International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 07, July-2022

Block Chain-based Access Control with Optimal Key Generation in Internet of Drones

Subhadra Perumalla
Research Scholar JNTU Ananthpuram
Andhra Pradesh

Dr. Santanu Chatterjee
Scientist RCI,DRDO
Hyderabad

Dr. A. P. Siva Kumar
Assoc. Prof
JNTU Ananthpuram
Andhra Pradesh

***Abstract*: Recently, there is a growing interest in the research of Internet of Drones (IoD) owing to its applicability in numerous fields, including civilian and military. The information gathered by the drones is transmitted over the internet, which makes them vulnerable to privacy and security threats. Hence, efficient methods of providing security to IoD are necessary to provide authenticity, integrity and confidentiality of data. These issues can be effectively handled by using blockchain, which is an immutable ledger-based technology. In this paper, a block chain-based access control system is developed based on an optimal key generation. The method is implemented using various phases, such as Pre-deployment, registration and authentication, Drone to drone (D2D) access control phase, Drone to server access control phase and Emergency access control phase. A coot algorithm based key generation is utilized in the D2D access control phase and Drone to server access control phase. Further, the performance of the COOT Keygeneration-based Access control is evaluated using metrics, such as delay, packet loss rate and throughput and the value obtained are 0.0725 sec, 0.883% and 73.547 bps respectively.**

Index Terms: Internet of Drones, Block chain, Coot algorithm, Access Control, Key generation

1. INTRODUCTION

Drones refer to the group of vehicles that possess the ability to navigate without the need of any pilot. The drones that are operated in sky are also known as Unmanned Aerial Vehicles (UAV). They are normally fitted with a camera for capturing and transferring the real time data to the ground equipment. Moreover, they are provided with a sensor that records data and a Global Positioning System (GPS) for acquiring information from Google Earth [5]. Drones are employed in various fields, like disaster mitigation, agriculture, transportation, communication, etc. They have the ability to enhance the quality of life by becoming a vital aspect in the building of smart cities where they can be used in monitoring traffic,delivering medicine,package delivery,fire-fighting,accident investigation, and so on. Drones can also be utilized in communication, where they can be employed as the aerial base station (BS) for transmitting and receiving data [6]. Drones are being used by search and rescue teams for delivering essential items. There has been a constant increase in the usage of drones owing to its capability in transporting and delivering goods and also in capturing real time information [7]. The advanced techniques, such as Software-Defined Network (SDN) and 5G have paved the way that offer high flexibility and capacity to drones, and have enabled creation of an aerial network called as IoD [8]. IoD makes use of various techniques and computation algorithms for controlling the physical objects, like sensors, drones and the ground equipment, thereby creating a cyber-physical system [9].

Nonetheless, the insecure communication links, weak encryption, dynamic changing network topology, distribution of drones in remote and open environment makes them susceptible to various attacks. Additionally, the constricted resources and energy available to the drones contribute to the existing security challenges [11]. IoD is prone to several attacks, such as forgery, replay, impersonation, Denial-of-Service (DoS), tampering, spoofing, etc. These attacks are carried out with the malicious intent of extracting the cryptographic keys, exploiting unauthorized connections, and obtaining the sensitive information gathered by the drones. It is highly important to mitigate these threats to provide security and confidentiality to the data transmitted[19]. The attackers may use unauthorized drones for destroying the authentic ones and hence authentication is highly vital in providing security. Since authentication aims at confirming the identity of the nodes, only legitimate and authentic drones will be granted access to the IoD network [12]. Once the identity of the component is established, access control is executed, wherein the users are provided access to the resources/network selectively based on the privileges. Lack of efficient access control scheme may contribute to the retrieval of confidential data, thereby compromising the network [1]. The cryptographic techniques are not suitable for providing security to drones, which has constrained resources and hence blockchain-based methods are used. Blockchain comprises of blocks of information, which are connected to each other [14],[20] and each node in the blockchain is made aware of the operations carried out in the block chain [15]. Thus, identification of tampering by manipulating a node can be performed by determining the blockchain which is in error state [10].

In this paper, an optimal key generation technique is introduced for blockchain-based access control in IoD. The proposed access control scheme comprises of entities, namely drone, control room, server and user. The control room performs the operation of controlling the movement of the drones in the specific flight zones. The drone is equipped with sensors that have the ability to gather information from the surroundings and the information is transmitted over WiFi to the network connected to the control

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 07, July-2022

room. While a user requests for access to drone, mutual authentication is performed by means of server. The proposed method is implemented using various phases, such as Pre-deployment, registration and authentication, D2D access control phase, Drone to server access control phase and Emergency access control phase. A coot algorithm-based key generation is utilized in the Drone-to-drone access control phase and Drone to server access control phase.

The major contribution of this research work is:

- **Introduced COOT Keygeneration technique:** In order to provide secure communication in IoD, the communication between the drones and the server has to be made secure, thereby a COOT Keygeneration method is developed for providing safe transmission.

The rest of the paper is organized as follows: section 2 reviews the existing access control techniques in IoD. In section 3, the system model is described. The introduced optimal key generation in the blockchain-based access control scheme is detailed in section 4. Section 5 examines the performance of the proposed technique, and the paper is concluded in section 6, along with future scope.

2. MOTIVATION BEHIND THIS WORK

IoD is an emerging field with its application increasing rapidly in several areas. The IoD data is transmitted using the open network which makes them vulnerable to attacks. Various techniques have been proposed to tackle the security issues faced in IoD. In this section, the few of the existing techniques of access control in IoD are reviewed. The methods are discussed with their advantages and demerits and this motivated in the development of an innovative technique.

