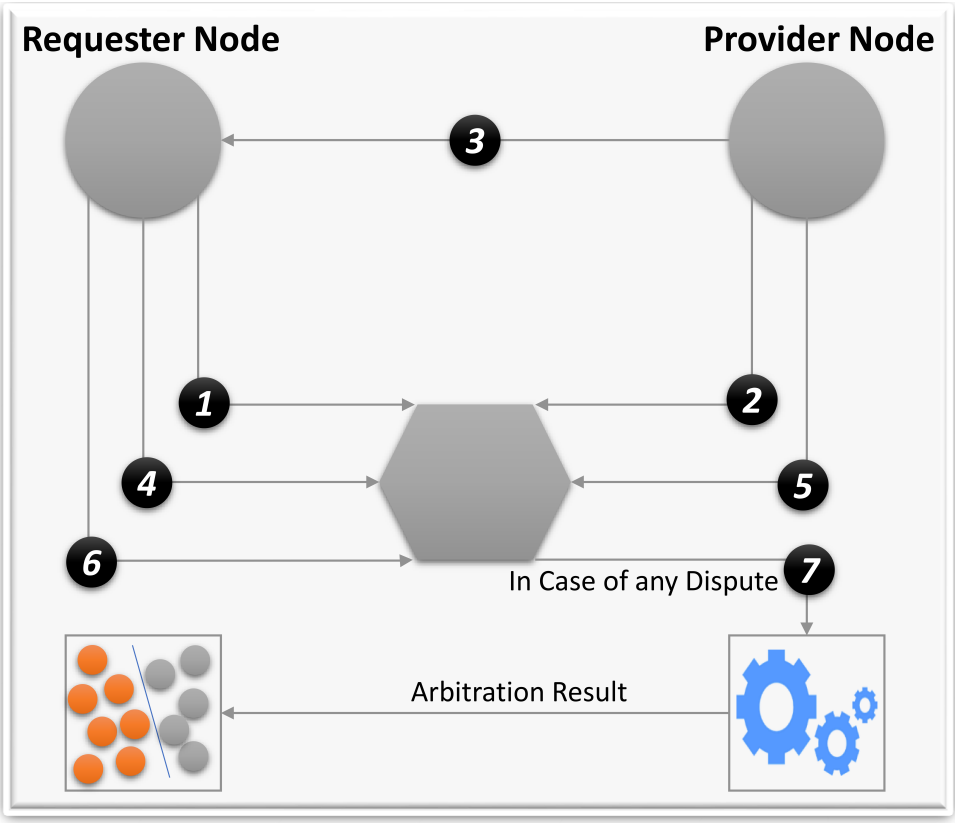
Graphical Abstract

Chained-Drones: Blockchain-based Privacy-Preserving Framework for Secure and Intelligent Service Provisioning in Internet of Drone Things

Junaid Akram*, Muhammad Umair, Rutvij H. Jhaveri*, Naveed Riaz, Haoran Chi, Sharaf Malebary

[0]*Corresponding Authors



1. Request Service *S* with Properties
2. Publish Hash of Signed S
3. Send Signed Service *(Offline)*
4. Confirm Signed S
5. Send Key *(blockchain)*
6. Confirm Service *S*
7. Service Evaluation on Predefined Properties

Highlights

Chained-Drones: Blockchain-based Privacy-Preserving Framework for Secure and Intelligent Service Provisioning in Internet of Drone Things

Junaid Akram*, Muhammad Umair, Rutvij H. Jhaveri*, Naveed Riaz, Haoran Chi, Sharaf Malebary

- We deploy a model that leverages federated learning and is enabled for use with Beyond Fifth Generation (B5G) networks to detect rogue nodes in order to offer improved identification and classification without compromising user privacy.
- The use of fog server characteristics facilitates the backup and transmission of data; In federated learning, Support Vector Machines (SVMs) and Random Forests (RFs) are used to detect and eradicate malicious network participants;
- The use of digital signatures and cascade encryption assures the nonspurning of the service provider;
- The feature assessment methodology supports both the customer's nonspurning and the continuing compliance of the services.

[0]*Corresponding Authors

Chained-Drones: Blockchain-based Privacy-Preserving Framework for Secure and Intelligent Service Provisioning in Internet of Drone Things

Junaid Akram*[a], Muhammad Umair[a], Rutvij H. Jhaveri*[b], Naveed Riaz[c], Haoran Chi[d], Sharaf Malebary[e]

[a]*School of Computer Science, The University of Sydney, Camperdown, 2008, NSW, Australia*
[b]*Department of Computer Science and Engineering, School of Technology, Pandit Deendayal Energy University, Gujarat , 382007, Gujarat , India*
[c]*Computer Vision Center, Universitat Autònoma de Barcelona, Barcelona, 08193, Catalonia, Spain*
[d]*Instituto de Telecomunicacoes, Universidade de Aveiro, Aveiro, 3810-193, Centro, Portugal*
[e]*Department of Information Technology, Faculty of Computing and Information Technology in Rabigh, King Abdulaziz University, Jeddah, 21911, Saudi Arabia*

Abstract

We leverage blockchain technology for malicious node detection in the Internet of Drone Things (IoDTs). IoDTs additionally provide a secure mechanism of service delivery based on cascade encryption and feature assessment. By making localisation and service delivery more challenging, malicious nodes deter new users. The identification and removal of such nodes is necessary for establishing trust between entities. Using federated learning, the proposed system identifies malware. Using SVM and RF classifiers, federated learning is capable of identifying malicious nodes. For the purpose of identifying malicious nodes, we examine their transparency and latency. Nodes that provide services to others provide one another incentives. During service delivery in IoDTs, the challenges that must be addressed are provider and consumer mistrust. These concerns are addressed via feature assessment and cascade encryption. The digital signature used in cascade encryption renders the service provider irrefutable. Due to feature evaluation, consumers get their

[0]*Corresponding Authors

requested services without fail. Functional testing ensures that a service fulfils industry requirements. Our simulation results demonstrate that our non-spurning model works as designed. Accuracy, recall, and overall F1 score are compared between SVM and RF classifiers. The accuracy of SVM is 79%, its F1 score is 0.88, and its recall is 0.78. The RF classifier has an accuracy rate of 95%, a precision rate of 0.92, an F1 score of 0.96, and a recall rate of 1. Utilizing RF significantly improves the precision of identifying malicious nodes.

Keywords: Privacy, blockchain, malicious drones, federated learning, cyber-physical systems

---

1. Introduction

Over the last few years, the drone technology has developed as an essential airborne technology with an inclusive range of environmental, industrial, military, and safety applications [1, 2]. For instance; aerial photography, surveillance, disaster monitoring, and rescue and search operation are some of the applications of drones [1, 3]. In our progressive cyber based society, the utilization of drone technology and drones will unquestionably increase with time. Therefore, the use of computational techniques and algorithms to develop intelligent systems for the advancement of industrial drones is significant in current literature[4]. The rapid development of drones enable us to do such tasks, which are nearly impracticable to perform in the remote areas of real world [5, 6]. Considering the technical perspective of drones, the designing and implementation of network models of drones have several limitations [3]. These limitations are primarily related to the exploitation of insecure connection issues and variety of topologies [7]. Particularly, the insignificant security connections and drone movement cause variety of problems for instance; excessive latency, unauthorized access, and high energy utilization in the network [8]. To overcome these challenges, the emergent technologies like software defined networks and 5G deliver additional flexibility and capability to drones, which are integrated with advanced sensors, high-vision cameras, and GPS system to offer military and commercial services establishing an aerial network acknowledged as internet of drone things (IoDTs) [9]. To develop the cyber based real systems for industrial IoDTs, the sensors, drones, and industrial equipment's are regulated by employing the different computational techniques and algorithms. In [8, 10], the IoDT

is defined a "control architecture with a layered network", which aids in the coordination of UAVs. The IoDT creates an environment in which several drones develop a network and coordinate to receive and transmit data from each other. IoDTs can be operated through internet via IP address or remotely[11].

