is decided after successful consensus, a participating nodes checks for two consecutive rounds i.e., round1 and round2 for block \( b \), in each round block \( b \) is mined (verified) by majority of miners (\( ES_i \)). Next, block \( b \) gets added into the blockchain network after successful mining (verification). The block verification and block Addition is detailed in Algorithm 1.

4 SECURITY ANALYSIS

This phase describes security analysis of the proposed model. It includes the formal verification to prevent various attacks. The detailed security analysis is summarized below.

1. Impersonation Attack: An attacker can generate temporary identity \( UAV \), pseudo identity \( ISPDUAV \), and partial private key \( PPR_{UAV} \) to perform operation as a legitimate user. Further, timestamp \( TSPP_{UAV} \) can be generated for access permissions in the framework. However, session based approach is applied to verify the unique identity of the devices \( UAV \). If all credential is matched then access permissions granted, else connections terminated immediately. Thus, this approach prevents from impersonation attack.

2. Insider Attack: The attackers are privileged (can be insider) and can sniff all the credential like UAV identification \( UAV \), pseudo identity \( ISPDUAV \), and timestamp \( TSPP_{UAV} \). However, the access can only be permitted after session based verification of the entities. Thus, the approach does not allow access without permissions and prevents from insider attack.

3. MITM and Replay attack: The attacker may get the details of the UAV from insecure channel and communications like \( UAV \) and timestamp \( TSPP_{UAV} \) of registration. The attackers may send the details to the UAVs for making certain operations. However, the UAVs checks for the timestamp and verifies the session. However, it is difficult to compute all the credential at certain interval of time from id generation to session verification. Performing all the required evaluation at perfect time edge is difficult. Thus, the attacker cannot perform the MITM and replay attack.

5 PERFORMANCE ANALYSIS

The proposed framework was implemented on a Tyrone PC with two 2.20GHz Intel CPUs and 128 GB of RAM. We have simulated the proposed framework on the Ethereum Rinkby blockchain platform using POA consensus algorithm. Ethereum Ropsten uses smart
6 CONCLUSION AND FUTURE WORK

In this article, we discussed the security aspect of secure UAVs communication and designed a novel secure authentication and key agreement framework. The proposed framework preserves four-factor authentication of an entity i.e., unique identity, pseudo-identity, certificate, and timestamp. The framework supports session key establishment with mutual authentication, to make secure communication between entities. The data received by P2P cloud data center uses PoA consensus algorithm to construct, verify and write transactions into blockchain. The blockchain-enabled distributed cloud makes data "temperproof", "trustable" and rescues data from poisoning attack. Future work includes implementing proposed framework in real-time 5G-enabled UAV network.

REFERENCES


5.1 Blockchain Result Analysis

The Fig.5 shows the blockchain result analysis, where transactions upload time, block mining time, block creation time, and transaction off-chain storage size is computed. The Fig. (2a) shows transaction upload time for varying number of UAV and transactions. From the observed computation, the upload time is dependent on number of transactions. The Fig.(2b) and (3a) shows the block mining time and block creation time in the proposed framework. It can be seen that, the computation time in both the cases are dependent on number of UAV and number of transactions shared in the network. The Fig.(3b) shows the off-chain storage size of transactions which is computed in KB. It can be noticed that, the storage size in dependent on number of transactions stored in the off-chain layer.