2.1 Major Challenges

The main issues encountered by the access control techniques in IoD are listed below,

- The iGCACS-IoD [2] method was developed for providing access control in the IoD environment, which is highly efficient in providing a high packet delivery rate; however the method did not succeed in reducing the computational as well as communication overhead, so as to enable its application in real time, which remained a major challenge.
- The drawback in [2] was overcome in [3], where the TCALAS was proposed for authenticating the user as well as drones. However, the method faced an issue where the main issue lies in performing fine tuning of TCALAS for enhancing the security of the IoD network.
- An enhanced security was offered by the BACS-IoD [4], devised for granting access control using block chain. Though, the technique is highly effective against multiple attacks, the major challenge lies in utilization of additional features, like drone anonymity for enhancing the performance.
- Various researches have been developed for providing security to the IoD network. Even though the drones have computational ability, they have to maintain a trade off between the limited power supply, increased flight time and security, thereby affecting the performance of the conventional systems. delay and queuing can be taken care of by network optimization using Genetic Algorithm. In order to provide high Quality of service to Networks, it is essential to provide a path between a given source and multiple destinations which satisfy certain constraints. Multimedia applications in general make use of k shortest paths whenever communication is to be carried out between a single source and one or more than one destination.

3. RELATED WORK:

Several researches have been carried out for protecting the data transmitted in the IoD environment. Here, four such techniques are considered and they are analyzed. Wazid, Met al.[1] proposed an Authentication and Key Agreement technique for performing authentication of the users for accessing information from the drones. The method employed the bitwise XOR operation and cryptographic hash functions for performing authentication. The technique offered high security and protection against several attacks with low end to end delay; however, it was unsuccessful in reducing the packet loss rate. The packet loss rate was minimised by themethod proposed in [2], where Das, A.Ket al.developed an improved certificate-enabled generic access control scheme for IoD deployment (iGCACS-IoD), which performed authentication in two phases, namely registration and access control with cryptographic hash function. The iGCACS-IoD achieved high packet delivery ratio and was efficient in handling several potential attacks; but failed to minimize computational overhead. The drawback listed in [2] was overcome in [3], where Srinivas, Jet al.[3] presented a Temporal Credential-Based Anonymous Lightweight Authentication Scheme (TCALAS) for authenticating user in IoD. The TCALAS method of authentication employed factors, such as biometrics, password and mobile device for performing authentication. Moreover, it utilized a fuzzy extractor method for verifying the biometrics of the user. TCALAS is highly efficient in providing security to the resource limited IoD environment against various kinds of attacks, although the technique works in the case of a single flying zone alone. The above issue is overcome in [4], where Bera, B. et al developed a blockchain-based access control mechanism in an IoT-enabled IoD environment (BACS-IoD), which offered access between drone to other drones and the Ground station server (GSS). The GSS utilized Ripple Protocol Consensus Algorithm (RPCA) for adding blocks in the blockchain. In addition, the BACS-IoD was highly efficient against passive as well as active attacks; however the method failed to provide anonymity to the drones.

4. SYSTEM MODEL

IoD finds applications in numerous fields in our day to day life and is aimed at improving the quality of life with the help of sensors. The drones have the ability to investigate the surroundings and perform actions accordingly. Although, the IoD data gathered are vulnerable to security threats owing to the open network over which the data is transmitted. In figure 1, the system model of the block chain based IoD is portrayed.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 07, July-2022