In industrial exploitations (natural gas and oil explorations sites, high terrain industrial locations, and thermal power plants) the drones are operated to gather data and then for the transmission of this data for analysis on remote sites[12, 13]. In addition to this, the IoDTs can act a probable router for sending the data traffic in remote industrial areas for continuous connectivity. The IoDTs are integrated with sensors can be applied to the gather the data and broadcast it to a central frame for further analysis[14]. Additionally, they have adequate computational power to execute quick processing and analysis at the site where permanent setup cannot be deployed[15, 16]. However, along with the several advantages the IoDTs have numerous limitations, mentioned above. One of the key reason of these limitations is the heterogeneous, distributed, and complex natures of IoDTs[17]. The IoDTs suffer from the potential privacy and security threat as they are not basically designed with considering the security factor, which must be addressed before its utilization in industry [18].

For a drone being a complex heterogeneous network in industrial applications, the privacy and security concerns are not just restricted to intrinsic privacy and security challenges delivered by open channel intranet, cellular networks, mobile communication, and sensor networks, nonetheless, they are also comprising the protection issues and privacy preservations [19, 20]. Consequently, the drones must be capable to adopt the enhanced security concepts and schemes, for instance; authorization, authentication, data protection and integrity, cyber-attack prevention and protection, confidentiality, and access control. The industrial and commercial IoDTs require the communication with every object around them and its named as drone-to-everything (D2X) communications [21]. In such scenario, where any device or object could be in communication with a drone, then more security measure must be taken because the losses could be irreversible and huge at the late stage [22].

For a secure D2X communication, the cryptographic methodologies could be implemented in IoDTs, however, the drones are integrated with restricted resources, and a complex cryptographic methods are not suitable. Nevertheless, the blockchain principle could aid in designing of a secure system

for IoDT [23]. In nature, the blockchain is decentralized; once the data is recorded in a block, is final, and the third party impartiality is a big gain of blockchain. It could be advantageous to IoDT to ensure the ecosystem's decentralization while, confirming the involved entities security. Blockchain constitutes on data blocks, which are interrelated with each other exploiting crypto graphic hash functions [24]. All the contributing nodes in a blockchain usually familiar with each of the transactions occurring in a blockchain [25]. Before creation of each block, it has to undertake a mining process, which is commenced by the blockchain network's nodes known as miner nodes. In ideal case, each node has an equivalent chance to become a miner node. In the network, when any transaction occurs, all miner nodes come to an agreement and updates each node's ledger [26]. In blockchain, numerous consensus algorithms could be utilized between unknown entities. For instance; proof of authority (POA), proof of stake (POS), and proof of work (POW), etc. Through this method, the blockchain creates trust in a network and stores the transactions in a block. Each block has a header and a body, and the blocks are normally linked in chronological sequence. Each block's header is comprised of some elements such as; timestamp, previous block's hash, transactions root, and nonce [27]. However, the genesis block's hash is not included in the calculation of future blocks' hashes. By default, the value of previous is usually set 0 because there is not previous hash block in a genesis block [28]. Furthermore, each block comprises several transactions in a tree form and each transaction's hash is computed utilizing hashing algorithm. The block header includes a transaction root that was generated from the hashes of all the transactions in the block. Some hashing algorithms examples are Keccak-256, Secure Hashing Algorithms, and message digest, etc. In several domains the blockchain is used such as; internet of things [29], shipping management [30], internet of vehicles [31], internet of drone things [32], internet of sensor things [33], and many more to resolve difference concerns like security breaches, privacy leakage, and single point failures, etc.

As mentioned above, the drones constitute sensors so, to develop a coordinated control between several drones, the concept of internet of sensors things can be implemented to the internet of drone things. An important aspect of any reliable IoDTs system is for sensor nodes to provide their precise locations when transmitting data. Still, it is challenging for the nodes with limited resources to pinpoint their precise position in a distant and dangerous environment. In [33], the author proposes a blockchain-based localisation strategy for low-resource nodes. The nodes use beacon nodes to determine

their position. Each beacon's node trustworthy value is computed in order to pick trusted beacon nodes. But the absence of thought given to the existence of malicious nodes casts doubt on the efficacy of beacon nodes as a whole. In addition, the client nodes must be serviced by the service provider nodes in IoDTs networks for entrusted service provisioning to occur. However, there is no proven approach to ensuring that neither the client nor the service provider node is ever spurned. In [34], a non-spurning model based on blockchain is proposed for reliable and secure provisioning. Nevertheless, in order to avoid the client mode from spurning of actual demand services, no mechanism is developed. Additionally, to attain non-spurning , the homomorphic hash is utilized. We propose a mechanism based on blockchain for malicious nodes detection in IoDTs network for secure service provisioning. In addition to this, we exploit the feature evaluation and digital signature capabilities to confirm the non-spurning of client node and service provider, respectively. The key contributions of this article are:

- We deploy a model that leverages federated learning and is enabled for use with Beyond Fifth Generation (B5G) networks to detect rogue nodes in order to offer improved identification and classification without compromising user privacy.
- The use of fog server characteristics facilitates the backup and transmission of data; In federated learning, Support Vector Machines (SVMs) and Random Forests (RFs) are used to detect and eradicate malicious network participants;
- The use of digital signatures and cascade encryption assures the non-spurning of the service provider;
- The feature assessment methodology supports both the customer's non-spurning and the continuing compliance of the services.

The rest of the paper is structures as follows. Section 2, presents the related work. In Section 3, the service provisioning models and B5G permitted malicious node detection are depicted. The Section 4, evaluates the performance of proposed system models and Section 5, presents the conclusion.

2. Related Work

In IoDTs, the critical factors needs to be considered are the threats, which are accountable for manipulating the vulnerabilities by presenting unwanted

alterations [35]. These threats must be considered important as the data in IoDTs is very sensitive. In IoDTs, the sensitive information is processed or gathered in bits and pieces while, categorizing them in their particular tasks. So, the such kind of information must not be leaked because it could be a huge loss in terms of trust and privacy [36]. The IoDTs have a significant role in case of network communications for public safety. In these cases, an intruder or attacker could breach the protocols and get access to the secure communication, which further lead to the privacy breach. After accessing this information, an intruder can modify or fabricate the sensitive information and misguide the receiver. In IoDTs the access control is a critical parameter, hence, security concerns about authorization and access must be stressed. If someone attacks the system then the intruder can alter the information by accessing the control information and this change in information can generate several disagreements with the particular IOD.

The vulnerabilities and securities in IoDTs are the main concern in this paper. The works related to this study are categorized into eight subsections. Each component is broken down further by addressing the restrictions that address it.

2.1. Localization of resource-constrained nodes securely

By broadcasting incorrect sensor positions or by tricking them into receiving their erroneous location coordinates, malicious nodes in sensors of IoDTs attempt to negatively impact network performance [33]. The network experiences inconvenience as a result of these malicious nodes' actions, which result in the acquisition of data with the incorrect or unknown location. The sensors based IoDTs untrustworthy environment makes nodes wary about joining the network. Additionally, it is challenging to localize sensor nodes because of the dynamic topology of drones wireless sensor networks [37].

