Blockchain-based Secure Delivery of Medical Supplies Using Drones

Muhammad Asaad Cheema[a,*], Rafay Iqbal Ansari[b], Nouman Ashraf[c], Syed Ali Hassan[a], Hassaan Khaliq Qureshi[a], Ali Kashif Bashir[d], Christos Politis[e]

[a] *School of Electrical Engineering and Computer Science (SEECS), National University of Sciences Technology (NUST), Islamabad, Pakistan.*
[b] *Computer and Information Sciences Department, Northumbria University, Newcastle, United Kingdom.*
[c] *Telecommunications Software and Systems Group (TSSG), Waterford Institute of Technology, Waterford, Ireland.*
[d] *Department of Computing and Mathematics, Manchester Metropolitan University, Manchester, United Kingdom.*
[e] *Department of Networks and Digital Media School of Computer Science and Mathematics, Faculty of Science, Engineering and Computing, Kingston University, United Kingdom.*

Abstract

The advantages provided by the drones with regards to three dimensional mobility and ease of deployment makes them a viable candidate for 5G and beyond (B5G) networks. Significant amount of research has been conducted on the aspect of networking for using drones as base stations to provide different services. In this work, we deviate from the traditional use of drones to provide connectivity and explore the delivery of products through drones in the context of maintaining social distancing. However, drone delivery process for critical applications such as delivering medical supplies is vulnerable to attacks such as impersonation attacks and eavesdropping. The security of drone operation is important to save the users from any breaches that can lead to financial and physical losses. To cope with these security issues and to make the delivery process transparent, we propose a blockchain-based drone delivery system that registers and authenticates the participating entities including products (medical supplies), warehouse (medical centers) and drones. To this end, we utilize Ethereum platform for implementation of blockchain and smart contract and

*Corresponding author
Email address: mcheema.msee18seecs@seecs.edu.pk (Muhammad Asaad Cheema)

we present an analysis of different factors that influence the authentication process in terms of time and the number of transactions. Furthermore, to make the communication of a drone with command and control center more secure and robust, we use machine learning (ML)-based intrusion prevention system to detect any impersonation attacks with an accuracy of 97%.
Keywords: unmanned aerial vehicles, blockchain, machine learning, fifth generation (5G) and beyond.

1. Introduction

The number of connected devices have undergone significant growth recently and they are expected to reach billions by 2030. The concept of massive internet-of-things (MIOT) envisions several applications which assist in improving different aspects of our lives [1]. To realize the vision of beyond the 5th generation (B5G) networks, there are several performance metrics such as high data rates, reliability and ultra low latency that need to be maintained for ensuring the desired quality-of-service (QoS). The high data rates and massive connectivity of devices will lead to extra load on the traditional network infrastructure. Moreover, due to the geoghraphical spread of the internet-of-things (IoT) devices, it may not be possible for all the devices to get access to the network. Therefore, several new avenues have been explored for providing connectivity to such devices. One solution that has been proposed is to utilize unmanned aerial vehicles (UAVs) to provide connectivity to the devices.

UAVs have several characteristics such as ease of mobility, that make them a viable candidate for becoming part of the IoT ecosystem. In situations where IoT devices are not able to gain access to the network infrastructure, the UAVs can play a vital role in providing connectivity. UAVs can act as base stations (BSs) to form a UAV cell, where the devices in the cell radius can connect through UAVs to the core network [2]. The major advantage of UAV BSs is the flexibility with which they can provide connectivity in remote locations such as rural areas. However, in this work we explore an additional use of UAVs as

means of delivering packages to customers. A lot of work has been conducted on the connectivity part of the UAVs, but viewing the recent experience of the pandemic and the idea of social distancing, the delivery through drones has gained significant interest of the research community.

In recent times, we have experienced a major threat from the pandemic in the form of covid 19. The authorities have been grappling with the issue of providing essential medicines and self-testing kits to the people. Moreover, the commercial providers have also not been able to serve their customers due to social distancing and restrictions on the movement of people. In this scenario, a drone delivery mechanism can play a vital role in helping to maintain social distancing while easing the pressures on the delivery of products such as essential medicines to the people, especially the vulnerable ones. There is a lot of potential in utilizing drones for delivering essential medicines and testing kits. Testing kits can be delivered to the people through drones and they can be returned to the testing centers without the need for the people to physically visit the centers. The navigation systems have undergone significant improvement in terms of accuracy, which makes drone-based delivery realizable. Moreover, the battery optimization and utilization of hybrid power sources for the drones has improved the hover time significantly. In this whole process it is important to ensure the security and integrity of the data shared over the delivery system. In this work, we explore the use of blockchain for ensuring secure drone-based delivery.

As the utilization of drones increases for delivering packages, the data sent over the delivery management network and the drones themselves will be vulnerable to cyber attacks. The advancements in machine learning algorithms and the advent of AI will make the drone operation more autonomous, hence making it susceptible to hacking [3]. The hackers can cause significant financial damage through manipulating the drone operation by adding in malicious drones to the network or making the drones deliver the product to a malicious user. In the context of drone-based delivery, the major retailers and authorities will be at the receiving end of any loss caused through fraud. In this scenario,

the concept of blockchain borrowed from the cryptocurrencies, can greatly help in reducing the risk of cyber attacks [4]. Therefore, in this work, we propose a blockchain based drone delivery system to make the order management secure as deliveries can be products that are critical in nature, e.g., delivery of medical supplies. Moreover, to stop the eavesdropping drones we utilize an intrusion prevention system based on ML, where any unusual activity by an unwarranted drone is sensed and blocked. To be specific, the blockhain will prevent the addition of any unregistered drones, products and warehouses along with ensuring the traceability. However, once the drone has left the warehouse the drone will be communicating with the warehouse without the involvement of blockchain network during this communication. The blockhain is not utilised during drone flight operation because it incurs additional processing and energy utilisation, while the drones are battery operated and energy conservation is required to prolong the flight time. Hence, the communication during drone flight operation is not secured by blockchain which makes it susceptible to attacks by any malicious users. We utilise the intrusion prevention system to introduce an extra layer of security for drone flight operation.

The rest of the paper is organized as follows. In Section II, we provide a brief overview of related works with regards to drone delivery and blockchain. We also highlight the motivation of this work with regards to supplying critical medicines and testing kits in a pandemic. Section III defines the system model and the ordering process, starting from the order request to the final delivery. In section IV, we present the simulation results, highlighting the impact of different factors on the transactions and authentication time. Moreover, an insight into impersonation attacks is also provided. Section V concludes the paper and provides future research directions.