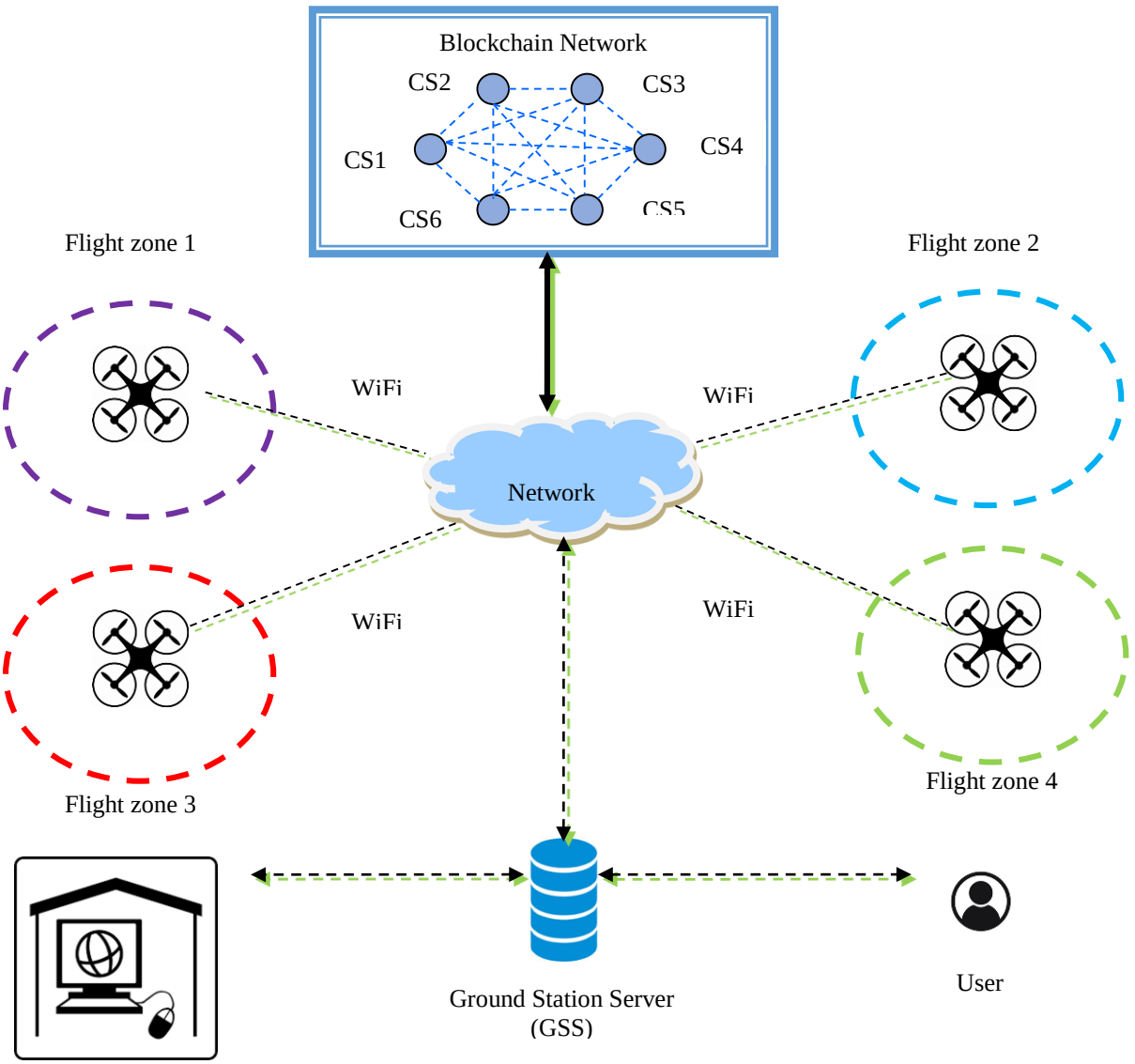


Fig. 1.System model of the Block chain based IoD

In the IoD network, the area where the drones are deployed are partitioned into several flight zones and a drone is deployed in each zone, which is utilized for various operations, like delivering goods in specific directions. The network comprises of a GSS, control room, Cloud Servers (CS) and drones. The control room is responsible for registering all the deployed drones and the GSS, moreover it is a trusted authority. On the other hand, the GSS is responsible for controlling flight of drones in the specific flight zones; they act as connecting points in the communication between drones to infrastructure (D2I). GSS gathers all the data acquired from the drones and converts them into blocks, which are then forwarded to the CS. The CS is responsible for verification and addition of blocks in the block chain. The drones are the UAV comprising of a number of IoT devices, such as magnetic-field change sensing,light-pulse distance sensing (laser),radio detection, sensors, etc. In order to provide secure information exchange, D2D access control as well as drone to GSS access control method is utilized.

5.PROPOSED COOT KEYGENERATION-BASED ACCESS CONTROL USING BLOCK CHAIN FOR IOD

This section details the proposed optimal key generation-based access control using block chain in IoD. The access control scheme comprises of entities, namely drone, control room, server and user. The control room performs the operation of controlling the movement of the drones in the specific flight zones. The drone is equipped with sensors that have the ability to gather information from the surroundings and the information is transmitted over WiFi to the network connected to the control room. While a user requests for access to drone, mutual authentication is performed by means of server. The proposed method is implemented using various phases, such as Pre-deployment, registration and authentication, D2D access control phase, Drone to server access control phase and Emergency access control phase. A coot algorithm-based key generation is utilized for establishing secure communication in the D2D access control phase and Drone to server access control phase. Here, the drones communicate to each other and the server with the help of block chain network. Fig. 2 displays the block diagram of the devised COOT Keygeneration-based access control using block chain in IoD. The various phases are detailed in the ensuing subsections.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 07, July-2022

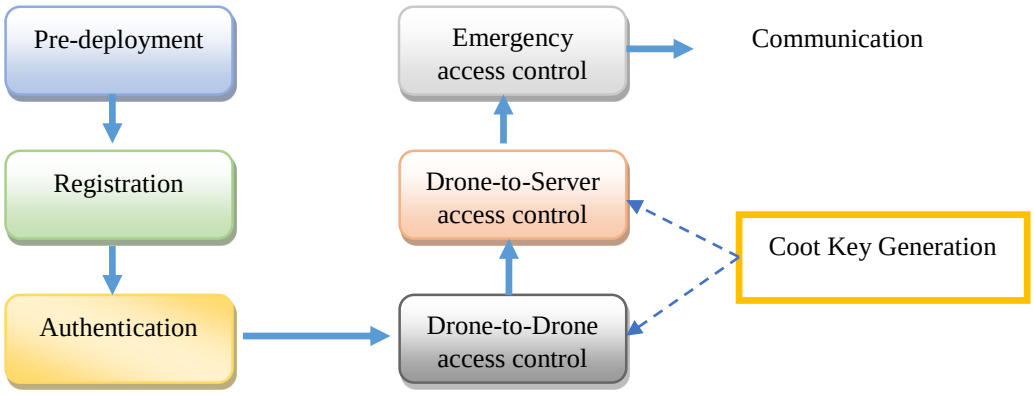


Fig. 2.Block Diagram of the devised COOT Keygeneration based access control using block chain in IoD

5.1 Pre-deployment, user registration and authentication phase

Initially, before deploying the drone, it has to be registered with the server, which chooses a unique identity and a secret message for each drone. Before initiating a session, a session identity is created by the server. The server then stores the relative, session and polynomial identity of the drone ahead of its deployment. Similarly, the user also needs to be registered with the server. Once the user produces all the relevant information, user registration will be initiated by the server where the biometrics of the user is captured by the sensors and the user can select his/her own password. During the process of registration, a distinct identity is shared by the server as well as the user. Hence, the user cannot access the services offered by the server even after registration, as the server has to authenticate the user. Once the server receives the login request, the process of authentication is performed. After the user has successfully logged in, a session key is established between the user and the drone, and then the user enables secure transfer of information.

5.2. D2D access control phase

The mutual authentication between neighboring drones is performed in this phase. The D2D access control is performed in four phases, namely request, key generation, session password update and access control. Once access is granted, information is transferred over the Block chain network. The process is detailed below.