2.2. Routing protocols to reduce unnecessary resource utilization

The selection of the wrong routing path and a lack of data security are two important problems in sensors based IoDTs. For the purpose of keeping data safe and selecting the most efficient path from origin to destination, users have a lot of alternatives. These methods, however, come with extra expenses and don't provide useful route choices [38]. The similar problem is brought up by the authors in [39]. The note the lack of a routing strategy to spot rogue routing nodes. There proposed methodology stops the threats to the path selection algorithm and data integrity. The attacks of malicious

nodes cannot be stopped or handled by this approach. One of the problems with internet of things (IoT) networks is that they are frequently governed by a centralized authority that makes all of the network's routing decisions [40]. Additionally, given this setting of lack of trust, the authors construct a trust management infrastructure. But it turns out to be a rather expensive solution. For reliable data transfer, numerous routing strategies are proposed. However, these systems only account for fixed nodes, and there is a lack of study into dynamic topologies [41]. Since the external nodes want to modify the network data for their own interests, participants and external users are discouraged from disclosing passwords. Many methods have been proposed to address both external attackers and malicious inside nodes; nevertheless, due to their mobility, nodes impose a heavy burden on the network. Internet of Underwater Things (IoUT) devices in use for exploration raise similar challenges [42]. The authors claim that various proactive routing techniques are put forth for dependable data transport and communication. These routing protocols, however, only work with static IoUT and are ineffective with dynamic IoUT.

2.3. Authentication protocols

The security and privacy of data are not addressed by conventional IoT authentication systems, which are centralized [43]. Additionally, they have a number of problems like privacy breaches, heavy power usage, and lengthy computation times [44]. IoT devices have limited hardware capabilities and little storage, which is the problem. Therefore, IoT devices cannot use these authentication protocols.

2.4. Blockchain-based secure service provisioning methods

There are numerous trust concerns in the service supply process. Nonconformance occurs when a service provider offers a client services that don't meet their expectations [34]. Additionally, the service provider offers malicious and pointless services to the client and refuses to continue doing so. However, the consumer obtains genuine services from the supplier, puts them to use for his own ends, and denies any involvement with the service. It has been stated by the consumer that the service does not fulfil their needs. Additionally, there are a lot of security and privacy issues with these service providing systems when communicating across entities [45]. The authors also claim that IoT devices are used by smart industries to manufacture goods

more quickly and more affordably. These gadgets are used to exchange personal data between industries. Various attacks could result in privacy leaks and issues over information confidentiality. Unfortunately, current methods of managing shipping and transportation are riddled with security and privacy vulnerabilities [30]. Additionally, they don't offer openness and traceability about goods transportation. They suggest a blockchain-based shipping management system that offers the system transparency, security, and traceability.

2.5. Techniques for enhancing network security and privacy

Data from IIoTs is sensed via dynamic wireless sensor networks (DWSNs) [46, 47]. However, DWSNs have some problems with trust. One reason for the lack of confidence is the vulnerability of the whole network to attacks on individual nodes, such as untrustworthy base stations. The authors of [48] believe that current methods for detecting attacks on base stations and other nodes in IoT networks are either decentralised or centralised, compounding the problem. Single points of failure, large computational and storage requirements are only some of the issues with centralised attack detection approaches. The decentralised approach for attack detection makes it difficult to compile information and historical data for a detection model. Intruders and internal attackers are the two main categories of network attackers. The first group is not a part of the network. They continue to attempt data manipulation, nonetheless, in order to gain advantage [49]. Participants in the network today are attempting to dominate the entire network in order to further their own objectives. As a result, the sensors based IoDTs have some major security concerns and must locate and take out the network-disrupting nodes. According to the authors of [29], the applications of smart cities in industry 4.0, banking, and healthcare necessitate high levels of security. The authors of [31] draw attention to the problems with privacy leaks in vehicle internet communications.

2.6. Blockchain-based storage optimization strategies

The sensor nodes in the sensors based IoDTs have constrained computing and storage resources, according to the authors in [50, 51, 52]. Occasionally, the volume of detected data exceeds the capacity of the sensor nodes to store it.

2.7. Models for resource optimization in networks with limited resources

The nodes in the sensors based IoDTs do POW, which uses up a lot of their resources and prevents them from sensing and serving the network [53]. Similar problems are discussed for sensors based IoDTs nodes with limited resources by the authors in [52]. They draw attention to the benefits of blockchain technology and provide a method for avoiding several drawbacks of centralized authority, such as high costs and single points of failure. Blockchain, however, necessitates powerful computing power for the POW consensus method. Similar to this, POW validates a block in about 10 minutes[54]. While other consensus algorithms take less time to generate blocks, their data rate is lower. Each transaction in Tangle must verify the validity of the two transactions that came before it. However, there are limitations on the power and processing capacity of IoT nodes. Because of their rapid battery drain while confirming prior Tangle transactions, the network is unreliable. The sensors based IoDTs, on the other hand, has a variety of other problems, such as bandwidth bottlenecks, latency, and cost overhead [55, 56, 57]. Numerous methods are suggested for monitoring the air quality in metropolitan areas [55]. But because these methods are centralized, a single node is in charge of keeping an eye on a huge area and recording each measurement along with its position. Such methods require nodes that have high deployment and maintenance costs in order to precisely sense data and save their precise location. IoT devices and their associated data are growing every day [57]. As a result, bandwidth constraints, high latency, and poor scalability are problems in smart cities. Furthermore, smart cities with adequate processing and storage resources lack a safe design.

2.8. Communication beyond the fifth generation

Because of its high bandwidth and low latency, Beyond 5G (B5G) networks are used in many different fields. The number of IoT devices is growing daily, and B5G communication technology is necessary for the IoT infrastructure to function well [58, 59]. Additionally, [60] proposes a routing protocol for heterogeneous WSNs that makes use of the B5G network's features. Decision trees and support vector machines are also used to improve the B5G network's functionality, flexibility, and efficiency. In a similar vein, the needs of the Intelligent Transportation System (ITS) are so comprehensive that they cannot be met by existing network designs, but ITS continues to grow at an exponential rate[61]. As a result, a communication technology that supports ITS's proper operation is necessary.

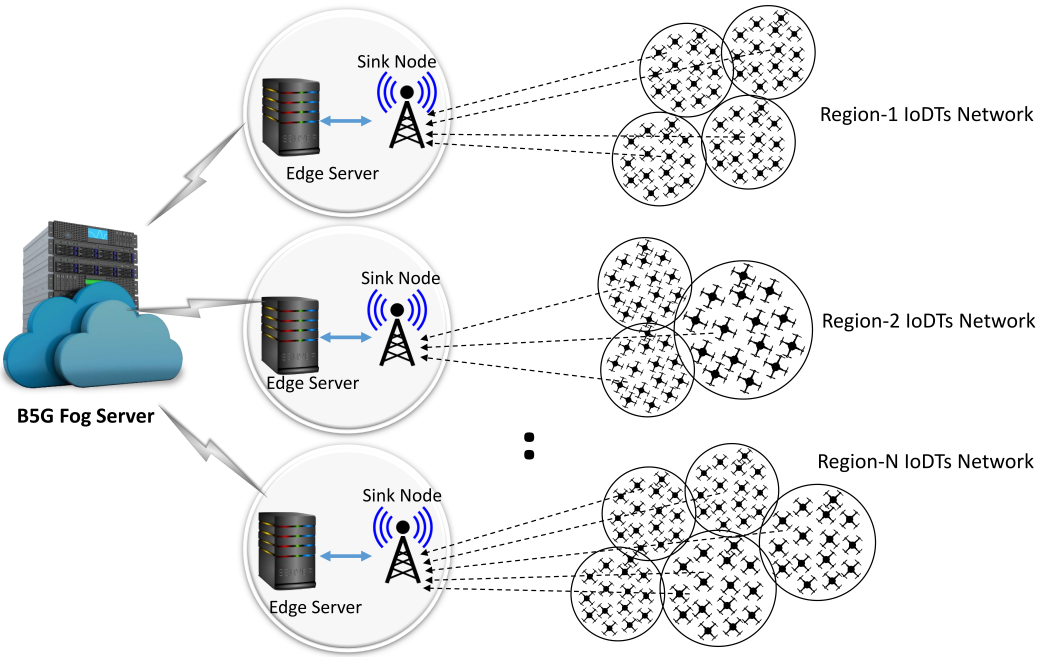


Figure 1: Abstract architecture of Internet of Drone Things

The limitations that the aforementioned efforts addressed are what are used to categorize them. In these publications, blockchain is used to address a variety of problems, including single points of failure, high costs, privacy breaches, and lack of legitimacy. These studies do, however, have a number of problems, including the presence of malicious nodes, excessive resource usage, non-spurning , the quality of the data, etc. We suggest employing federated learning to address the problem of malicious nodes in the network. The supervised learning algorithms used in our model for malicious node detection are driven by [37, 38, 39, 40, 41]. Furthermore, we offer a non-spurning model based on the blockchain that is effective and provides enough proof that neither the service provider node nor the client node can dispute the activities of the other. Additionally, it is made sure that the client cannot deny the services that were truly requested [33].