2. Related Work and Motivation

2.1. UAV (Drone) Delivery

The idea of parcel delivery by drones has gained significant traction in recent times. Amazon Prime air is an example of utilizing drone for logistics, where the packages are delivered to the customers in their homes [5]. Similarly other logistics related companies such as DHL and Federal Express have been exploring the use of drones for parcel delivery. Delivery by drones requires minimal human effort and can lead towards providing a low cost and efficient solution for delivery. The battery limitations can hamper it's operation so it is proposed that the depot or the warehouse from where the fleet of drones operate should be closer to the point of operation. Authors in [6] explore the concept of a hybrid model involving the truck-drone delivery. However, in this work, we assume a dense urban scenario where the depots or warehouses are close to the area of operation and the fleet of drones operates directly from the warehouses. In our case, the warehouse will be the pharmacy or the health facility that provides essential medicines and testing kits to people. In the context of the pandemic, the proposed system can be very beneficial in providing services to the people who are vulnerable and have to maintain social distancing.

The concept of drone delivery also complements the concept of sustainable cities where the delivery through drones will leave lower carbon footprint as compared to the conventional delivery through trucks. One of the initial efforts to introduce delivery service through drones was undertaken by a company called TacoCopter. The idea of this initiative was to deliver tacos in San Francisco through drones. However, due to regulatory issues and security concerns the US Federal Aviation Administration (FAA) disallowed it's use. Drones have been used for both military and non military applications and the idea of delivering food, medicine and general packages is an interesting proposition for retailers [7]. Future holds great prospects for different business opportunities through drone delivery. In this work, we address the security issues related to the drone delivery system and propose a blockchain based framework.

The main advantages of drones include the ease of movement, flexibility and speed. The drones come in various sizes with various battery power capabilities. Their flight time is dependent on various factors ranging form the speed at which they are operating to the payload capacity. The delivery through drones is not affected by the town street planning, which augments its agility as compared to the delivery by trucks. The energy requirements of the drone are impacted by the aforementioned factors, which in turn impacts the hover time. Other environmental factors such as wind and rain can also impact the hover time. In this work, motivated by the advantages provided by the drone, we analyse the utilization of drones for the supply of essential medicines and testing kits to the people. We explain the proposed system model in detail in Section III.

The socio-economic impact of delivery through drones can be huge in the coming times. However, there are several privacy and security issues associated with its use that need to be catered before the idea is rolled out on a larger scale. It is imperative that the along with the economic benefits, the security and integrity of the drone delivery system is ensured. To this end, in this paper we explore the concept of blockchain and ML for intrusion prevention for delivery. There has been considerable research on providing connectivity to the drones as the drones have the capability to use a transceiver mounted on them for transmissions [8]. Moreover, the advancement in localisation techniques and routing protocols has made it easier for drones to navigate through the area and realize the delivery services [9] [10]. Several routing and scheduling mechanisms for drone based networks have been proposed for ensuring an efficient drone flight operation [11]. These works provide the platform for utilizing the drones for parcel delivery. Our focus is on addressing the security aspect of the drone delivery by ensuring that the process from order placement to the final delivery is secured. A brief overview of the blockchain and smart contract is provided in the subsequent section.

2.2. Blockchain, Escrow and smart contract

Ensuring integrity and security of the data has always been a major challenge for the network designers, especially in the era of e-commerce where the online shopping is increasing and a small security breach can lead to huge financial implications. The need for a building a secure network is not limited to any particular field as it has become an essential ingredient for a majority of industries. In industrial IoT networks that are involved in sensitive operations or are collecting data that is sensitive, it is important to ensure security and integrity by auditing the operations carried out [12]. In this context, researchers have proposed different methods to ensure the integrity of the data. One such effort that paved the way for future was introduced in on January 3rd 2009 with the invention of bitcoin by Satoshi Nakamoto. Satoshi introduces the concept of blockchain as a distributed ledger which keeps the record of the different transactions and events by providing the security to the ever growing list of records through the cryptography [13]. The most interesting feature of the blockchain is that it doesn't depend on the single entity or authority as it is distributed, therefore, there is no single point of failure. In order to provide the security, it connects blocks (containing transaction and event information) of the chain in such a way that each block stores the hash of the previous block. In this case, if someone tries to make changes in the ledger they need to make changes in every block all the way to the genesis blocks. which seems like an impossible task to manage.

Blockchain possesses some characteristics which are mentioned as follows:

- Integrity
- Decentralization
- Auditability

These three characteristics of the blockchain have made it quite popular for utilization in cryptocurrencies.

Smart contract is a computer program that replicates the idea of a contract between two or more parties. The term was introduced by a computer scientist named Szabo in the 1990s. The initial idea was to utilise the concepts involved in paper based contracts and developing a digital solution that introduces more features, making the system secure, efficient and trustworthy.

The program binds the parties to the contract in order to ensure successful execution and minimising the risk of parties backing out of the contract[14]. The utility of smart contracts in more pronounced in transactions where there is no third party involved in the transaction as a guarantor and only the parties to the contract establish a smart contract to realize the transaction. The interest and development of blockchain has brought the concept of smart contract at the forefront for applications such as e-voting, medical and banking. The blockchain technology introduced decentralization along with a trusted environment for the execution of smart contracts. The deployment of smart contracts on blockchain makes the contract robust with regards to any tampering, which is due to the fact that the execution of contract is undertaken by individual parties without any centralized control.

The smart contract also ensures that the contract is executed only when certain conditions are met. The cryptocurrency Bitcoin is one of the examples of such a system, where the transactions are approved only if certain preconditions are met [15]. Ethereum is a widely used blockchain platform that is used to develop smart contracts using the Ethereum virtual machine (EVM). EVM provides an environment for dynamic implementation of smart contracts by allowing the nodes in the Ethereum network to run the EVM implementation. The popularity of Ethereum for developing smart contracts is due to the fact that it supports decentralized applications.

Motivated by aforementioned technologies, the aim of this work is to explore the utility of smart contracts for drone delivery of essential medicines and testing kits. The provision of such essential supplies in the pandemic can be managed by drone delivery but the security issues may dissuade the users from using drones. Moreover, it is imperative that the testing kits and the essential medicines are

supplied to the authorised customer and the identification process of each item and every customer is robust enough to avoid security issues. In the subsequent section, we highlight the contributions of this work.

