Securing Multi-rotor UAVs using Blockchain Technology over Confidential Consortium Framework

Hardeep Singh Raike, Aasminpreet Singh Kainth, Ria Ria, Sai Lakshmi Pravallika Samayamanthula

Department of Computer Science

Middlesex College, Western University,

London, Ontario, Canada.

Abstract- UAV is in its initial stage but the day is not far away when our lifestyle will be impacted by UAV (Unmanned Aerial Vehicles). From aerial Photography to mission critical applications UAV has expanded its pawn in every other industry. One of the most exercised applications of UAV is in smart inventories. The supply chain management process can be eased by using UAV as it minimizes the human intervention. However, the more it is included into our lifestyle, the more we have been concerned about the threat of being misused. Hence, there is utmost necessary to secure the UAV environment. As these UAVs are controlled through a ground station it may be vulnerable to attacks such as man in the middle attack, DoS (Denial of Service) etc. So, securing the communication between UAV and ground station(control commands) and securing the data collected by UAVs is a critical issue. Therefore, in order to improve the security in UAVs we have proposed an architecture which collectively uses a framework known as CCF(Confidential Consortium) and Block chain. In this paper along with the proposed solution we have also briefly provided an overview of blockchain along with CCF framework.

1. INTRODUCTION:

We are in the 21st century, and the way technology, industries, and equipment are evolved with the help of incessantly development in each industry. Development of smart homes, smart vehicles to smart factories has surprised the world with the power of emerging ideas. With the help of latest advancement like Artificial Intelligence, IOT (Internet of Things), Machine Learning, Robotics we are in an era where we can think to build smart cities. Take an instance, Big Data analytics and Data science is proven effective in Supply Chain Industry. With its application, people are able to develop a better decision for different activities across the supply chain. In general, it helps to address various inventory task, consumer needs, and sales. Big Data can improve the forecasting, improve inventory management, transportation management, and human resource. Moreover, it provides a holistic approach to optimize and accelerate the complete SCM process [1].

With the advancement of technology we can't overlook the importance of UAV(Unmanned Aerial Vehicles) and it's application. UAV are considered as one of the keys factor in automatic supply chain industry. In the last years, UAVs is proven really useful in many fields like remote sensing (e.g., mining), real-time monitoring, disaster management, border and crowd surveillance, military applications, delivery of goods, precision agriculture, infrastructure inspection or media and entertainment [2,3]. UAV has been used in the past to smart the inventory tasks. It is subjected that UAV operates remotely, can be operated over Computer Network and has susceptible to cyber attacks. Thus, many ambitious solution and papers has suggested the medium which can be secured with the implementation of block-chain model. Blockchain and other Distributed Ledger Technologies (DLTs) are

essential for different industries like military, crypto currency, banking, finance, etc. Because they provide a medium for storing the collected data and they can be shared in a secure channel with the nodes which do not trust each other. The practical application of UAVs is in every industry are incessantly increasing, and it is a prime objective that the complete systems like Autonomous supply chain, Disaster relief which uses UAV technology should be secure.

The following paper is structured as follows: In Section II author discussed about the background related to drones, Raft Algorithm and block chain in industrial applications. In section III author has discussed the research that is already done in this area. In section IV detailed architecture of CCF framework and its components are discussed. In section V author has dig deeper into working of CCF framework. In section VI and section VII scientific contribution and validation of proposed solution is discussed respectively. In section VIII author has explained the future works. Finally, section IX has references.

2. BACKGROUND:

Blockchain:

Blockchain is a sequence of blocks, which holds a complete list of transaction records in conventional public ledger [17]. Each block in the block chain contains the hash of previous block. The first block in the block chain called the genesis block which doesn't have any previous block. A block consists of following part, i.e., block version, merkle tree root hash, timestamp, nBits, nonce, parent block hash.It solely depends upon the size of transactions and size of block, how many transactions one block can hold. BlockChain uses asymmetric cryptography mechanism to validate the authentication of transaction [18]. In any untrustworthy environment digital signature based on asymmetric cryptography is used to validate the transactions.