3. System Model

In this part, we present the suggested malicious drone detection model enabled by B5G. The proposed model is based on federated learning. The

model detects the malicious drone and eliminates the threat it poses to the rest of the drones in an IoDT network. In addition, we provide a service provisioning technique to guarantee non-spurning behavior of both the client and the service provider in an IoDT. The non-spurning service model uses cascaded encryption and feature evaluation to ensure the conformance of services. The proposed model is based on the following assumptions:

- All drones in an IoDT are randomly deployed.
- All legitimate and sink drones in an IoDT are addressable.
- All drone nodes are mobile.
- All sink drones in an IoDT are trustworthy and generate keys for other nodes.
- All sink nodes have ethereum addresses.
- Fog node provided secure storage for IoDT data.
- All sink drones have relatively high computational power, energy resources and payload capacity.
- Ordinary drones are homogeneous.
- The data in a network may be safely stored on a fog server.
- Sink drones are responsible for data aggregation.

3.1. Blockchain-based Malicious Drone Detection Model

Sink drones, regular drones, and cluster heads are the various nodes that make up an IoDT network. Normal drones are usually responsible for sensing the environment e.g., capturing pictures and videos, sensing the wind speed and pollution index etc. Regular drones are also responsible of sharing their precise location with sink drones. Cluster head drones are mainly responsible for setting up the network. Sink nodes usually have more capabilities in terms of computation, power backup and storage etc. They are mainly responsible for collecting data from other drones. Each drone sends its data to sink drone along with its location and address. Authors in [33] claim that there may be some nodes in sensor networks that are unable to determine

their location. We may encounter similar conditions in chained drones where drones deployed in forests, battlefields and other hostile environments are unable to determine their precise location. Inaccurate location information of drones can cause issues in surveillance. We use the term "unknown drones" for drones having no or imprecise location information. The location of unknown drones is estimated with the help of beacon drones. Beacon drones are mainly responsible for assisting unknown drones to estimate their precise location information. A fundamental assumption in the existing IoDT models has hitherto been that the beacon drones are trustworthy. However, the issue of trust becomes paramount in large scale IoDT networks. Large scale IoDT networks are relatively more vulnerable of possessing malicious beacon drones.

As stated earlier, there may be malicious nodes in an IoDT network. Existing approaches to identify the presence of malicious nodes in a network are based on machine learning solutions [62]. Existing approaches to detect malicious drones in IoDT networks are based on centralized learning. Data from the whole IoDT network is sent to a central server using sink nodes. The data is then used in the training of machine learning models to isolate legitimate and malicious drones. This centralized training compromises on the privacy of different IoDT regions. We propose a federated-learning-based approach to detect malicious drones in an IoDT network. We divide an IoDT network in to multiple regions. Each region is divided in to multiple clusters. Each cluster has its own cluster head and a sink drone as shown in Figure 1. Federated learning is a relatively more privacy preserving approach as compared to centralized learning. In federated learning, we consider four clusters of an IoDT region. A virtual machine is associated with each cluster. Sink nodes of each region send data to the assigned virtual machines which are connected with a B5G fog server. Machine learning classifiers are then trained on this data on virtual machines. The B5G fog server receives the trained models from the virtual machines. The trained models are then fused on the fog server. The fused model is then shared with each virtual machine. This data is then analysed on the virtual machines using machine learning approaches to differentiate between legitimate and malicious drones. In this way, the proposed model trains the machine learning algorithms on the private data of each cluster without compromising the privacy of an IoDT cluster.

In state-of-the-art, a costly blockchain storage is used to store the fused trained models. Since the suggested federated-learning-based solution uses

individual virtual computers for each area, the problem of incredibly expensive blockchain storage may be addressed. Moreover, the proposed federated learning is relatively more accurate in determining malicious drones because the data from different regions is analysed separately on multiple virtual machines. A machine learning model is trained on this data locally on each virtual machine to isolate malicious and legitimate drones. It also resolves the privacy issue. The proposed privacy preserving model can be divided in to three layers: B5G fog server layer, training layer and sensing layer. B5G fog layer is responsible of fusing trained models received from individual virtual machines. Virtual machine layer is responsible of training machine learning models on the data collected from sink nodes. The sensing layer consists of regular drones deployed in the environment.

Virtual machine of each region is connected to a B5G-enabled fog server. Specifically, the B5G network is responsible for carrying data between the various IoDT zones and the fog server. B4G network may under perform in relatively dense IoDT networks due to large footprint of the fused models. The size of the fused model becomes large in large-scale IoDT networks having large number of regions and virtual machines. It is due to the fact that the fused models contains all local attributes. In large-scale IoDTs, Fourth Generation (4G) networks may underperform due to their high latency and low data rate. Therefor, we propose to use B5G network to avoid the delays in highly scalable IoDT networks. The data rate in Fifth Generation (5G) models is usually 1000 Mbps. However, the B5G network have high loss of frequencies. Therefore, it provides relatively low coverage distance. Moreover, the most of rural areas do not have 5G infrastructure.

3.2. Determining Trust of Beacon Drones

Anonymous drones rely on beacon drones to estimate their location information. These beacon drones may be malicious. Therefore, beacon drones are mainly responsible for creating a vulnerability in an IoDT network. We determine three different types of trust for beacon drones: behavioral trust, data-based trust and feedback-based trust. Behavioral trust depends on four different parameters: honesty, intimacy, frequency of interaction and closeness. Closeness reflects the number of drones closer to a beacon drone. The overall trust of a beacon drone is affected if there is a malicious drone in the vicinity of the beacon drone. The overall trust of beacon nodes helps to identify the likelihood of a beacon node to be a malicious drone. We

leverage machine-learning-based approach specifically Support Vector Machine (SVM) classifier and Random Forest (RF) classifiers to label a drone as either a legitimate or a malicious drone. SVM classifier basically draws a decision boundary between data points representing malicious and legitimate drones. Whereas, RF classifier is a decision-tree-based approach. We exploit RF classifier to enhance the classification accuracy. RF, in our case, relies on end-to-end delay and honesty of a node to classify it as either a malicious or legitimate node. The end-to-end delay is the time taken by a data packet to reach from one drone to another.

3.2.1. Honesty

Honesty is an important parameter to compute behavioral trust. We consider honesty and end-to-end delay of a beacon drone to identify malicious drones in an IoDT network. Honesty of a beacon drone is determined by the ratio of number of successful interactions and number of unsuccessful interactions of the beacon drone with other nodes. Equation 1 shows the expression to determine honesty of a beacon drone.

$$Honesty = \frac{N_s}{N_u} \tag{1}$$

Where N_s is the total number of successful contacts with a beacon drone and N_u is the total number of contacts between a source drone and a destination drone.

The following work flow results in the detection of malicious drones: **Step 1:** Calculating the honesty and end-to-end delay. Afterwards, a dataset of all drones is generated.
Step 2: Labeling the dataset (in to 1 and -1) according to the computed honesty and end-to-end delay.
Step 3: Dividing the data in to training set and test set. The models are trained on 80% of the data. Whereas, 20% of the data is reserved for testing.
Step 4: Training the SVM. It results in a hyperplane that classifies malicious and legitimate drones.
Step 5: Testing the machine learning model. After this step, harmful drones are removed from the IoDT.