2.3. Drone Security and Contributions of this work

The increase in the applications related to drones has led to an interest in addressing the security aspect of the drone operation. The communication between the BS and the drones can be compromised due to the involvement of any eavesdropping nodes. Physical layer security (PLS) techniques have been explored to secure the wireless links from any eavesdroppers. Identifying the eavesdropper and employing jamming to improve the PLS is one of the techniques that has been explored to secure the communications between peer-to-peer (P2P) wireless links [16]. A drone-based jammer is different from the conventional ground jammers due to it's ability to move in 3D space, making it more effective against jamming eavesdroppers. The cryptographic approaches have not been considered as highly effective for drone-based networks, especially in scenarios where the mathematical model behind the cryptographic approach can be easily determined [17]. Thereby the focus has been directed towards physical layer security that addresses a secure transmission design. The presence of drone jammers provide an apt solution for network environments where the drone base station is transmitting to multiple users in the presence of multiple eavesdroppers.

Most of the solutions with regards to the drone security address the PLS in 2D space, which makes it a simplistic approach towards providing security for drone operation. Providing security in 3D space is more complex as the eavesdroppers can also move in 3D space. The change in the position of malicious nodes in 3D space makes the security aspect more complex. Regular updates regarding the prediction of position of malicious nodes can incur extra overhead and compromise the overall secrecy performance. Moreover, the drones may be flying in high altitude or low altitude, which can impact the secrecy performance [18]. The trajectory of the drones and the transmit power can be optimized to improve the secrecy performance [19]. The trajectory can be de-

signed as such that the transmitter receiver pairs are aligned for transmissions by avoiding transmissions towards any malicious nodes. Moreover, the transmit power plays an important role in determining the secrecy performance. Optimizing the transmit power can ensure that the eavesdroppers cannot decode the transmissions due to the propagation characteristics.

Authentication of drones through radio frequency identification (RFID) is one of the methods that can ensure that only the authorized drones can become a part of the network [20]. The authorization of drones can help in identifying if any eavesdroppers are trying to gain access to the network. However, the RFIDs can be cloned by the nodes to act as legitimate nodes and compromise the security of the network. Blockchain can be utilised to provide secure communications for drones. The authors in [21] present the utilisation of blockchain for secure routing for drones to block the malicious nodes in a drone swarm. Our work focuses on using the blockchain for another application of drones, where the delivery of essential medical supplies is carried out through the drones.

In this work, we propose a blockchain-based drone delivery management system in the context of a pandemic or situations where social distancing needs to be maintained. Our work is different from the aforementioned works on PLS as we motivate the use of blockchain for drone delivery and consider the end-to-end order management system. The aforementioned works don't consider the specific security issues related to drone delivery such as impersonation attacks and authorization. We present a comprehensive model for drone delivery and consider the utilization of intrusion prevention system based on machine learning to identify any malicious nodes. The main contributions of this work are as follows:

- We propose a blockchain-based system for parcel delivery, where all the entities such as drones, warehouses and products are registered over the blockchain.
- We introduce robustness to the drone flight operation by utilizing a ML-based intrusion prevention system to block any eavesdropping nodes from

compromising the communication between the drone and the warehouse.

- We use an Ethereum platform for the deployment of the smart contract with blockhain for carrying out the registration and verification process.
- We present an analysis of different factors that influence the authentication process in terms of time and the number of transactions.

Our distributed blockchain-based proposed model builds the mutual trust between the participating entities and helps in mitigating the denial of service and single point of failure. The registration process is undertaken at the supplier side where sufficient energy resources are available. However, during the drone flight operation the blockchain is not employed for the communication between the drone and the warehouse due to energy constraints at the battery powered UAV. Thus, we utilise a ML-based intrusion detection system to provide additional robustness during the flight operations.

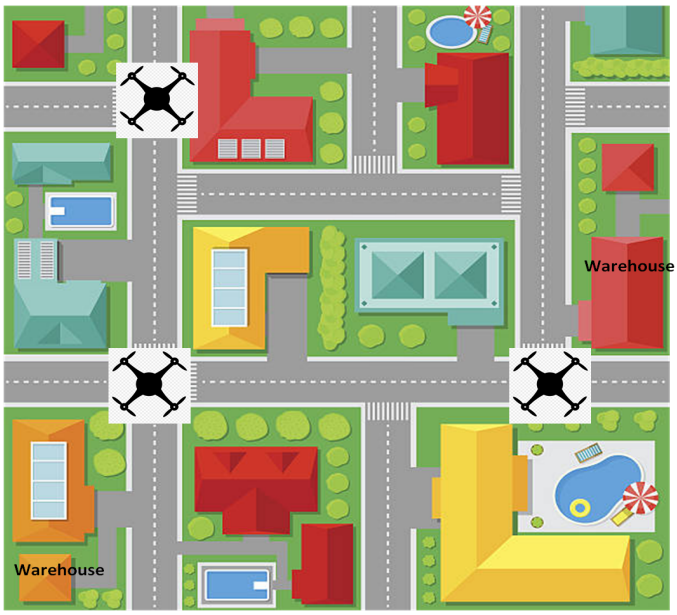

Figure 1: Drone-based delivery

3. System Model

In this section, we present the system model and explain the overall transmission flow, starting form order placement to the final delivery. The model addresses the delivery for medical supplies or testing kits in case of a pandemic or otherwise. Fig. 1 shows the main concept behind the idea, where a dense urban environment is assumed and there are several warehouses (health facilities or pharmacies) in the area. Every warehouse is assigned a fleet of drones according to the demands within the radius of that warehouse. It is assumed that the drones possess the required strength to carry the payload to the customer, where the payload consists of medicines or testing kits. The demand for the particular service is initiated by the customer. In our work, we consider two services that are available to the customers:

- Premimum Service: This service is an urgent service where the order of the customer is give priority. This service can be provided to vulnerable customers or those in need of immediate supply of medicines or testing kits.

- Normal Service: A delay tolerant service where the orders don't need to be delivered urgently. Such service can be provided to customers

Integrity and auditability is necessary while delivering products as the order goes through different steps, starting from order processing at the warehouse and transportation to the customer. The whole process in vulnerable to security issues if a robust mechanism is not put in place to block any malicious requests. For example, an unwarranted drone can sabotage the delivery process. Or the drone can be induced into delivering the product to the unauthorised customer. In our case, as the delivery parcels comprise of medicines and testing kits, it is important that the overall order management is secure and conforms to the GDPR regulations. We need a mechanism that can provide integrity to the delivery process information and can also help us in auditing of supplies. The mechanism should also be able to authenticate the drones to avoid any malicious

drone coming into the network that can sabotage the process by launching different kind of attacks such as impersonation attack. Therefore, we leverage the concept of blockchain and propose a smart contract based mechanism to handle the orders in a secure manner. Later, we also discuss the ML-based intrusion prevention system for blocking malicious drones.