The main characteristics of block chain are:

1. *Decentralized*: It is completely decentralized system and used consensus algorithms to maintain data consistency in distributed network.As blockchains are decentralized which makes them resistant to Denial of service attacks as there is no single point failure.
2. *Persistent:* As each block contains hash of previous block. So, it's merely impossible to manipulate the blocks because hashes will change if data is manipulated and chain will no longer be valid. This property of public blockchains help in maintaining the integrity of the stored data.
3. *Anonymity:* In the public blockchain each user can interact with the block chain without revealing its true identity. In public blockchain each user interacts with its pseudo anonymous identities. This characteristic of public blockchains make them less accountable. So it is not reliable to use public blockchains in trusted applications like UAVs.

In block-chain the main concern is to reach at the consensus among untrusted nodes. There are different algorithms through which the consensus can be achieved, for example Proof Of Work, Proof Of state, Ripple, Tendermint. However, the above mentioned algorithms are computationally expensive takes a lot of time and resources to reach consensus. Thus, it is not suggested to use in mission critical applications. The one which we are using is RAFT consensus algorithm which is comparatively faster when compared with other consensus algorithms.

Raft Consensus Algorithm:

Consensus is required to achieve agreement upon replicating the data in the ledger by all the nodes in the CCF network. RAFT is one of the most recognized consensus algorithms in which all nodes come to an agreement in lesser amount of time.In CCF network a node can be any of the following states:

1. **Leader:** One of the nodes from the network is elected as a leader and this leader can only interact with the client.
2. **Candidate**: In the beginning of the network, every node will be in candidate state i.e, specifying that nodes are ready for election.

3. **Follower**: Once the leader is elected, every other node other than leader will act as a follower. This follower nodes syncs up the data with the leader node in regular intervals of time.

RAFT uses of the following functions to request votes and log replication:

1. **RequestVotes:** RPC is a function that is sent by the Candidate nodes to the other candidate nodes for requesting votes [4].
2. **AppendEntries:** It is used by the Leader for replicating the data into the log [4].

Raft divides time into small periods of random length. Each period(term) is recognized by an increasing number, called **term number [4]**.

Leader Election:

In the beginning of the network the candidate node which receives the major number of votes will be elected as a leader. Once it is elected as a leader it will start sending heartbeats to every follower in the CCF network. If any of the follower doesn't respond to the heartbeat it means that particular follower node is rising a condition for election, that particular follower node will be turned into candidate and starts requesting votes from the other nodes in the CCF network. This particular node can be elected as a leader if it is having the term number which is greater from all the other nodes in the network.

If none of the candidate receives major number of votes then that term ends with no leader, this condition is known as split vote. It uses randomized election timeouts in order to make sure split votes are rare.

Log Replication:

After leader has been elected every request from the client to any other nodes in the network is redirected to the leader. If the leader receives any data from the client it will first append the data to its log and sends the requests to the follower nodes before committing to the ledger. If the leader receives confirmation from the majority number of follower nodes then data is replicated to the ledger. When the followers receives the next heartbeat from the leader, they will also commit the data.

3. RELATED WORK:

As the UAV applications rely on different technologies like image processing, cloud computing, artificial intelligence and using multiple sensors to collect data and sharing the data with base stations. It becomes important to secure the communications among drones, between the drones and control stations. Further it is equally important to secure the data collected and control commands of the UAVs to protect from different attacks. As when UAVs became technologically and economically feasible solution for a variety of tasks, many research papers have proposed solutions to secure drones and methods of communication among them. The work can be primarily classified into two types

- Securing the communication between drones and its base control station.
- Securing the data collected by UAVs and Control station commands.

The authors of [15] have explored different security vulnerabilities in UAVs and conducted an experimental study of the countermeasures to make UAVs secure from these attacks. Different approaches have been proposed to achieve the above-mentioned objectives. The [6] have proposed hardware-based solution by using embedded Secure Element (SE) and [7] have proposed a protocol to secure the communication. The [8] have considered different behaviours of hijacked Drones and proposed a technique to secure UAV networks using Blockchain inspired trust policy, thus improving the security of UAV networks. The [9] have proposed to use encrypted channels for the authentication system and used this encrypted channel to secure communication between middleware, UAV and base stations to protect UAVs from Cyber attacks. In [10], author have reviewed the use Deep learning techniques for obstacle detection and avoiding collision to physically secure a drone. The related works to secure UAVs and its communication networks include hardware-based solutions, cryptographic techniques, trusted secure distributed systems and Deep learning techniques. In [11], the authors have proposed a solution to secure to UAV network by removing the nodes with malware by

correctly detecting the attacks using detection mechanism based on the Bayesian game model