3.2.2. Closeness

Closeness of a beacon drone is determined by the ratio of number of one-hop close drones and the total number of drones interacting with the beacon

drone. Equation 2 shows the expression for calculating the closeness of a beacon drone.

$$Closeness = \frac{N_o}{N_t} \tag{2}$$

Where N_o represents the number of drones within a single hop of the beacon node, and N_t represents the total number of drones in range of the node except the beacon node.

3.2.3. Frequency of Interaction

The number of times a given beacon drone communicates with another beacon node is used to calculate the interaction frequency. Equation 3 shows the expression for computing frequency of interactions.

$$FoI = \frac{I_m}{I_n} \tag{3}$$

where I_m represents the number of interactions of a particular beacon drone with another beacon drone m and I_n represents the interactions of this node with beacon node n.

3.2.4. Intimacy

An individual beacon node's level of intimacy with other beacon drones is proportional to the length of time that node has been communicating with other drones. Equation 4 shows the expression of Intimacy.

$$Intimacy = \frac{t_m}{t_m + t_n} \tag{4}$$

where t_m represents the time for which a beacon node interacts with another beacon drone m and t_n is the interaction time of this drone with beacon node n.

Afterwards, we compute the feedback-based trust and data-based trust of beacon drones. Feedback-based trust is determined based on the accuracy of location coordinates sent by a beacon drone to other beacon drones. Data-based trust is determined by comparing the measured and predicted distances between beacon nodes. The actual distance is the euclidean distance of beacon nodes. It is computed according to the following equation:

$$d_{ab} = \sqrt{(x_m - x_n)^2 + (y_m - y_n)^2} \tag{5}$$

where d_{ab} is the euclidean distance.

3.3. Selecting Miners and Trilateration Process

The equation 6 shows how the three types of trust (behavioral, feedback and data trust) used in a beacon drone are combined to form the overall level of trust. The most reliable beacon drone is selected based on its trust score. The beacon drone with the highest trust score acts as the miner, either for the purpose of adding new drones to the network or for confirming transactions. The selection of the most trustworthy beacon drone is actually a PoA consensus mechanism that is being used in our blockchain. In this network, drones act as both sinks and beacons, with each drone running its own private blockchain. All the information that the drones share with one another is encrypted and kept on this blockchain. This information can not be altered or deleted. The integrity of this information is preserved.

$$Trust_{beacon} = trust_{behavioral} + trust_{feedback} + trust_{data} \tag{6}$$

The localisation procedure is then started thereafter. Each drone's position is calculated using a trilateration method. Each drone uses trilateration to determine its relative position with respect to the three beacon drones with the greatest trust ratings. Equation 7 shows the expression of calculating distance between two drones.

$$d_{tri} = \begin{cases} \sqrt{(x_i - x_a)^2 + (y_i - y_a)^2} \\ \sqrt{(x_i - x_b)^2 + (y_i - y_b)^2} \\ \sqrt{(x_i - x_c)^2 + (y_i - y_c)^2} \end{cases} \tag{7}$$

where d_{tri} is the trilateration distance of node i. x_i and y_i are x and y coordinates of a unknown drone *i*. (x_a, y_a), (x_b, y_b) and (x_c, y_c) represent coordinates of a beacon node a, b and c respectively.

3.4. Non-spurning Service Provisioning Mechanism

Service provisioning ensures the availability of services and intended resources to the client. In this paper, we propose a blockchain-based non-spurning service mechanism for IoDT networks. In an IoDT network, malicious drones can cause an interruption in services. Therefore, it is necessary to ensure that the neither client nor the service provider can repudiate its actions. This is called as the non-spurning behavior. Non-spurning service mechanism also ensures the standard of the offered services. The following three things are ensured in the proposed service provisioning mechanism:

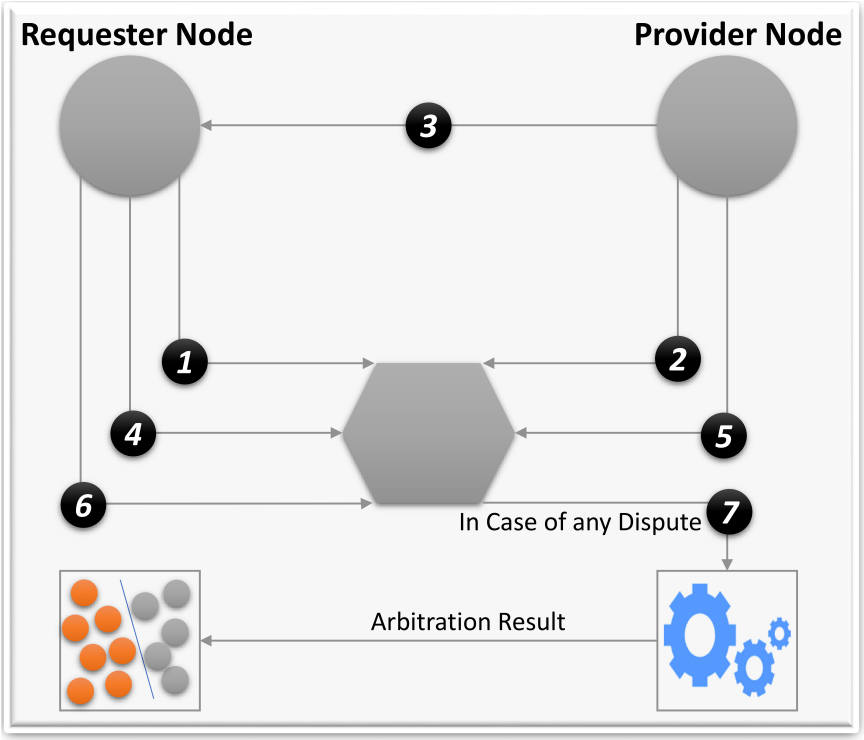


Figure 2: Non-spurning service provisioning mechanism

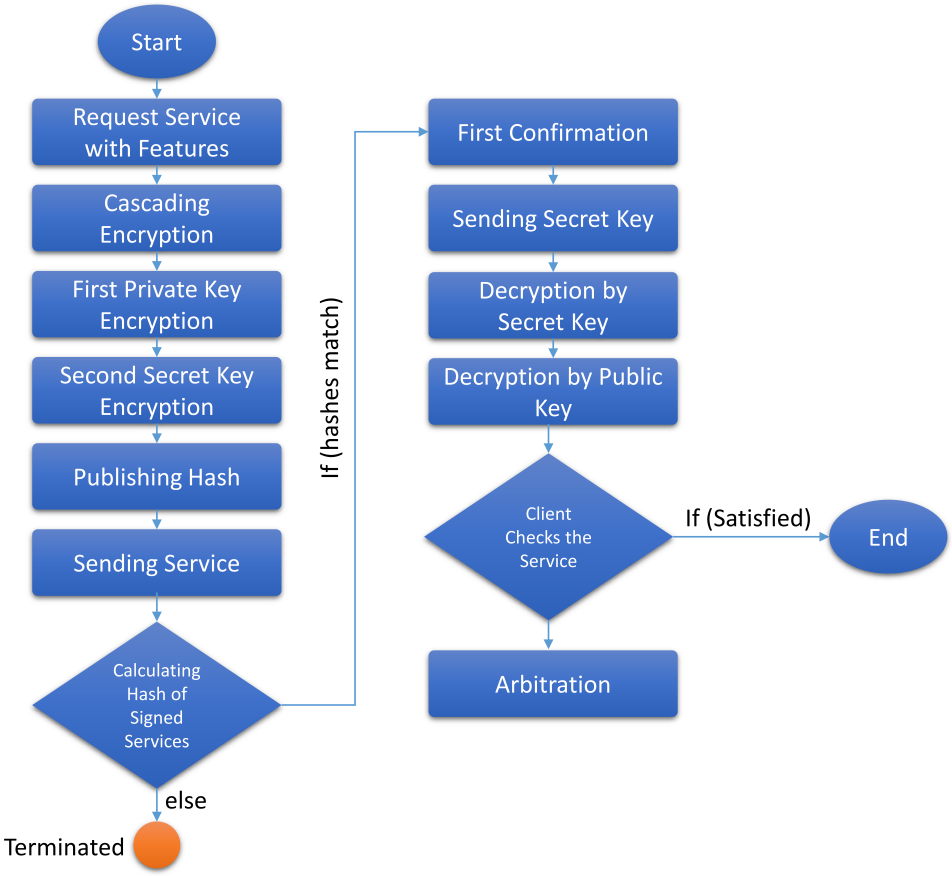


Figure 3: No-spurning scheme workflow

- Conformance of the service standards.
- Client can not spurn the availed services.
- Non-spurning services by the service provider.