The overall system flow chart describing the order management is presented in fig 2.

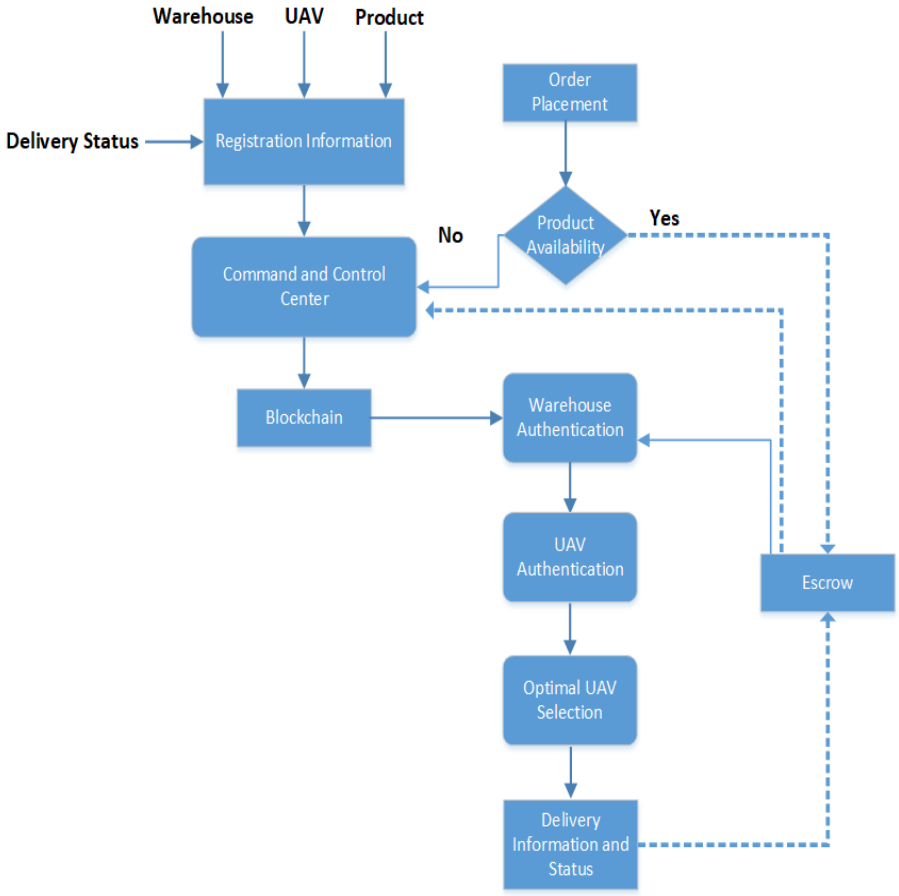

Figure 2: System Flow Chart

As it can be observed in the flow chart, first, we need to register the products on the blockchain. These products can only be get registered if the transaction

is made by the command and control (C & C) centre. If the registration request is not made by the C&C the smart contract would not be able to store data on the blockchain and reject the registration request. Our system comprises of two smart contracts; first one handles the delivery procedures for the products, and the second one deals with the efficient payment procedure. As our model specifically addresses the scenario where the customers are delivered the self-testing kits, we consider that the testing kits are returned by the customers through the same drone. In the sequel, we explain the registration process followed by the product tracking.

3.1. Registration

The first smart contract consists of two main functions. The first function handles the authentication and verification of the UAVs. All the UAVs which are part of the network are assigned with a 20-byte unique address. We mapped the information related to each UAV against this address and store this information on the blockchain. The information that is stored on the blockchain includes the UAV Model ID and information about its flying domain. The smart contract function takes this information as an input and maps it against a 20-Byte Ethereum ID. The gas used by this UAV registration function can be managed by controlling the length of the string information which we are giving as an input to our UAV registration function. If the number of characters used to specify the flying domain and its Model ID are higher then higher will be the gas used by this function. Once we have registered the UAV by using the registration function, we can authenticate our UAVs to verify that if the available UAV is eligible to pick up the product for the delivery or not. In order to authenticate the UAV, all that is needed is the Ethereum address related to UAV that is requesting for the permission to pick up the specified product. This Ethereum address is then matched with the addresses present in the authenticated UAVs address list. A positive match triggers a go ahead for the UAV to deliver the product. This address can also help in identifying if the UAV is flying in its designated area or not.

We have also taken into consideration the fact that an attack can be initiated where the attacker can change the home address of the UAV and make it land at any other place than it's warehouse or the delivery address. This attack can compromise the integrity of the system and can lead to the product being stolen. Especially when we consider medical supplies or testing kits, we want to ensure that any such attacks are identified and the network is robust enough to counter such attacks.

In order to add a layer of security for the UAVs and to keep the product delivery secure, our model stores the UAV home address on the blockchain so that it becomes impossible to change until and unless the such request is authorised by the C&C. A similar process is undertaken to register the products at the warehouses by taking the information as an input of the smart contract and mapping it against unique address which is assigned to it.

3.2. Product Tracking

It is important for the warehouse to keep the track of the product, not only to ensure that the product is delivered but also to update the recipient of the product delivery status. We need a robust mechanism to keep track of the information shared by the UAV that is delivering the product and we want to ensure that the information related to the delivery cannot be modified arbitrarily by any eavesdropper. This is where blockchain comes into play, in order to track the information related to each product which is on route or delivered. The product is considered to be delivered when it is digitally signed by the receiver of the product. We designed a function in our smart contract to handle this type of information related to the product. The function takes the information which includes the departure time of the product when it leaves from the warehouse as well as the arrival time when it reaches some other warehouse or reaches the customer. The function takes this information as an input and maps it against the ID assigned to each product. To make sure that the information is coming from the right source or from the right person, we deploy a check to authorize. If the information is coming from the authorized

source, then the status of the variables related to the product transportation gets updated on the Blockchain. Otherwise the transaction will be denied and the information about the product transportation on the blockchain will not be updated. All the information associated to each product ID can be retrieved from the Blockchain by providing the product ID in the call function designed in our smart contract.