The author of [12] have proposed a solution based on blockchain-base structures. In this solution each UAV will be part of blockchain based network called "UAVNet" as shown in Figure 1. and will have functionality of creating and reading blocks. However, UAV are resource constrained devices and Blockchain consensus mechanisms are computationally expensive. The authors of [13] have explored the use of blockchain technology in securing the internet of things and have proposed a model for securing IoT using blockchain. Specifically, they have explored how blockchain based solution can help in securing the communication between different IoT devices, authentication of users and configuring the IoT devices. In their solution they have used of blockchain's distributed ledger to store the public keys and used cryptographic principles to achieve above mentioned security aspects. They have also established framework for trusted and secure configuration of IoT devices by hosting the configuration files on distributed ledger**.**

Another project called Hyperledger by Linux foundation has striven to improve Blockchain technology's performance and reliability. This framework provides a platform for developing permissioned and private blockchain. The authors of [14] have explored the Hyperledger fabric and proposed its application to increase security in swarm of UAVs. The authors of [16] have proposed a solution called DroneChain utilizing blockchain and cloud server to preserve the integrity of the data collected by drones and to secure communication between UAVs and control station. The authors of [5] have developed a decentralized system and a protocol called Autonomous Intelligent Robot Agent protocol. This protocol formalizes the communication and data exchange between robotic agents and Ethereum blockchains smart contracts.

Many different industries are also researching on the use of blockchain to securing UAV operations. Monitoring of UAVs airspace is another area where blockchain systems are researched in UAV industry. A company named Distributed sky has proposed a universal and integrated Air traffic control system powered by public Ethereum blockchain to monitor UAVs [13]. Another company named chronicled has developed a prototype solution to use Cryptographic microchips as identifiers for UAVs and use IoT connected chip reader device to check for UAVs unique signature in blockchain network to authenticate UAV for Package delivery [13].