(i) Request

Whenever a sender places a request for initiating data transmission to the server, the server performs storage of the sender drone ID Dr_s, the request message Rq, and the receiver drone ID Dr_{rx}. The data stored is then utilized in the validation process to check the authenticity of the drone. The process is detailed in fig. 3.

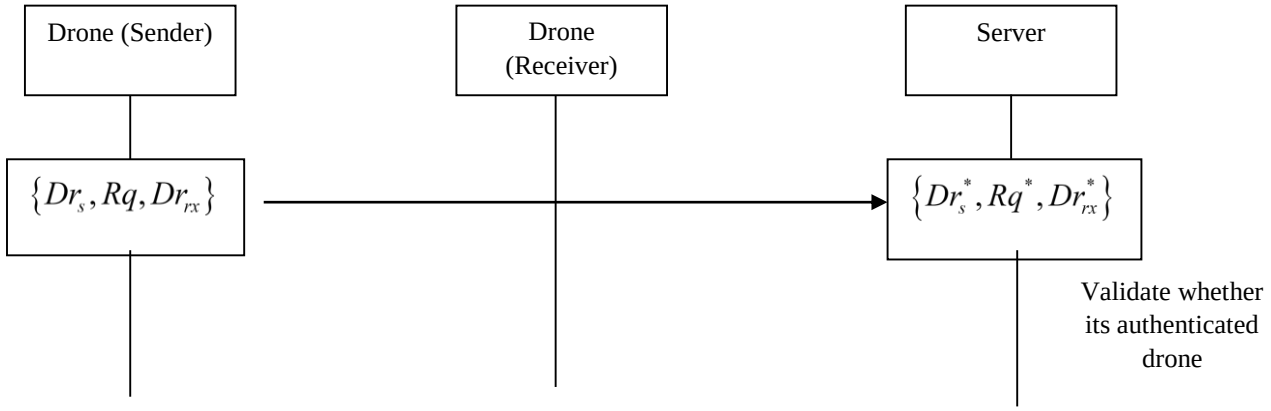


Fig. 3. Request for initiating communication in D2D access control phase

(ii) Key generation

Once the drones are authenticated, key generation is performed by the server based on the credentials of the drones involved. Coot algorithm [18] is employed in the process of key generation. Coot algorithm is a population-based algorithm developed based on the behavior of coot bird in a swarm on the water surface. The algorithm is highly effective in providing solution to problems in unknown solution space. The algorithm is implemented using various movements, such as as random movement, chain movement, alter the position based on group leader, and guiding the group to the most favourable region.

a) Location encoding of Coot

Location encoding represents the schematic representation of the optimal solution. Here, key represents the solution that has to be attained. Figure 4 depicts the Location encoding f the COOT Keygeneration.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 07, July-2022

Fig. 4.Location Encoding

Here, $1\times m$ represent the key size, and m denotes the dimension of the optimal key.

b) Fitness function

The optimal key is found by computing the fitness function, which is given by,

$$Fit = \frac{Z+E}{2} \tag{1}$$

where, Z is the accuracy, and E represents the encryption quality.

The steps of the COOT algorithm are detailed as follows.

Step 1-Initialization: Initially the population of Coot is initialized randomly using the following equation,

$$Ct(i) = rnd(1,n)*(u-l)+l \tag{2}$$

where, $Ct(i)$ is the position of the i^{th} Coot, n denotes the dimension of the problem, u and l represents the upper and upper bound of the search space.

Step 2-Fitness evaluation: Fitness of the coot is evaluated using equation (1), and the maximum value of fitness is considered to find the best solution.

Step 3-Random movement: The Coot performs exploration of the search space and moves towards the arbitrary location, which is given by,

$$X = rnd(1,n)*(u-l)+l \tag{3}$$

If a local optimal is attained, the position of the coot is updated as per the following,

$$Ct(i) = Ct(i)+Y\times rnd_2\times(X-Ct(i)) \tag{4}$$

where, rnd_2 is an arbitrary number in the range $[0,1]$ and Y is obtained from,

$$Y = 1-I\times\left(\frac{1}{itr}\right) \tag{5}$$

Here, I and itr represents the current and maximum iteration, respectively.

Step 4-Chain movement: Chain movement is established by taking the average of the position of the two coot birds $Ct(i)$ and $Ct(i-1)$, which is expressed as,

$$Ct(i) = \frac{Ct(i-1)+Ct(i)}{2} \tag{6}$$

Step 5- Alter position according to leader: The coot birds move in swarm and hence the position is updated as per the leader and can be expressed as,

$$Ct(i) = Lp(G)+2\times rnd_3\times\cos(2\pi r)\times(Lp(G)-Ct(i)) \tag{7}$$

Here, $Lp(G)$ represent the position of the leader G, r and rnd_3 are arbitrary numbers in the range $[-1,1]$ and $[0,1]$.

Step 6-Guiding the group: The optimal location if found by considering the global optimal location and the leader moves towards the global optimum location using,

$$Lp(i) = \begin{cases} U\times rnd_4\times\cos(2\pi a)\times(Best_g - Lp(i))+Best_g & ;rnd_5<0.5 \\ U\times rnd_4\times\cos(2\pi a)\times(Best_g - Lp(i))-Best_g & ;rnd_5\geq 0.5 \end{cases} \tag{8}$$

Here, rnd_4, and rnd_5 are arbitrary numbers in the range $[0,1]$ and a is arbitrary number in the range $[-1,1]$, $Best_g$ is the best location determined, and $U = 2-I\times\left(\frac{1}{itr}\right)$.