3.3. Escrow Payments

The issues related to monetary transactions can hinder the smooth order management. For example, a customer orders a product but on delivery they refuse to claim the product or can claim that it is not the desired product. In such scenarios, the customer can refuse to pay the dues for delivery. On the other hand, the warehouse can refuse to refund the money on the pretext that the delivery conforms to the order placed by the customer. In such a scenario, to make the system more reliable so that it can be trusted by the customers, we utilize a mechanism for money transfers related to the product. Escrow can be a good solution to these kind of issues [22]. Escrow services are now playing a major role with regards to the blockchain [23]. Escrow acts as a representative for the parties involved in the transaction. It dispenses money or documents as a neutral third party. The money or documents submitted to the Escrow are not released until the conditions of both parties in the transaction are not met.

In our model, the second smart contract is basically an escrow contract to build a trusted method of the payment between the seller and the buyer. In this smart contract the buyer deposits its money to a neutral authority (escrow) to order the product. The authority confirms the order once it receives the money. When the product is delivered from the seller to the buyer and the state variable associated to the transportation of the product gives the confirmation of the product delivery, the neutral authority transfers the deposited amount to recipient, which in our case is the warehouse. In our designed smart contract, only the neutral authority can allow refunds to the buyer. In the instances where the warehouse is late on delivering the product or the quality of the product

is compromised the customer can refuse to accept delivery. In this case, the warehouse doesn't have access to the deposited money and can only get access once the order is being cleared by the customer. The Escrow flow diagram is presented in the Fig. 3.

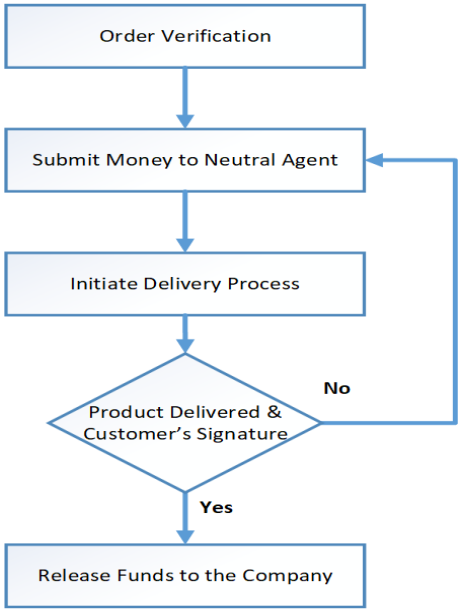

Figure 3: Escrow Flow Chart

4. Simulation Results

In this section, we explain the assumptions of our simulation model and present the simulation results. We assume that the drones have ubiquitous connectivity. The warehouses are spread in the area and are assumed to be close to major delivery areas. The drones are assumed to be possessing the capability to carry the payload. As discussed earlier, two types of services can be requested by the customer: the premium service and the normal service. A significant amount of research has been done on drone localization, making the drone trajectory more and more precise. In this work, we assume that the drones follow the assigned path for delivery.

Fig. 4 provides a block diagram of the registration process, where mapping of different information is done against the Ethereum address associated with the specific UAV. The figure provides the list of functions employed for the order management and storing the information over the blockchain. The flying area (the designated limits of the drone flight), $home_address$ (address of home warehouse where UAVs can return for charging or in case of emergency), UAV_class (provides information about the type of UAV) and the UAV eligibility which is a binary variable highlighting if the eligibility takes the value 'true' or false' depending on if the UAV is registered or not. Once all the information against the associated UAV Ethereum address is stored, the associated address is stored into the array of registered addresses for authentication in future. Other information that is stored is the warehouse location ($WH_Location$), the eligibility of the warehouse with regards to registration. This information is also stored in an array of registered warehouse addresses. The products undergo registration by being assigned with a produce ID (P_ID)and mapping the warehouse at which the product is stored. The quantity and the type of product is also stored as shown in the figure.

After deploying the smart contract, the transactions are sent on personal ethereum blockchain using web interface and observes the gas used by each function. Fig. 5 provides an insightful look at no of transactions a single block can accommodate for registration purposes while having a specific gas limit. The aim is to observe as to how quickly a piece of information can get on the blockchain ledger. Number of transactions which a single block can accommodate is purely the function of the block gas limit. It can be observed that as the block gas limit increases, the number of transactions that a single block can accommodate also increases. From a designer's perspective, this graph provides insights into the magnitude with which the number of transactions increase for different registration function that are part of the smart contract. In our case, the registration functions include the UAV registration, the warehouse registration and the product (testing kit or medicine) registration. The purpose of including the warehouse registration is to ensure that the system is scalable. For

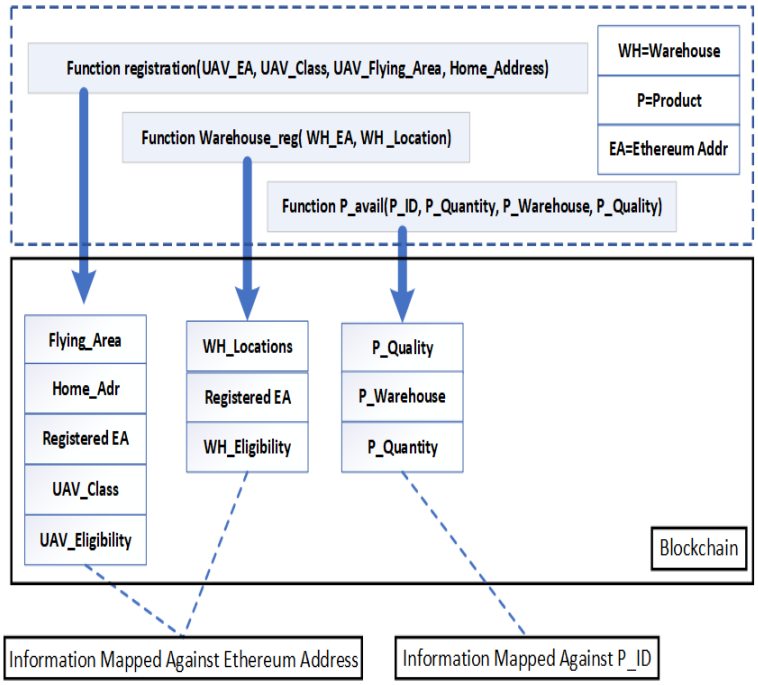

Figure 4: Registration functions flow chart

example, if an ad-hoc warehouses such as mobile health centers or pharmacies are introduced, the proposed solution will initiate the registration process for such additions and also register the corresponding fleet of drones.