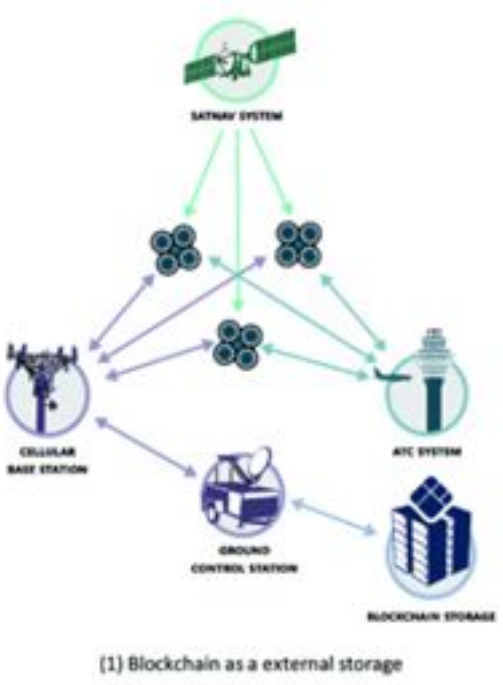


Fig 1. Blockchain as an external storage

4. BRIEF DESCRIPTION OF THE COMPONENTS USED:

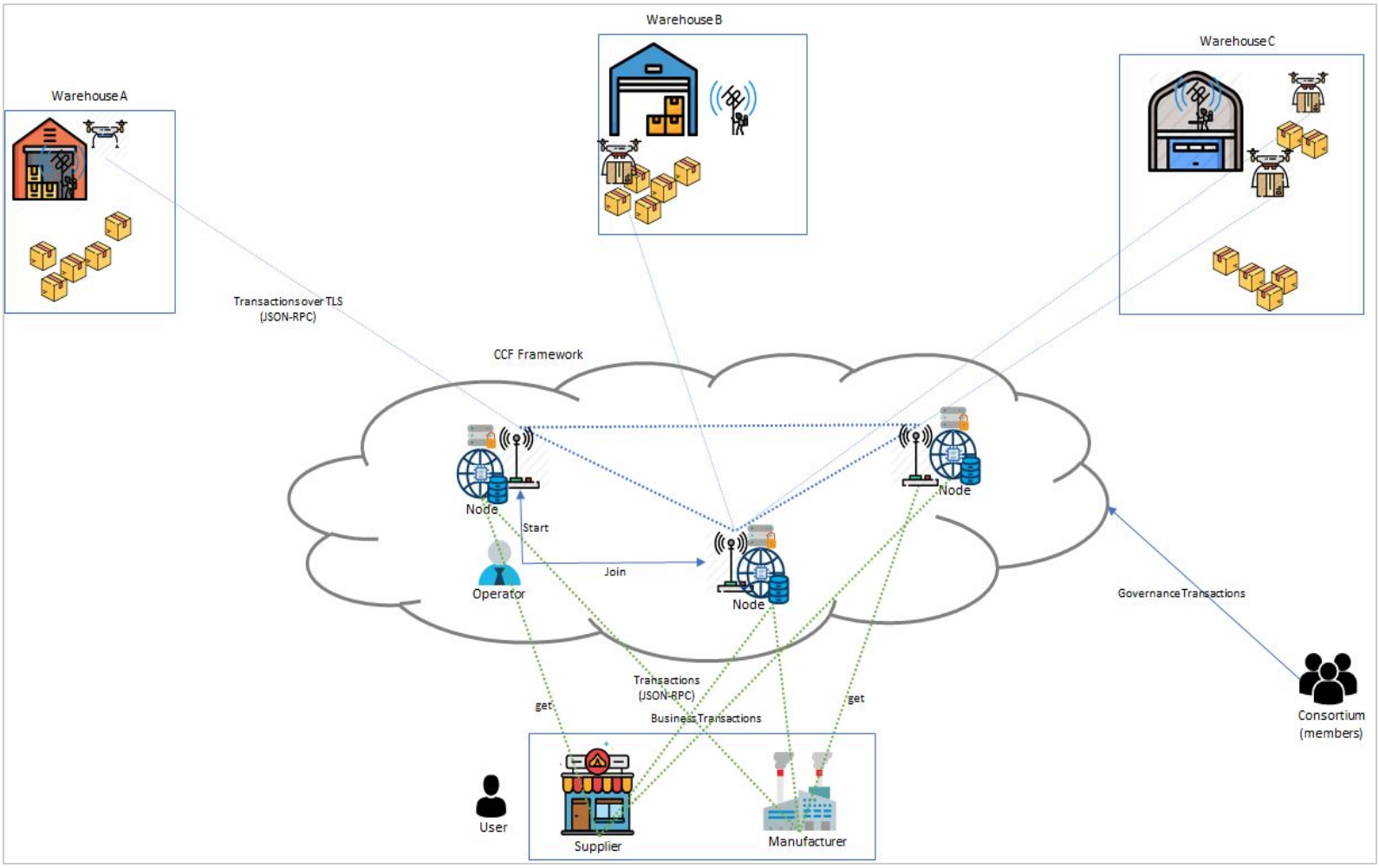


Fig 2. The Architecture of the model

COMPONENTS

Clients We have 3 clients in our model which are Operators, Users and consortium members. These clients uses JSON-RPC format over TLS (Transport Layer Security) to interact with CCF. Where, JSON-RPC is a remote procedure call protocol encoded in Javascript Object notation and, TLS is a cryptographic protocol that provides end-to-end communications security over networks and is widely used for internet communications and online transactions. It is an IETF standard made to prevent tampering, eavesdropping, and message forgery.

Operators are responsible for operating a CCF network for the tasks like adding or removing nodes. Nodes are run and maintained by operators. The identities of operator are not registered in our framework.

Users are the components which can directly interact with the transaction engine(nodes) running in our model. Users public identity should be voted in by members before they are allowed to issue any requests. Similar to the clients, our users uses JSON-RPC format over TLS (Transport Layer Security) to interact with nodes. In our model, Suppliers, Manufacturers and drones act as users.

The **multirotor drone** has **antenna** to communicate with nodes and the control stations at the warehouse. It has RFID reader attached to support the application of reading the tags where **RFID i.e Radio-frequency identification** uses electromagnetic fields to automatically identify and track tags attached to objects. The tags contain electronically stored information. Unlike a barcode, the tags don't need to be within the line of sight of the reader, so it may be embedded in the tracked object.

Members constitute the consortium governing a CCF network. In our model, consortium is an alliance of business companies, individuals, or other entities that got together to achieve a secure environment for the drones and nodes to work. A Member must follow the constitution(i.e. the set of rules and conditions written as a Lua scripts) for their proposals to be accepted. For example, in the CCF network governed by *4* members, a strict majority **constitution** would only execute proposals once *3* members have voted for that proposal where each Member has a unique proposal id.

The **node** consists of Open Enclave Engine for the hardware security, Distributed Ledger to maintain the records and Private Network for communications. All nodes in our model are connected to each other and they constantly exchange the latest data with each other so all nodes stay up to date.