Step 7-Reevaluate fitness: The fitness of the coot is reevaluated using equation (2) and if the value obtained is less than that of the leader, them the coot is made as the leader.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 07, July-2022

Step 8-Termination: The above process is kept iterated until the maximum number of iteration is attained.

The key generated is represented by A, which is then send to the sender and receiver, where it is stored as A^*

(iii) Session password and update

Once the key is generated, the sender drones send the corresponding drone IDs and the accept message $\{Accept, Dr_s\}$ to the server. Similarly, the receiver drone also forwards $\{Accept, Dr_{rx}\}$ to the server. The server stores the data acquired as $\{Accept^*, Dr_s^*\}$ and $\{Accept^*, Dr_{rx}^*\}$. After, these data re received by the server, it generates the session password using the following equation.

$$P_{session} = B(h(TS) \oplus A) \tag{9}$$

where, $B(.)$ is the encryption function, $h(.)$ is the hashing function, and TS represents the current timestamp. The server forwards the session password to the receiver and the sender, where it is stored as $P_{session}^*$.

(iv) Access control

The sender drone creates a message containing both the key, and stores the session password using the following equation,

$$Q = B(P_{sesssion}^*) \oplus h(A^*) \tag{10}$$

where, $\oplus$ represent the XOR operation. This information is then sent to the receiver drone. The receiver drone also creates a message in the similar manner like the sender and the message produced is represented as Q^* and this message is compared with the received message Q. If both are same, then access is granted and communication is established over the block chain network.

5.3. Drone to server access control phase

The process of providing access control between the drone and the server is similar to the one between drones. The sender drone forwards the request message and the drone ID to the server. Upon reception, the sender validates the information to authenticate the drone. Once the drone is validated, the server generates the key using the Coot algorithm, which is detailed in the section 4.2. The key generated is then forwarded to the drone, which then transmits the accept message along with the key to the server for generating server password. The drone and the server frame message by using a hashing function on the concatenated drone ID, key and the server password. Both the messages are compared, and if they are similar access is granted, and then communication is carried out using block chain network.

5.4 Emergency Access control phase

This phase comes into action when failure in any drones due to accidents or capture by any attackers occurs and in such cases, the need to deploy another drone arises. An emergency request Erq is placed by the drone to the server along with its ID. The control room performs validation of the drone. A server password is generated by the server and is forwarded to the drone and the control room. The drone then frames a message using the control message and the encrypted password to the control room, where validation is performed to authenticate the drone.

5.5. Block chain network for communication

When access is granted, data is transmitted between the sender and the receiver drones over the block chain network using the created session key. Block chain is highly effective in preserving the secrecy of the information. Moreover, the data is gathered at the server and the blocks are added to the prevailing block chain. The gathered data is converted into transactions, which are encrypted using public key. Further, a Merkle tree is constructed by calculating the Merkle tree root (MR) using the encrypted transactions. A hash block is used in computing of data hashing with blocks and the blocks formed are send to the cloud server. The block generate will contain a header and a payload, with the header containing data regarding the block version, Previous block hash, Merkle tree root, Timestamp, Block owner, Public key of owner and Flying zone number. The payload containing information regarding the encrypted transactions, Current block hash and Signature on block [16].

6. RESULTS AND DISCUSSION

This section deals with the results obtained during the experimentation of the proposed COOT Keygeneration method. Moreover, the evaluation of the introduced block chain based access control system in comparison with the existing authentication schemes is detailed.

6.1. Experimental Setup

The quantitative analysis of the introduced block chain based access control system is performed by implementing the technique using NS2 on a PC with the following specifications: Ubuntu software, 2 GB RAM as well as Intel i3 processor.

6.2. Evaluation metrics

The introduced method is evaluated on the basis of three parameters, such as throughput, delay, as well as packet loss, which are briefed in the ensuing subsections.

i) Delay

Delay refers to the time needed for the data to be transmitted across the network, and is given by,

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 07, July-2022

$$T_d = \frac{N_b}{TR} \tag{15}$$

where, N_b represents the number of bits, and TR is the rate of transmission.

ii) Throughput

Throughput can be defined as the total amount of data that can be transmitted or received in a unit time, and is obtained by using the following equation,

$$Tput = \frac{N_b}{T} \tag{16}$$

Here, T represents the time taken to transmit or receive N_b bits.

iii) Packet loss

Packet loss is a measure that is used to measure the reliability of the network and denotes the ratio of the packets lost during transmission. Packet loss can be represented as,

$$Pk_{loss} = \frac{N_l}{TR} \tag{17}$$

Here, N_l represents the number of packets lost.

6.3 Comparative techniques

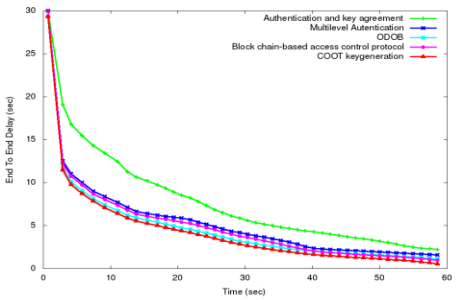
The evaluation of the proposed COOT Keygeneration technique used for Block chain-based access control is performed by comparing it with the existing authentication systems, such as Authentication and key agreement [1], multilevel authentication [17], One Drone One Block-based Lightweight Blockchain Architecture (ODOB) [13], Block chain-based access control protocol [16].