In our proposed framework, it is ensured that the client can not deny that it did not get the right service. It is called as the non-conformance of services. A feature evaluation process is used to ensure the non-conformance of client. Elliptic Curve Cryptography(ECC) is used in the proposed service provisioning approach to assure non-spurning behaviour of the service provider. The data between the the client and service provider is totally encrypted. Public and private keys are generated on the trusted sink drones. These sink nodes are responsible of generating public, private and secret keys. The non-conformance of the service provider is ensured by encrypting the service using its private key and converting it in to a cipher text. The network is encrypted in a way that the clients cannot falsely claim that they did not get the service. Moreover, service providers can not falsely pretend that they provided the service. The detailed workflow of the proposed service provisioning is shown in Figure 2.

Algorithm 1 : Non-spurning Service Provisioning Model

1: **Input**: ζ (service), τ (trust factors), κ (keys)
2: **Output**: drone-label i.e., malicious/legitimate
3: Service request with the specified features
4: Encrypting the service
5: Sending the signed service
6: Service confirmation from client
7: Sharing secret decryption key
8: First Decryption of service
9: Second Decryption of service
10: Conforming the service standards
11: Giving verdict on the participating drone as either malicious or legitimate.

The pseudo code of the proposed service provisioning mechanism is shown in Algorithm 1 and Figure 3. Non-spurning behaviour of the client is ensured using double encryption. Initially, a file or data to be transmitted is encrypted. Afterwards, another layer of encryption is introduced to safely share this encrypted data among different drones. If a conflict occurs between a client and a service provider, one of the entities initiates a smart

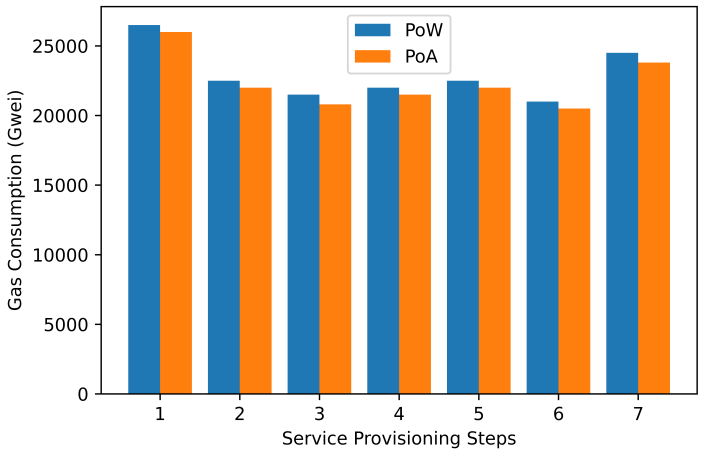


Figure 4: Average transaction cost for every service provisioning steps.

contract which investigates the digital signatures and acknowledgements to detect which drone is malicious.

4. Results and Discussion

In this section, we present the simulations used to validate our system's models. The simulation results indicate that our suggested method for detecting rogue nodes enabled by B5G is successful. Moreover, the data demonstrate that the non-spurning technique we proposed is effective. A 2.80 GHz Intel Core i7 CPU and 16 GB of RAM are used to evaluate the performance of the models. We implemented our blockchain-based B5G malicious node detection and non-spurning models across three IoDTs network areas. This model employs the PoA consensus technique. A select set of trustworthy network nodes are entrusted with the responsibility of verifying transactions and creating new blocks to the blockchain using this mechanism.

Figure 4 compares the gas consumption of PoW and PoA in the IoDTs network of region-1 throughout the service provisioning process. Figure 5 compares PoW and PoA with regards to the average gas consumption of the IoDTs networks across all 3 locations. The data reveal that the gas consumption of PoW is much greater than that of PoA. This is because, under PoW, the miner nodes chosen to verify transactions must first solve an extremely difficult mathematical problem. This is how PoW works. Under

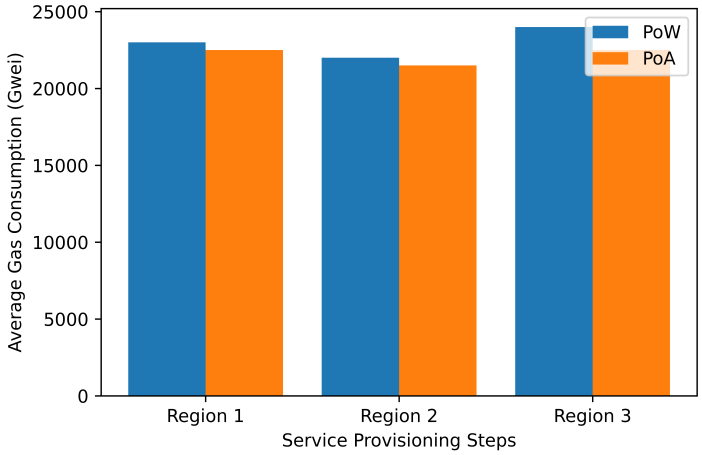


Figure 5: Average transaction cost for 3 regions.

PoA, however, miners are chosen to verify transactions and add new blocks to the distributed ledger based on the stakes they possess. Since miners in Proof of Authority are hand-picked nodes on which all transactions depend, it stands in contrast to the distributed nature of blockchain technology. Therefore, Proof of Authority contributes to the rising centralisation of blockchain networks.

Figures 6 and 7 exhibit a comparison of the transaction latency induced by the adoption of the Keccak-256 and SHA-256 hashing algorithms in Region-1's IoDTs network with the other three regions. Figures 6 and 7 demonstrate that we undertake 25 transactions inside the IoDTs network of region-1 and 250 transactions throughout all 3 regions. These examples demonstrate that SHA-256 and Keccak-256 behave identically while hashing data. Results indicate that SHA-256 calculations need almost twice as much time as Keccak-256 computations. Unlike the SHA-256 hashing method, Keccak-256 has an unlimited input space. Our non-spurning model may be used to any size network and proves that neither the service provider nor the client can claim ignorance of their activities.

B5G-enabled hazardous node identification uses federated learning, SVM, and RF classifiers. SVM can divide linearly separated data points into two groups using a hyperplane. It is valid if the class has a high honesty value and minimal transaction latency overall. On the other side, malicious nodes

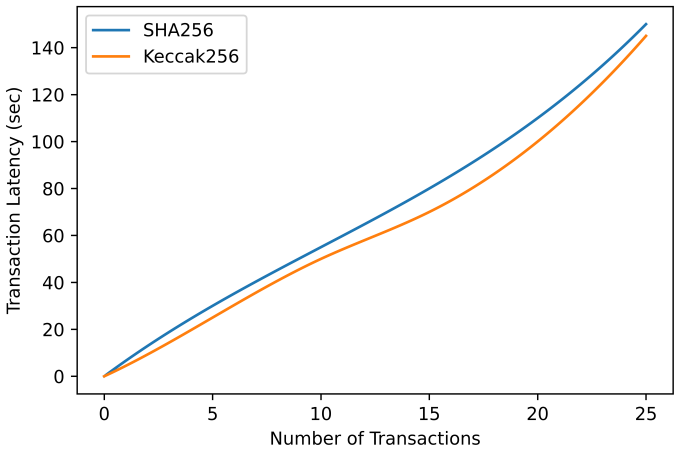


Figure 6: Average transaction cost for every service provisioning steps.

are those with both a high round-trip latency and a low honesty score. RF functions brilliantly in identifying malicious nodes in regionally isolated networks (region-1 IoDTs network) and globally scattered networks (all three regions' IoDTs network). This stays true regardless of how many regions are included in the networks. RF is 95 percent accurate, but SVM is only 79 percent accurate, as illustrated in Figure 7a.