Open Enclave Engine is a template generation tool that protects the confidentiality and integrity of the data and code while it is being processed in the public cloud. It defines the private region of memory i.e. the secure area of a main processor. Here, in our model, we are working with intel SGX which is referred as the software guard extension. Intel Software Guard Extensions are a set of instructions that increases the security of application code and data, giving them more protection from disclosure or modification where, developers can make enclaves, which are areas of execution in memory with more security protection, to partition sensitive information.

Distributed Ledger is a database that will be consensually(collectively) shared and synchronized across multiple nodes. It stores information about the RFID tags on the boxes placed at different warehouses. So by observing the ledger, Manufacturers and supplier may come to know about the demand and supply of particular box at the particular warehouse.

5. DETAILED DESCRIPTION OF THE PROPOSED SOLUTION

As drones are mission critical and it is not feasible to utilize the public blockchains. Hence, a framework is needed which reduces the computation overhead from the ledger and smooth the process of computation. The recent development of CCF framework by Microsoft which helps to meet both of our requirements, that are latency of transmission and security. In a public blockchain every pseudo-anonymous node can be part of the network and have complete access of the ledger with ability to participate in consensus mechanism. In contrast to public blockchain, the CCF framework proposes a blockchain consortium network backed with TEEs. The Confidential Consortium Framework (CCF) have utilised the decentralised systems concepts, Cryptography and TEEs to propose a framework to develop blockchain networks suitable to enterprise computation demands.

The motivation behind this solution lies in the fact that the majority of the applications like Autonomous delivery, Surveillance and disaster relief UAVs work in distributed setup with multiple stakeholders. It is likely that in most of the use cases UAVs may be working in collaboration with other IoT devices, Software systems and Air Traffic control system. So, the data collected by UAVs as well as data regarding the flying schedule and navigation path may be accessed by multiple devices located at different geographical regions. Blockchain can serve as an effective way to provided trusted, immutable and reliable access of this data to multiple users (devices, software systems and organizations). However as already explained the security of public Blockchain lies in the fact that it is computationally expensive to add block which contains data in form of transactions. But as UAVs are mission critical and the use of public blockchain with computationally expensive consensus mechanism like Proof of Work can lead to poor performance and serious repercussions. So, to effectively utilize blockchain and its

principles to make systems secure a framework is required to effectively decrease the latency without compromising security. The CCF framework inherent design of this framework gives application developers flexibility in terms of the identity generation mechanisms, encryption algorithms, and consensus mechanisms to be used on the blockchain network.

The following paragraph explains the detail Architecture for the UAV application with CCF framework. The architecture for the proposed model is shown in Figure 2. All the elements in this model are individual explained in Section 4. Here we will explain the working of the model. First and foremost, the identity of consortium members is generated. The CCF framework provides Member RPC API to generate the identity of members which will include a public certificate and private key for each of the member. The stakeholders in any use case scenario of UAV will act as consortium members with tunable power and will make the decisions. The stakeholders varies with the application as the decision making body changes. These stakeholders will govern the distributed blockchain network with predefined governance rules in a constitution written in Lua Script. The consortium members will submit a proposal to make any changes like adding new node to run transaction engine, opening the network for UAVs, warehouses to make requests to store data, adding new users like UAVs, Control stations to the network and decision is made once the quorum of members has accepted the proposal.

Once the identity of stakeholders(consortium members) is generated the operators will run the nodes which are distributed across geographically different locations as per application requirements. Any node can join an unopened network, but to join an already opened network consortium members must vote for a proposal. These nodes will host application on the server over trusted execution environment (TEE) and this application can be triggered by multiple UAVs, client application run by different suppliers and manufacturers to store and access data from the encrypted ledger. Only trusted UAVs and client application can make request to the application. The identity of each UAV and client application will be generated by CCF framework API and will be identified by public certificate and private key. The CCF framework provide a master secret to generate the public certificate and other encryption keys. Once the identity of trusted users including UAVs and other clients is generated and voted for, than network is opened to them to make JSON RPC requests over TLS to access the encrypted ledger to commit new data or access the already existing data. For example in SCM application the Autonomous UAV on completing delivery will update the ledger with corresponding transaction thus making this data available to all the other users and warehouses. Each transaction committed to ledger will be signed by its private key leading to accountability and signed evidence for any possible malicious activity.