6.4. Comparative Evaluation

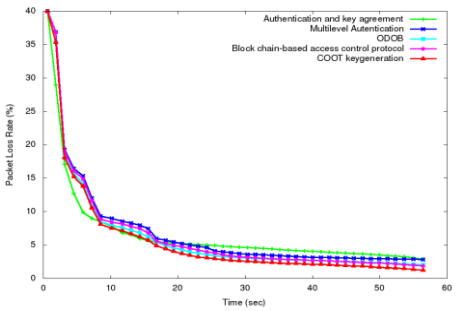
The proposed COOT Keygeneration method for block chain based access control is evaluated using performance metrics, such as delay, packet loss rate and throughput considering 50 and 100 nodes.

i) Evaluation with 50 nodes

Figure 5 depicts the analysis of the block chain-based access control systems using 50nodes. The evaluation of the COOT Keygeneration technique based on delay is portrayed using figure 5 a). The value of end-to-end delay computed by the existing block chain based access control techniques, such as Authentication and key agreement, multilevel authentication, ODOB, Block chain-based access control protocol is 13.052sec, 8.038sec, 7.152sec and 7.75sec at time 10.05sec, whereas the introduced COOT Keygeneration technique is 6.78sec. In figure 5 b), the block chain based access control techniques are evaluated with respect to the packet loss rate. The prevailing methods, like Authentication and key agreement, multilevel authentication, ODOB, Block chain-based access control protocol achieved packet loss rate of 5.245%, 5.331%, 4.417%, and 4.839% for time 20sec, while the introduced COOT Keygeneration attained a low packet loss rate of 3.83%. Likewise, the assessment of the COOT Keygeneration technique for access control in IoD based on throughput is displayed in figure 5 c). For time 25sec, the devised COOT Keygeneration based access control achieved a throughput of 71.883 bps, but the prevailing access control techniques, like Authentication and key agreement, multilevel authentication, ODOB, Block chain-based access control protocol attain only values of 62.283bps, 65.323bps, 68.993bps and 70.438bps, respectively.

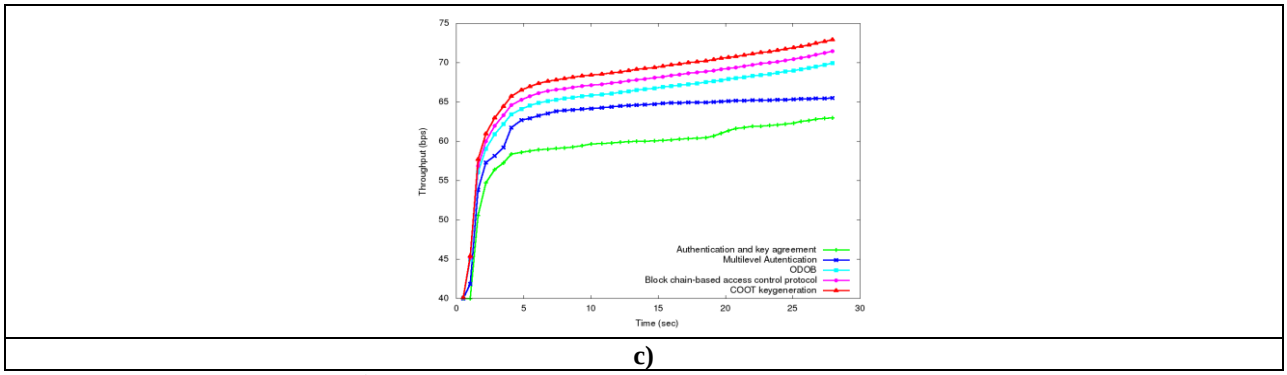


a)



b)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 07, July-2022

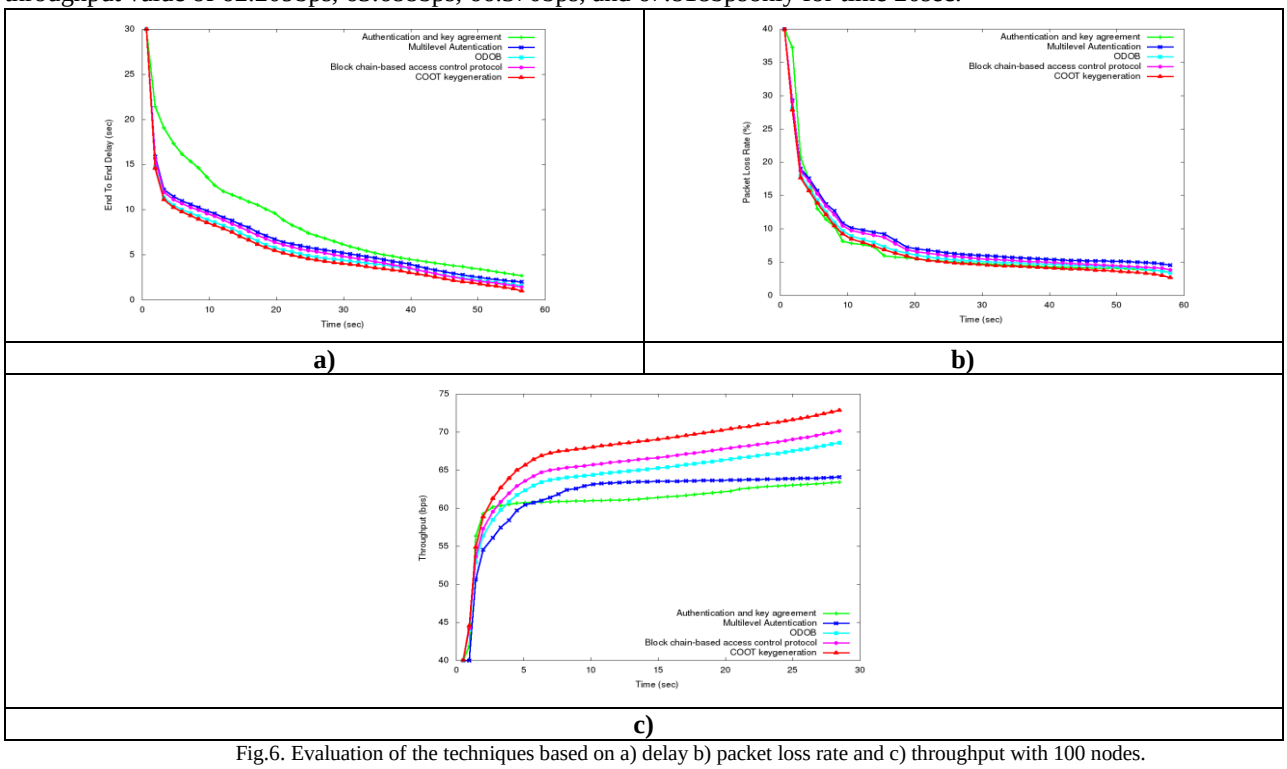


c)