SVM has an average accuracy of 76 percent across all 3 zones, while RF has an average accuracy of 96.36 percent. Based on the honesty value and end-to-end latency of the nodes in question, it would seem that RF is more effective than SVM in identifying rogue nodes in networks belonging to both a single region and many areas. RF is especially successful because it incorporates ensemble learning, which comprises several decision trees, in addition to its greater accuracy. The same challenge of recognising malicious nodes may be addressed by training several decision trees. In addition, it is shown that the SVM's F1 score is 0.88 whereas the RF's F1 score in a single area is 0.95. The average F1 score for the SVM technique across all 3 IoDTs networks is 0.85, whereas the average F1 score for the RF approach is 0.96. This demonstrates that the RF is less likely to falsely identify dangerous nodes as valid nodes in networks that are confined to a single region or cover a large geographical area. SVM has a lower recall score than RF. This is the situation because RF can more precisely forecast which nodes would act

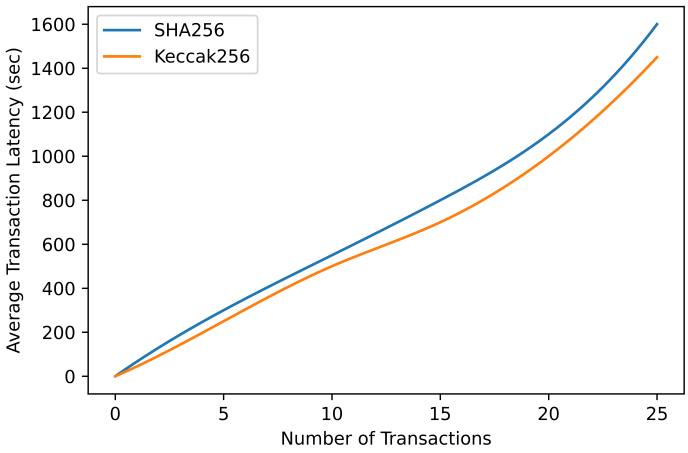


Figure 7: Average transaction cost for 3 regions.

maliciously. Moreover, the presented data demonstrate that SVM is more accurate than RF. SVM helps identify positive data by providing a support vector.

Our suggested non-spurning model is validated by the IoDTs network in all three regions. A transaction's latency is the length of time it takes for a network to process it. The results also include the amount of time required for a client and a service provider to conclude an arbitration transaction. All of these encounters result in the same conclusion: either the service provider or the user was malevolent. Our proposed system can handle several transactions rapidly. It takes 131 seconds to complete 100 arbitration transactions on a single region's network, and 1,410 seconds to complete 1,000 arbitration transactions across all three regions' networks. This is due to the fact that there is no actual data exchange during these sorts of transactions, but a fair comparison can be made between the characteristics listed in step 1 and services offered in the sixth step. It proves that arbitration transactions consume little in the way of bandwidth, throughput, and other resources. These numbers also suggest that the latency of transactions that do not involve spurning is rather low. Due to its scalability, this demonstrates that the non-spurning strategy we offer may confidently service a large number of user.

Figure 8 depicts the veracity of regular nodes extracted from the IoDTs

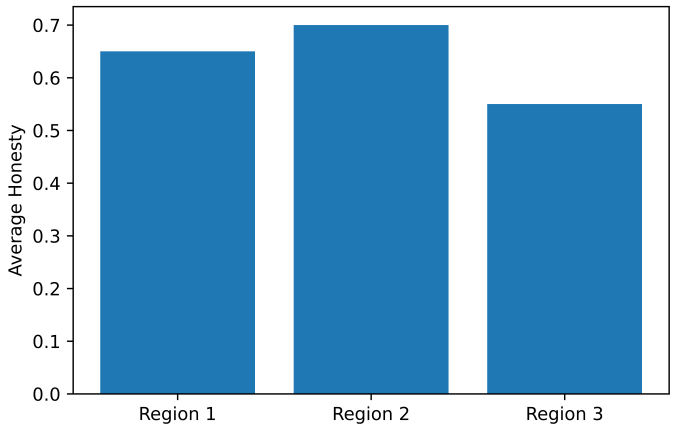


Figure 8: Average honesty of the model.

network in all regions. The IoDTs network supplies the candidate pool from which fifty ordinary nodes are selected. The diagram depicts how distinct nodes have diverse definitions of what makes honesty. This is because the nature of each node defines its own unique amount of successful interactions. As illustrated in Figure 8, the same procedure is used to establish the dishonesty rating of each of the three locations' IoDTs networks. A high ranking for integrity shows that the nodes in issue are genuine. If a node in a network has a high honesty rating, it suggests that it communicates extensively with other nodes in the network. Integrity is regarded as a crucial aspect in identifying whether or not a node is valid inside our networks. When determining a node's authenticity, it is also vital to take into account the whole time it takes for a transaction to complete from beginning to finish. First determine the transmission delay, then the propagation delay, the processing delay, and lastly the queuing delay. Flagged nodes have end-to-end latency over the malicious threshold. This is because the nodes are too slow to handle requests from other nodes. In addition, they are unable to handle the data packet because of their subpar processing power, leading to a denial of service. A node of this kind announces across the network that it either cannot or will only be able to deliver the data packet after an extremely long end-to-end delay (latency).

Figures 9 show end-to-end latency of distinct IoDTs nodes and the average

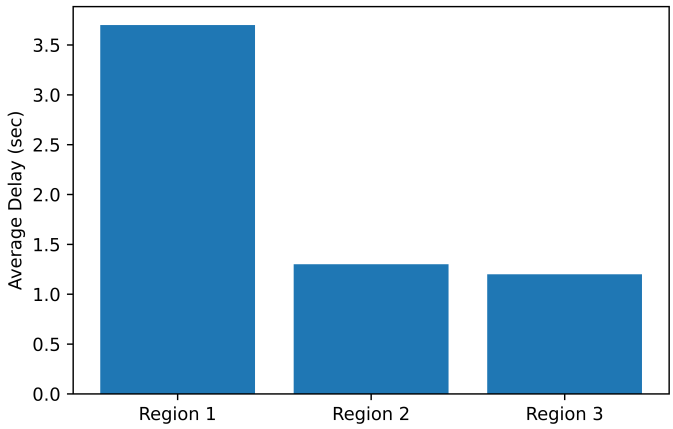


Figure 9: Average delay.

for all three networks. Figure 9 shows the average end-to-end delay over all ten IoDTs networks, together with each node's end-to-end latency. As shown in delay, fifty regular nodes are chosen from each region using a random selection. It is evident from the diagram that each node has a unique end-to-end delay value. This occurs because the time it takes for a given network node to process a request from another network node varies. Network nodes are malicious if their end-to-end latency is much higher than a predefined threshold. Figure 9 also show that average network integrity and end-to-end latency values vary among the various IoDTs area networks. In terms of the provision of secure services, this suggests that the various IoDTs region networks function differently.