This communication between users which include UAVs, client-side applications, base control station will take place over TLS and encrypted using public and private encryption keys to prevent any “Man in the middle attack”. Once the data send by UAV or any other client is received the node closest to the requester then consensus algorithm will be used to replicate this transaction in ledger over the entire consortium based blockchain network. As the root of merkle tree in the ledger is periodically signed by the leader node the integrity of the ledger is preserved. The traffic between the nodes will be symmetric using Diffie Hellman key exchange. The data is only replicated once confirmation is received from majority of nodes as explained in RAFT consensus algorithm. Other consensus mechanism like PBFT(Practical Byzantine fault tolerance) can also be used. This reliable and immutable data can be used by any stakeholders as manufacturers, suppliers and other warehouses in autonomous delivery application. Similarly in case of disaster recovery application the data regarding flying path of drones can be accessed by Air Traffic control station. The network certificate generated when creating first node will act as certificate authority when distributed to UAVs and control stations for the TLS connection. Further it is possible that a UAV may be controlled malicious actor and can be used to affect the integrity of the data store but in the consortium based blockchain the members can use proposal to revoke the membership of the affected UAVs. For revoking the access rights consortium members will use proposal and voting mechanism. So in this way a trusted and accountable blockchain network is established.

6. SCIENTIFIC CONTRIBUTIONS:

It was early 1990, when first drone was launched from that era to this epoch the drones or Unmanned aerial vehicles got high demand in each and every Industry. Whereas, in the early years of development like 1990, the drones application was limited to Military. Whilst, today every other industry is somehow trying to use drones for automation, surveillance, shipping, delivery, aerial photography, crowd surveillance, disaster management, agriculture to inject pesticides, and weather forecast. In a nutshell, it is considered that drones has eventually become the powerful instrument in various applications.
While we have different successful UAV applications and it is being considered that scientists are looking to improve the different aspects of UAV technology.Their prime areas of concerns are security, reliability, and efficiency. As drones are considered to collect the data from assigned sources it is suspected that drones can be hijacked or hacked. Thus, in any application the communication channel between the drones and the third party needs to be secured, i.e., channel needs to be reliable. On the other hand, while imposing security certainly there is a high possibility that user has to compromise with latency. However, we cannot compromise on latency. Thus, we need the best of both worlds.

Hence, this article deals with the following contributions:

- As per our literature review this is one of the finest articles which deals with security and throughput at the same time.However, we are unable to find any other article which Utilize Consortium Framework to implement drone ecosystem.

- As CCF framework provides an opportunity to use distributed ledger. Hence, enable the system to avoid single failure.

- As all the users are already known there are least chances of any anomaly. In CCF framework every user has a private certificate and if they want to register to a network they should have the network certificate.

- Moreover, the consensus algorithm which we have used is quite faster as compared to existing algorithms. Hence, we don't need to compromise on the throughput as we have evaluated the performance.

Moreover, as per our analysis existing literature review just define the block chain can secure the UAV system but the solution proposed by the authors is too fancy to implement..

7. VALIDATION OF THE PROPOSED SOLUTION:

The proposed solution can be validated in terms of security as well as latency.

Security Analysis of the solution:
As the data submitted by the UAVs and other users is stored in a distributed encrypted ledgers in the consortium based blockchain network. This data store has the following security characteristics :

Tamper-Resistance and Accountability:
Tamper resistance refers to tampering of any entity in the network such as application code running on the node, data stored in the ledger etc. In the proposed solution any information that is stored in the distributed ledger cannot be altered after the block is generated because the each block contains the hash of the previous block and changing the one blocks data will make entire chain invalid. Further as the transaction is also signed by the UAV and then it is sent for approval and verification to all the nodes in the CCF network. This leads to accountability for actions. If any compromised UAV is used by any malicious actor to alter the information in any of the block, its identity will be known by all the nodes in the CCF network because the UAVs and other users are required to sign the transaction by its private key so the entire system is accountable and permission of such UAV can be revoked.

Resistance to DDoS attacks:
DDos is known as "Distributed Denial of Service" attack. It means compromising the whole network or application

server by flooding requests of illegitimate user and making the system unavailable to the actual users. In our solution the node are distributed at multiple locations making it a decentralized system. If an attacker compromises some of the individual nodes in CCF network even though block chain can work with the remaining available nodes in the network. In order to be a successful attacker, attacker should have sufficient computational resources to compromise the large CCF network of nodes. The larger the CCF network, harder to have a successful DDos attack [5].