4.1. Order Placement Transactions

If we observe the procedure shown in the flow chart in Fig. 2, we can observe the number of transactions required for the delivery of a single product. In our model, a single product delivery will consume two transactions. One transaction for the tracking information and one for the escrow payment(in our model we consider the escrow transactions as a single transaction for the product delivery). If we need to avoid the impersonation, we have to make sure that the true available entities have to request for the authentication by itself so we could be able to verify that entity properly.

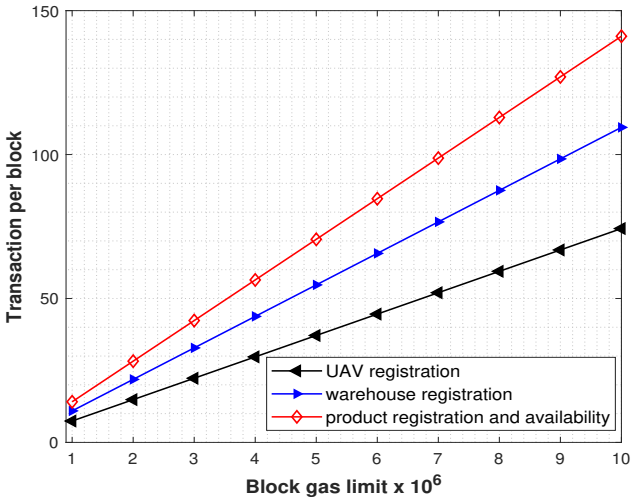

Figure 5: Ethereum Gas Analysis

Fig. 6 shows the rate of increase in the number of transactions increases with the increase in the no of delivery products. Moreover, this figure also helps in analysing the impact on the number of transactions due to any impersonation attacks. It can be observed from the figure that the delivery mechanism, which is tackling with the impersonation attack (a drone can steal information from a registered drone and can pretend as a registered drone using this information) of the drones, require more no of transactions. A new transaction is needed to make sure that drones ready to pick up the product for delivery is providing valid credentials for the authentication. It can be done by adding a new function in the smart contract, which each drone must execute to show its availability for the product before requesting the authentication. Only those drones can get access to the function, which are part of the blockchain network and registered in the first place. This function on the blockchain will consume some gas units, limiting the number of transactions for verification, with a block depending on the block gas limit. If we observe the bar graph for different number of products and block gas, we can observe the increase in the number of transaction required to tackle the impersonation attacks. For instance, if we observe at the number

of products at 100, we can identify that 200 transactions are needed for the case with no impersonation attacks. However, if there is an impersonation attack, the number of transactions for the same block gas rises approximately to 300 transactions. Moreover, Fig. 6 also provides the information about the no of verification requests that each block can accommodate, where such requests are executed by the drones to avoid impersonation.

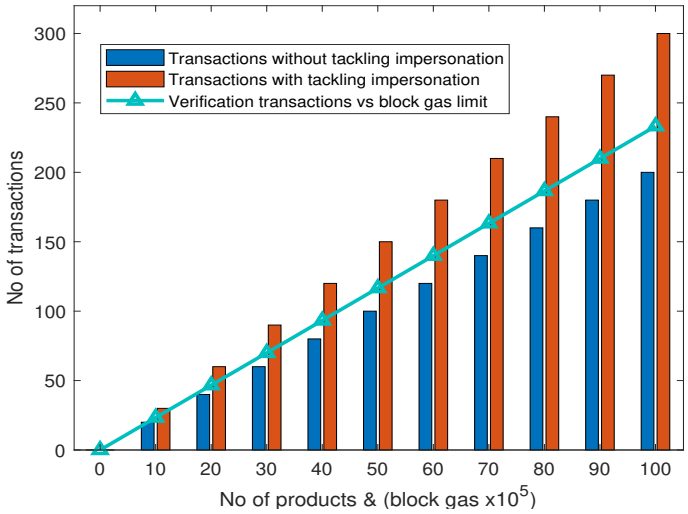

Figure 6: Transactions

In our model, we used the blockchain to not only provide the integrity to our delivery process but also to add a layer of security to our UAVs by providing a blockchain based authentication and verification mechanism. Moreover, we are also storing the home address for each UAV on the blockchain to make it robust against any unwarranted changes. The UAVs only accept the information coming from the C&C. Otherwise, the updation process for the blockchain is not initiated. Additionaly, as mentioned earlier, we also cater to the impersonation attacks. Fig. 7 provides an insight into tackling the impersonation attack. The entity requesting authentication is required to inform the blockchain network by calling a function designed in the smart contract. The entities have to call that function before requesting the standard authentication, where each entity needs

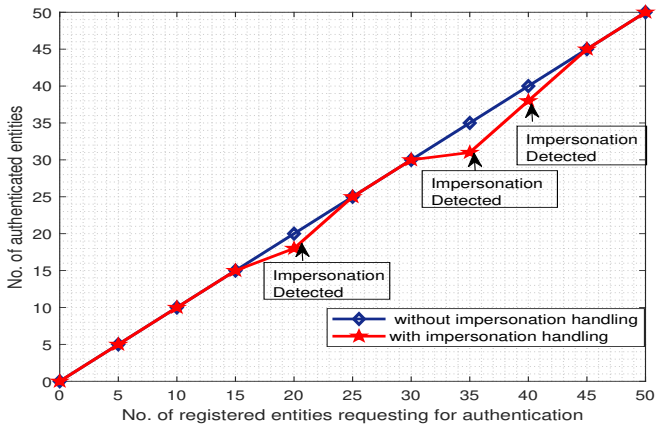

Figure 7: Impersonation Detection

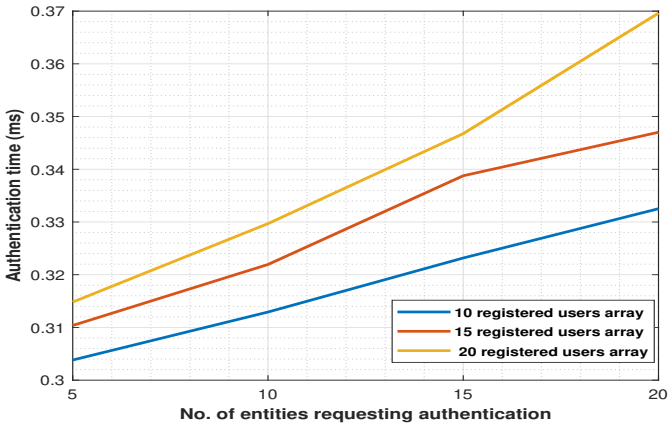

Figure 8: Authentication Time

to provide the information associated with it. It can be observed from the figure that without impersonation handling, all the registered entities can enter into the system, without looking into the entity's identities that are providing the information for the authentication. Once we handle the impersonation attack by adding functions in our smart contract, we can observe from the graph that the system is not allowing all the entities to be authorised, even if they provided the relevant information with regards to the delivery order. Therefore, the proposed

system can detect an impersonation attack.