Fig. 5. Evaluation of the techniques based on a) delay b) packet loss rate and c) throughput with 50 nodes.

ii) Evaluation with 100 nodes

In figure 6, the evaluation of access control systems considering 100 nodes using end-to-end delay, packet loss rate and throughput is depicted. Figure 6 a) displays the analysis based on delay. The proposed COOT Keygeneration technique of access control attained a value of end-to-end delay of 4.026sec, whereas the prevailing techniques of access control, like Authentication and key agreement, multilevel authentication, ODO and Block chain-based access control protocol attained higher delay of 30.01sec, 6.141sec, 5.231sec 4.381sec, and 4.812sec respectively at time 30.01 sec. The evaluation of the access control systems based on packet loss rate is portrayed in figure 6 b). At time 40sec, the value of packet loss rate attained by the access control techniques, such as Authentication and key agreement, multilevel authentication, ODOB and Block chain-based access control protocol is 4.301%, 5.417%, 4.701%, and 4.971%. The proposed method, however, attained a value of 4.148% packet loss, which is lesser than all the existing techniques. In figure 6 c), the evaluation of the access control systems is portrayed with respect to throughput. The value of throughput attained by the devised COOT Keygeneration technique is70.317bps, but the existing techniques, namely Authentication and key agreement, multilevel authentication, ODOB and Block chain-based access control protocolachieved the throughput value of 62.209bps, 63.688bps, 66.370bps, and 67.818bpsonly for time 20sec.



a) **b)**

c)

Fig.6. Evaluation of the techniques based on a) delay b) packet loss rate and c) throughput with 100 nodes.

6.4. Comparative Discussion

In this section, the assessment of the devised COOT Keygeneration is carried out by comparing it with existing techniques based on end-to-end delay, packet loss rate and throughput considering 50 and 100 nodes. Table 1 illustrates the comparative discussion of the devised COOT Keygeneration method. From the table, it can be inferred that the introduced COOT Keygeneration method of access control attained a minimum value of end-to-end delay at 0.072 sec, which is due to the usage of Block chain network for communication. The utilization of COOT Keygeneration method accounts for the minimal value of packet loss rate achieved at 0.883% which indirectly contributed to the high value of throughput at73.547bps.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 07, July-2022

Table 1. Comparative discussion of the block chain based access control methods in IoD

Methods	Using 50 nodes			Using 100 nodes		
	End-to-end delay (sec)	Packet loss rate (%)	Throughput (bps)	End-to-end delay (sec)	Packet loss rate (%)	Throughput (bps)
Authentication and key agreement	2.172	2.568	63.209	2.561	3.153	63.644
Multilevel Authentication	1.524	2.718	65.551	1.938	4.261	64.207
ODOB	0.870	2.00	70.493	1.268	2.434	69.178
Block chain-based access control protocol	0.688	1.619	72.014	1.070	3.288	70.780
COOT Keygeneration	**0.072**	**0.883**	73.534	0.448	1.518	**73.547**

7.CONCLUSION

The utilization of drones in varied fields requires transmission of data over open access networks, which make them vulnerable to malicious attacks. Hence, the need for developing secure schemes of data transmission in IoD arises. In this paper, an efficient key generation method is proposed for performing access control in IoD. The technique uses a block chain based network for performing communication and is implemented in various phases, such as Pre-deployment, registration and authentication, D2D access control phase, Drone to server access control phase and Emergency access control phase. The access control phases require the need of a key to initiate communication, and hence a Coot algorithm based key generation technique is developed for generating the key in the D2D and server phases. The introduced COOT Keygeneration based Access control in IoD is evaluated for its performance using various metrics and is found to have produced superior performance by attaining low values of delay and packet loss rate at 0.072sec and 0.883%, along with maximum throughput of 73.547 bps. In future, the performance of the technique will be enhanced using other hybrid optimization algorithms.

Subhadra Perumalla received the MTech degree in Computer Science Engineering from JNTU College of Engineering,Hyderabad, India and pursuing the PhD in
Computer Science and Engineering from the JNTU Ananthapuram, India.
She is currently working as an Associate Professor in Vignana Bharathi Institute of
Technology, Hyderabad. Her current Research interests include network security, image processing, Block chain,remote user Authentication, internet of things (IoT).

Dr.Santanu Chatterjee is currently working as Senior Scientist inDICT, at RCI (DRDO), India.He has received his PhD in CSE from Jadavpur University, in the area ofWireless Sensor Network's Security. He received M.E.and B.E. in Computer Science and Engineering from the Jadavpur University and Burdwan University respectively.His current research interests include Applied Cryptography, Security in IoT,WSN&Network Security,Data Mining etc.He has published almost 30+ research papers in various reputed International Journals and conferences and also working TPC Member for Various Conferences and Reviewer for various International Journals. Presently he is supervising four PhD Scholars and one has already awarded.He has received various awards including CSI Excellent Contribution Award 2015, SAP ACE Award in Nation Building Category 2015, CSI e-Governance Nihilent Award 2015, and DRDO Technology Group Award 2012 etc.