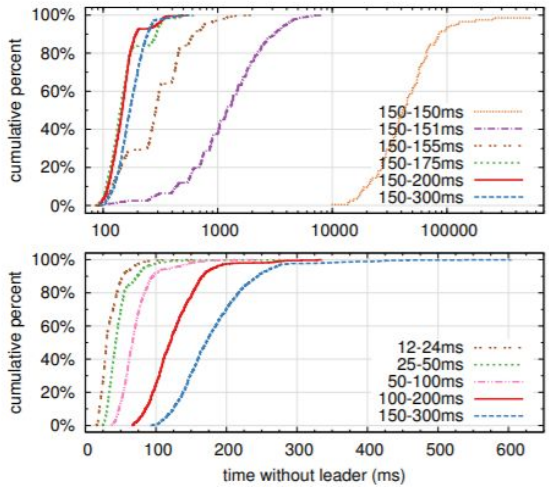
Consistency and Confidentiality:

Consistency refers to that every node in the network have the same state of the ledger at the same time i.e, containing the same data at any point of time. Blockchain follows strong consistency mechanism. Strong consistency mechanism states that, if suppose a read/write operation is requested while a current transaction is taking place the requested operation waits until the current transaction is replicated in the ledgers of all the nodes in CCF network avoiding the return of stale data [5]. Further the data stored in encrypted form in the ledger so it ensures that confidentiality of any sensitive data collected in maintained.

Analysis of RAFT (Consensus Algorithm):

As RAFT algorithm is used for the consensus mechanism in our solution to replicate the transactions made by UAVs, Control stations or other user like Web Clients, over every node in the network the following section analyses its performance in terms of latency in different operations**.**

RAFT algorithm provides highest throughput and low latency. Time complexity of RAFT algorithm deals with two important things i.e, time taken by the algorithm to elect the leader and the downtime taken by the algorithm after the leader has been crashed or timed out. One of the authors provided a detailed explanation for performance of RAFT through an experimental analysis. In the experimental analysis, in order to measure leader election, author repeatedly crashed the leader of a cluster of five servers and timed how long it took to detect the crash and elect a new leader and to encourage the split vote condition leader has been crashed randomly in a uniform manner within the time of heart beat [4].



The above figure depicts time to detect and replace a crashed leader.The first graph shows the variation of amount of randomness in election timeouts, and the second graph scales the minimum election timeout. Each line represents 1000 trials (except for 100 trials for “150–150ms”) and corresponds to a particular choice of election timeouts; for example, “150–155ms” means that election timeouts were chosen randomly and uniformly between 150 ms and 155 ms [4].

So, from the top graph it is clear that if the election is randomized uniformly split vote conditions are avoided or else the leader election took an approximate time of 10 milliseconds with a mean downtime of 287 milliseconds. If the randomness is increased it results in the worst case behavior of the algorithm which takes a time of 513 milliseconds to complete 1000 trails. From the bottom graph it is evident that downtime can be reduced by reducing the election time out.

If the election time out is between 12 and 24 milliseconds, it takes an average time of 35 milliseconds to elect a leader.So, to conclude the worst case time for electing a leader would be around 153 milliseconds.
Having analysed consortium based blockchain and RAFT algorithm in detail we have decided to use both the techniques for the sake of consistency, tamper-resistance, DDoS and consensus that they provide. Through Blockchain, we attain good consistency, tamper-resistance and DDoS while RAFT algorithm

provides a good consensus in less time (around 153 milliseconds in worst case).

8. POSSIBLE FUTURE WORK:

As future work, the defined model could be used in real world supply-chain drone delivery management system as this model is secure and attains less time overhead. The model can be proven beneficial for large companies such as Amazon, Walmart, etc. for faster and secure delivery of items to warehouses, and customers. As far as this model is only concerned with storing the RFID tags information, where there are different possibilities to use the model in different application, let's take an instance, the framework can be used to send the GPS locations of the drones so that we can remotely observe the activity of the drones in the warehouses. Also, many other applications like disaster management, weather forecasting, terrain exploration can be explored further. This prototype can be used by future researchers to check the reliability of CCF framework. .

9. REFERENCES:

[1] Fernández-Caramés, T., Blanco-Novoa, O., Froiz-Míguez, I. and Fraga-Lamas, P. (2019). Towards an Autonomous Industry 4.0 Warehouse: A UAV and Blockchain-Based System for Inventory and Traceability Applications in Big Data-Driven Supply Chain Management. Sensors, 19(10), p.2394.