Fig. 8 provides us the information about the time required to authenticate the requested entities, which depends on the system speed. To authenticate an entity, the provided ID is compared to the list of registered entities to see if the entity is available. In this figure, the authentication time is plotted for different number of registered users array. The registered users array refers to the collection of IDs that are registered in the system, and any authentication request is compared with those registered IDs. It is important to note that the authentication time doesn't necessarily double when the number of registered users array is doubled. For example, if we observe the plot for 10 registered users array at 15 number of entities requesting authentication, we can identify the authentication time of 0.324 ms. Similarly, if we observe the plot for 20 registered users, we observe an authentication time of 0.346 ms. From this figure, it can be seen that authentication time is increasing with the increase in the number of requested entities. This figure is important from a system designer's perspective, providing insights into the authentication time required for a particular scenario involving a particular size of registered users and the numbers of entities requested.

While analyzing the smart contract functions behavior on the public Ethereum network, the transaction fee can be an essential factor as high transaction fees can increase the overall system's cost. The transaction fee is extracted using the gas consumed by each transaction Fig. 9 explains how the combined transaction fees is rising with the increase in the number of transactions. If we observe at number of transactions=30, we can identify that UAV registration incurs the highest transaction fee, followed by warehouse registration and product registration. In the next section, we address the issue of attacks from unwarranted drones to enter the communication network of drones and analyse a machine learning- based attack detection.

4.2. Machine learning based attack detection

Securing the communication between the drones and C&C is also very crucial in order to provide the secure delivery to the customer and to protect our system from external intrusions. In order to detect the intrusion, we utilise the data set for the intrusion detection for the drones given in [24]. This dataset captures the uplink and donwlink traffic and the total traffic flow between drones and the central communication point, which is the C&C in our case. The statistical measures that are extracted from this dataset include mean, median, standard deviation, kurtosis and mean square. We trained different SVM classifiers using different set of settings and compared them to analyze the performance. The aim is to detect any anomalies in the data being generated in the system and detect if the messages are being generated by the drones or an unwarranted intrusion is trying to access the communication.

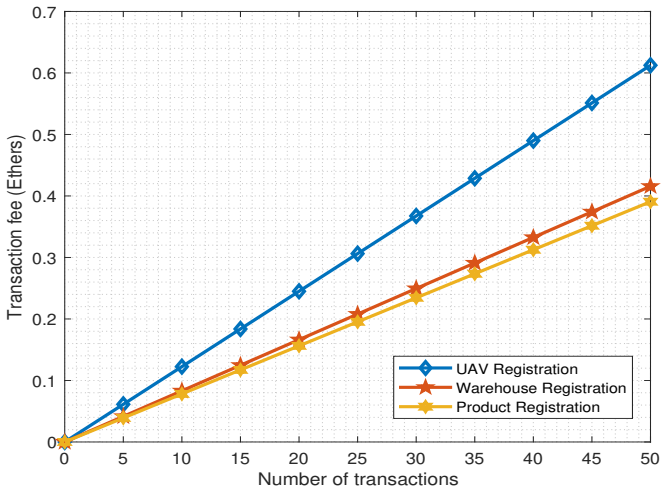

Figure 9: Transactions Fee

Classifier	Accuracy	TPR
Linear SVM	97.0%	96.0%
Quadratic SVM	97.5%	98.0%
Fine Gaussian SVM	97.3%	98.0%
Medium Gaussian SVM	97.5%	98.0%
Coarse Gaussian SVM	97.0%	97.0%

We can observe from the table that the highest accuracy is provided by quadratic support vector machine (SVM) and medium gaussian SVM. We have shown the receiver operating characteristic (ROC) curves for the two classifiers which have shown the maximum accuracy. We also highlight the area under the curve (AUC), where AUC measures the performance of classification in terms of probability, across all possible classification thresholds. It can be observed that the detection of access into the network by any unwarranted drones can be achieved with a high accuracy. This provides an added robustness against malicious drones in the proposed model. This is important in the context of the proposed model, where the critical products such as medicines and testing kits are being delivered. Any malicious intrusion that tries to enter the communication system between drones and the C&C should be detected so that

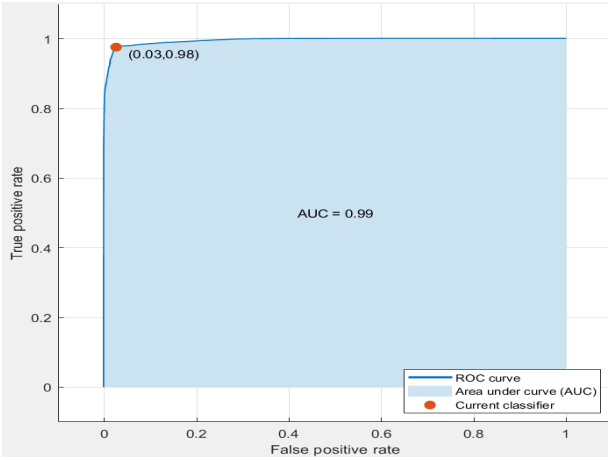

Figure 10: ROC Curve Medium Gaussian SVM

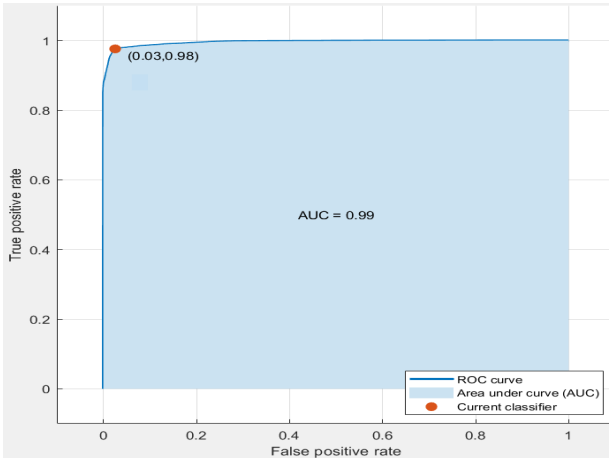

Figure 11: ROC Curve Quadratic SVM

5. Conclusion and Future Directions

In this work, we explore the utilization of drones for product delivery. We motivate the blockchain-based model for authentication and registration to make the delivery process secure and transparent, especially for delivery in critical applications such as medical supplies. We present a transmission flow model which explains the order placement and delivery. The Ethereum platform is utilized for implementation of blockchain and smart contract. An analysis is presented to identify the impact of a change in the number of entities on the number of transactions and the authentication time. Furthermore, we demonstrate how the proposed machine learning (ML)-based intrusion prevention system is able to detect an impersonation attacks during the drone flight operation.