A.P. Siva Kumar, completed BTech from JNTU Hyderabad,MTech from JNTU Anantapur, PhD from JNTU Anantapur in area of "Information Retrieval And Cross Lingual Intelligent Systems" in year 2011. Out of intense Passion for Teaching in year 2006 joined JNTUA, Ananthapuramu as Associate Professor in the Department of Computer Science and Engineering. He worked in various Administrative positions like Deputy Warden,Placement Officer, Addl. Controller of Examinations of JNTUA University. He currently teaches in the Department of Computer Science and Engineering. His subjects of interest include Data Analytics, Data Ware Housing and Data Mining and Internet of Things. Developed ExaminationManagement Software "JEMS" JNTUA ExaminationManagement System (EMS) which automates various tasks and procedures associated with the pre-examination and the post-examination phases associated with the Examination branch of an Autonomous College. Currently the Software is in live at JNTUACE Ananthapuramu, JNTUCE Pulivendula, Audisankara College,Gudur and KSRM Kadapa. Also, executing one AICTE and one UGC project.Master Trainer of Associate Analytics Trained by Nasscom in association with APSSDC.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 11 Issue 07, July-2022

REFERENCES

[1] Wazid, M., Das, A.K., Kumar, N., Vasilakos, A.V. and Rodrigues, J.J., "Design and analysis of secure lightweight remote user authentication and key agreement scheme in Internet of drones deployment", IEEE Internet of Things Journal, vol.6, no.2, pp.3572-3584, 2018.
[2] Das, A.K., Bera, B., Wazid, M., Jamal, S.S. and Park, Y., "iGCACS-IoD: An Improved Certificate-Enabled Generic Access Control Scheme for Internet of Drones Deployment", IEEE Access, vol.9, pp.87024-87048, 2021.
[3] Srinivas, J., Das, A.K., Kumar, N. and Rodrigues, J.J., "TCALAS: Temporal credential-based anonymous lightweight authentication scheme for Internet of drones environment", IEEE Transactions on Vehicular Technology, vol.68, no.7, pp.6903-6916., 2019.
[4] Bera, B., Chattaraj, D. and Das, A.K., "Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment", Computer Communications, vol.153, pp.229-249, 2020.
[5] Yahuza, M., Idris, M.Y.I., Ahmedy, I.B., Wahab, A.W.A., Nandy, T., Noor, N.M. and Bala, A., "Internet of drones security and privacy issues: Taxonomy and open challenges", IEEE Access, vol.9, pp.57243-57270, 2021.
[6] Alsamhi, S.H., Ma, O., Ansari, M.S. and Almalki, F.A., "Survey on collaborative smart drones and internet of things for improving smartness of smart cities", Ieee Access, vol.7, pp.128125-128152, 2019.
[7] Yaacoub, J.P., Noura, H., Salman, O. and Chehab, A., "Security analysis of drones systems: Attacks, limitations, and recommendations", Internet of Things, vol.11, pp.100218, 2020.
[8] Gharibi, M., Boutaba, R. and Waslander, S.L., "Internet of drones", IEEE Access, vol.4, pp.1148-1162, 2016.
[9] Singh, M., Aujla, G.S. and Bali, R.S., "A deep learning-based blockchain mechanism for secure internet of drones environment", IEEE Transactions on Intelligent Transportation Systems, vol. 22, nol.7, pp.4404-4413, 2020.
[10] Aste, T., Tasca, P. and Di Matteo, T, "Blockchain technologies: The foreseeable impact on society and industry", computer, vol.50, no.9, pp.18-28, 2017.
[11] Yaacoub, J.P., Noura, H., Salman, O. and Chehab, A., "Security analysis of drones systems: Attacks, limitations, and recommendations", Internet of Things, vol.11, pp.100218, 2020.
[12] Michailidis, E.T. and Vouyioukas, D., "A Review on Software-Based and Hardware-Based Authentication Mechanisms for the Internet of Drones", Drones, vol.6, no.2, pp.41, 2022.
[13] Singh, M., Aujla, G.S. and Bali, R.S., "Odob: One drone one block-based lightweight blockchain architecture for internet of drones", In the proceedings of IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 249-254, IEEE, July 2020.
[14] Aggarwal, S., Chaudhary, R., Aujla, G.S., Kumar, N., Choo, K.K.R. and Zomaya, A.Y., "Blockchain for smart communities: Applications, challenges and opportunities", Journal of Network and Computer Applications, vol.144, pp.13-48, 2019.
[15] Aggarwal, S., Chaudhary, R., Aujla, G.S., Jindal, A., Dua, A. and Kumar, N., "Energychain: Enabling energy trading for smart homes using blockchains in smart grid ecosystem", In Proceedings of the 1st ACM MobiHoc workshop on networking and cybersecurity for smart cities, pp. 1-6, 2018.
[16] Perumalla, S., Chatterjee, S. and Kumar, A.S., "Block chain-based access control protocol in Internet of Drones", International Journal of Computers and Applications, pp.1-16, 2021.
[17] Singh, K. and Singh, N., "Multi-level authentication protocol for enabling secure communication in IoT", 2021.
[18] IrajNaruei and FarshidKeynia,, "A new optimization method based on COOT bird natural life model", vol.183, pp.115352, 2021.
[19] Jaafer Saraireh,Haya Joudeh "An Efficient Authentication Scheme for Internet of Things", International Journal of Communication Networks and Information Security (IJCNIS), Vol. 13 No. 3 (2021)
[20] Yassine El Khanboubi,Mostafa Hanoune,Mohamed El Ghazouani," A New Data Deletion Scheme for a Blockchain-based De-duplication System in the Cloud",IJCNIS, Vol. 13 No. 2 (2021)