[2] Blanco-Novoa, Ó.; Fernández-Caramés, T.M.; Fraga-Lamas, P.; Vilar-Montesinos, M.A. A Practical Evaluation of Commercial Industrial Augmented Reality Systems in an Industry 4.0 Shipyard. IEEE Access 2018, 6, 8201–8218.[CrossRef]

[3] Wohlgemuth, W.; Triebfürst, G. ARVIKA: Augmented Reality for development, production and service. In Proceedings of DARE 2000, Elsinore, Denmark, 12–14 April 2000.

[4]GeeksforGeeks. (2019). Raft Consensus Algorithm - GeeksforGeeks. [online] Available at: https://www.geeksforgeeks.org/raft-consensus-algorithm [Accessed 17 Dec. 2019].

[5]Arxiv.org. (2019). [online] Available at: https://arxiv.org/pdf/1903.07602.pdf [Accessed 17 Dec. 2019].

[6] R. N. Akram, P. F. Bonnefoi, S. Chaumette, K. Markantonakis, and D. Sauveron, "Secure autonomous uavs fleets by using new specific embedded secure elements," in 2016 IEEE Trustcom/BigDataSE/ISPA, Aug 2016, pp. 606–614.

[7] J. A. Steinmann, R. F. Babiceanu, and R. Seker, "Uas security: Encryption key negotiation for partitioned data," in 2016 Integrated Communications Navigation and Surveillance (ICNS), April 2016, pp. 1E4–1–1E4–7.

[8] Iván García-Magariñoa, Raquel Lacuestaa, Muttukrishnan Rajarajanc, Jaime Lloret "Security in networks of unmanned aerial vehicles for surveillance with an agent-based approach inspired by the principles of blockchain," Ad Hoc Networks, 01 April 2019, Vol.86,pp. 72-82.

[9] K. Yoon, D. Park, Y. Yim, K. Kim, S.K. Yang, M. Robinson, "Security authentication system using encrypted channel on UAV network" in Robotic Computing (IRC) IEEE International Conference on, IEEE, 2017.

[10] Paula Fraga-Lamas, Lucía Ramos, Víctor Mondéjar-Guerra and Tiago M. Fernández-Caramés, "A Review on IoT Deep Learning UAV Systems for Autonomous Obstacle Detection and Collision Avoidance" Remote sensing, 1 September 2019, Vol.11(18)

[11] H. Sedjelmaci, S.M Senouci, N. Ansari, "Intrusion detection and ejection framework against lethal attacks in UAV-aided networks: a Bayesian game-theoretic methodology" in IEEE Trans. Intell. Transp. Syst., 18 (5) (2017), pp. 1143-1153

[12] Madhusudan Singh, Abhiraj Singh, Shiho Kim , "Blockchain: A Game Changer for Securing IoT Data", 2018 IEEE 4th World Forum on Internet of Things, May 2018.

[13] "Drones + Blockchain = Combining Two Exciting Technologies | Projects Around World,"

dronesonvideo.com, URL: http://dronesonvideo.com/drones-and-blockchain-technology

[14] Isaac J. Jensen, Daisy Flora Selvaraj, Prakash Ranganathan, "Blockchain Technology for Networked Swarms of Unmanned Aerial Vehicles (UAVs)" 20th IEEE International Symposium on A World of Wireless Mobile and Multimedia Networks, WoWMoM 2019, June 2019

[15] Vishal Dey, Vikramkumar Pudi, Anupam Chattopadhyay and Yuval Elovici, "Security Vulnerabilities of Unmanned Aerial Vehicles and Countermeasures: An Experimental Study". IEEE International Conference on VLSI Design, 2018, pp. 398-403

[16] X. Liang, J. Zhao, S. Shetty and D. Li, "Towards Data Assurance and Resilience in IoT using Blockchain ", IEEE Military Communication Conference, December 2017, pp.261-266

[17] D. Lee Kuo Chuen, Ed., Handbook of Digital Currency, 1st ed.Elsevier, 2015. [Online].Available: http://EconPapers.repec.org/RePEc:eee:monogr:9780128021170

[18]NRI, "Survey on blockchain technologies and related services," Tech.Rep., 2015. [Online]. Available: http://www.meti.go.jp/english/press/2016/pdf/053101f.pdf