As a future direction to this work, the drone trajectory optimization and path planning can be added to enhance the efficiency of the delivery system and to make the system more autonomous. Moreover, the time optimization of delivery process in case of multiple deliveries through a single drone can be pursued. This optimization can consider factors such as drone size, product type, flight environment and multiple other factors. Another factor that can be analysed include the energy efficiency of drones for the delivery to increase

the overall flight time. The proposed system in this work focuses on delivery of medical supplies, where the identify of the customers can be confidential. Therefore, a privacy preserving mechanism is required to avoid revealing the identity of the customers.

References

[1] A. Balcı, R. Sokullu, Massive connectivity with machine learning for the internet of things, Computer Networks (2020) 107646.

[2] X. Zhou, S. Durrani, J. Guo, H. Yanikomeroglu, Underlay drone cell for temporary events: Impact of drone height and aerial channel environments, IEEE Internet of Things Journal 6 (2) (2019) 1704–1718.

[3] X. Liu, Y. Liu, Y. Chen, L. Hanzo, Trajectory design and power control for multi-uav assisted wireless networks: A machine learning approach, IEEE Transactions on Vehicular Technology 68 (8) (2019) 7957–7969.

[4] G. Liang, S. R. Weller, F. Luo, J. Zhao, Z. Y. Dong, Distributed blockchain-based data protection framework for modern power systems against cyber attacks, IEEE Transactions on Smart Grid 10 (3) (2019) 3162–3173. doi:10.1109/TSG.2018.2819663.

[5] I. Guvenc, W. Saad, M. Bennis, C. Wietfeld, M. Ding, L. Pike, Wireless communications, networking, and positioning with unmanned aerial vehicles [guest editorial], IEEE Communications Magazine 54 (5) (2016) 24–25. doi:10.1109/MCOM.2016.7470931.

[6] D. Wang, P. Hu, J. Du, P. Zhou, T. Deng, M. Hu, Routing and scheduling for hybrid truck-drone collaborative parcel delivery with independent and truck-carried drones, IEEE Internet of Things Journal 6 (6) (2019) 10483–10495.

[7] A. Goodchild, J. Toy, Delivery by drone: An evaluation of unmanned aerial vehicle technology in reducing co2 emissions in the delivery service industry,

Transportation Research Part D: Transport and Environment 61 (2018) 58–67.

[8] M. M. Azari, G. Geraci, A. Garcia-Rodriguez, S. Pollin, Uav-to-uav communications in cellular networks, IEEE Transactions on Wireless Communications (2020) 1–1.

[9] M. Y. Arafat, S. Moh, Localization and clustering based on swarm intelligence in uav networks for emergency communications, IEEE Internet of Things Journal 6 (5) (2019) 8958–8976.

[10] J. Baek, S. I. Han, Y. Han, Optimal uav route in wireless charging sensor networks, IEEE Internet of Things Journal 7 (2) (2020) 1327–1335.

[11] J. Baek, S. I. Han, Y. Han, Energy-efficient uav routing for wireless sensor networks, IEEE Transactions on Vehicular Technology 69 (2) (2019) 1741–1750.

[12] W. Liang, M. Tang, J. Long, X. Peng, J. Xu, K.-C. Li, A secure fabric blockchain-based data transmission technique for industrial internet-of-things, IEEE Transactions on Industrial Informatics 15 (6) (2019) 3582–3592.

[13] X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen, A survey on the security of blockchain systems, Future Generation Computer Systems 107 (2020) 841–853.

[14] J. Liu, Z. Liu, A survey on security verification of blockchain smart contracts, IEEE Access 7 (2019) 77894–77904.

[15] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, F. Wang, Blockchain-enabled smart contracts: Architecture, applications, and future trends, IEEE Transactions on Systems, Man, and Cybernetics: Systems 49 (11) (2019) 2266–2277.

[16] Y. Zhou, P. L. Yeoh, H. Chen, Y. Li, R. Schober, L. Zhuo, B. Vucetic, Improving physical layer security via a uav friendly jammer for unknown eavesdropper location, IEEE Transactions on Vehicular Technology 67 (11) (2018) 11280–11284. doi:10.1109/TVT.2018.2868944.

[17] X. Zhou, Q. Wu, S. Yan, F. Shu, J. Li, Uav-enabled secure communications: Joint trajectory and transmit power optimization, IEEE Transactions on Vehicular Technology 68 (4) (2019) 4069–4073. doi:10.1109/TVT.2019.2900157.

[18] J. Ye, C. Zhang, H. Lei, G. Pan, Z. Ding, Secure uav-to-uav systems with spatially random uavs, IEEE Wireless Communications Letters 8 (2) (2019) 564–567. doi:10.1109/LWC.2018.2879842.

[19] G. Zhang, Q. Wu, M. Cui, R. Zhang, Securing uav communications via joint trajectory and power control, IEEE Transactions on Wireless Communications 18 (2) (2019) 1376–1389. doi:10.1109/TWC.2019.2892461.

[20] P. Gope, O. Millwood, N. Saxena, A provably secure authentication scheme for rfid-enabled uav applications, Computer Communications 166 (2021) 19 – 25. doi:https://doi.org/10.1016/j.comcom.2020.11.009. URL http://www.sciencedirect.com/science/article/pii/S0140366420319897

[21] J. Wang, Y. Liu, S. Niu, H. Song, Lightweight blockchain assisted secure routing of swarm uas networking, Computer Communications 165 (2021) 131 – 140. doi:https://doi.org/10.1016/j.comcom.2020.11.008. URL http://www.sciencedirect.com/science/article/pii/S0140366420319885

[22] O. Brown, D. Joseph, Secure digital escrow account transactions system and method, uS Patent App. 10/010,340 (Jun. 5 2003).

[23] P. De Filippi, What blockchain means for the sharing economy, Harvard Business Review 15.

[24] L. Zhao, A. Alipour-Fanid, M. Slawski, K. Zeng, Prediction-time efficient classification using feature computational dependencies, in: Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, ACM, 2018, pp. 2787–2796. doi:10.1145/3219819.3220117.