5. Conclusions

This work intends to assist researchers identify malicious nodes in IoDT networks using a blockchain-based technique. Malicious nodes inside IoDTs may be identified using federated learning in combination with RF and SVM classifiers. Neither the service provider nor the client may dispute accountability for the actions of the other when using the mechanism of service provisioning defined for IoDTs. This is accomplished by using cascade encryption and feature assessment algorithms, which provide non-spurning on both the client and service provider sides. The outcomes of our simulation

validate the effectiveness of our proposed approach. Recall, precision, accuracy, and F1 scores will be used to evaluate the performance of the SVM and RF classifiers. The SVM has a recall of 0.78, an accuracy of 79%, a precision of 0.88, and an F1 score of 0.88. In comparison, the RF classifier has 95% accuracy, 98% precision, 98% F1 score, and 100% recall. For identifying malicious nodes, the findings indicate that RF is more trustworthy than SVM. Examining non-spurning models from the viewpoints of gas usage and transaction times. When a client requests step 1 data from the non-spurning model, its privacy is endangered. This issue is unfortunately inherent to the non-spurning technique. If a single service provider supplies data, all other organisations will assume it meets the requirements.

References

[1] W. Shi, H. Zhou, J. Li, W. Xu, N. Zhang, X. Shen, Drone assisted vehicular networks: Architecture, challenges and opportunities, IEEE Network 32 (3) (2018) 130–137.

[2] S. Vashist, S. Jain, Location-aware network of drones for consumer applications: Supporting efficient management between multiple drones, IEEE Consumer Electronics Magazine 8 (3) (2019) 68–73.

[3] P. Kumar, P. Singh, S. Darshi, S. Shailendra, Analysis of drone assisted network coded cooperation for next generation wireless network, IEEE Transactions on Mobile Computing 20 (1) (2019) 93–103.

[4] A. Rafi, G. Ali, Efficient energy utilization in fog computing based wireless sensor networks, in: 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE, 2019, pp. 1–5.

[5] R. Durga, E. Poovammal, K. Ramana, R. H. Jhaveri, S. Singh, B. Yoon, Ces blocks—a novel chaotic encryption schemes-based blockchain system for an iot environment, IEEE Access 10 (2022) 11354–11371.

[6] A. U. Rehman, Z. Rehman, W. Ali, M. A. Shah, M. Salman, Statistical topic modeling for urdu text articles, in: 2018 24th International Conference on Automation and Computing (ICAC), IEEE, 2018, pp. 1–6.

[7] K. Namuduri, Y. Wan, M. Gomathisankaran, R. Pendse, Airborne network: a cyber-physical system perspective, in: Proceedings of the first ACM MobiHoc workshop on Airborne Networks and Communications, 2012, pp. 55–60.

[8] J. Kim, G. Caire, A. F. Molisch, Quality-aware streaming and scheduling for device-to-device video delivery, IEEE/ACM Transactions on Networking 24 (4) (2015) 2319–2331.

[9] M. Gharibi, R. Boutaba, S. L. Waslander, Internet of drones, IEEE Access 4 (2016) 1148–1162.

[10] A. Tahir, Lexicon and heuristics based approach for identification of emotion in text, in: 2018 International conference on frontiers of information technology (FIT), IEEE, 2018, pp. 293–297.

[11] Z. Najam, A. Rafi, Efficient resource utilization in cloud-fog environment integrated with smart grids, in: 2018 International Conference on Frontiers of Information Technology (FIT), IEEE, 2018, pp. 188–193.

[12] Z. Najam, H. Rizwi, Energy efficient localization in wireless sensor networks using computational intelligence, in: 2018 15th International Conference on Smart Cities: Improving Quality of Life Using ICT & IoT (HONET-ICT), IEEE, 2018, pp. 78–82.

[13] J. Akram, A. Javed, S. Khan, A. Akram, H. S. Munawar, W. Ahmad, Swarm intelligence based localization in wireless sensor networks, in: Proceedings of the 36th Annual ACM Symposium on Applied Computing, 2021, pp. 1906–1914.

[14] H. Rizvi, Handover management in 5g software defined network based v2x communication, in: 2018 12th International Conference on Open Source Systems and Technologies (ICOSST), IEEE, 2018, pp. 22–26.

[15] S. Malik, S. Ansari, H. Rizvi, D. Kim, R. Hasnain, Intelligent target coverage in wireless sensor networks with adaptive sensors, in: 2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall), IEEE, pp. 1–5.

[16] M. Mehmood, N. Javaid, S. H. Abbasi, A. Rahman, F. Saeed, Efficient resource distribution in cloud and fog computing, in: International

Conference on Network-Based Information Systems, Springer, 2018, pp. 209–221.

[17] A. Tahir, H. S. Munawar, M. Adil, S. Ali, A. Z. Kouzani, M. P. Mahmud, Automatic target detection from satellite imagery using machine learning, Sensors 22 (3) (2022) 1147.

[18] V. Sharma, G. Choudhary, Y. Ko, I. You, Behavior and vulnerability assessment of drones-enabled industrial internet of things (iiot), IEEE Access 6 (2018) 43368–43383.

[19] M. T. R. Khan, M. M. Saad, M. A. Tariq, D. Kim, Spice-it: Smart covid-19 pandemic controlled eradication over ndn-iot, Information Fusion 74 (2021) 50–64.

[20] H. S. Munawar, A. Z. Kouzani, M. P. Mahmud, Using adaptive sensors for optimised target coverage in wireless sensor networks, Sensors 22 (3) (2022) 1083.

[21] R. Altawy, A. M. Youssef, Security, privacy, and safety aspects of civilian drones: A survey, ACM Transactions on Cyber-Physical Systems 1 (2) (2016) 1–25.

[22] A. Tahir, A. Akram, A. Z. Kouzani, M. P. Mahmud, Cloud-and fog-integrated smart grid model for efficient resource utilisation, Sensors 21 (23) (2021) 7846.

[23] H. S. Munawar, F. Ullah, D. Shahzad, A. Heravi, S. Qayyum, Civil infrastructure damage and corrosion detection: An application of machine learning, Buildings 12 (2) (2022) 156.

[24] S. Peng, Y. Zhou, L. Cao, S. Yu, J. Niu, W. Jia, Influence analysis in social networks: A survey, Journal of Network and Computer Applications 106 (2018) 17–32.

[25] S. Aggarwal, R. Chaudhary, G. S. Aujla, A. Jindal, A. Dua, N. Kumar, 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, 2018, pp. 1–6.

[26] D. Berdik, S. Otoum, N. Schmidt, D. Porter, Y. Jararweh, A survey on blockchain for information systems management and security, Information Processing & Management 58 (1) (2021) 102397.

[27] R. Zheng, J. Jiang, X. Hao, W. Ren, F. Xiong, Y. Ren, A blockchain-based big data model for bim modification audit and provenance in mobile cloud, Advances in Civil Engineering (2019).

[28] R. Shrestha, R. Bajracharya, S. Y. Nam, Blockchain-based message dissemination in vanet, in: 2018 IEEE 3rd International Conference on Computing, Communication and Security (ICCCS), IEEE, 2018, pp. 161–166.

[29] U. Majeed, L. U. Khan, I. Yaqoob, S. A. Kazmi, K. Salah, C. S. Hong, Blockchain for iot-based smart cities: Recent advances, requirements, and future challenges, Journal of Network and Computer Applications 181 (2021) 103007.

[30] R. W. Ahmad, H. Hasan, R. Jayaraman, K. Salah, M. Omar, Blockchain applications and architectures for port operations and logistics management, Research in Transportation Business & Management 41 (2021) 100620.

[31] L. Campanile, M. Iacono, F. Marulli, M. Mastroianni, Designing a gdpr compliant blockchain-based iov distributed information tracking system, Information Processing & Management 58 (3) (2021) 102511.

[32] A. Yazdinejad, R. M. Parizi, A. Dehghantanha, H. Karimipour, G. Srivastava, M. Aledhari, Enabling drones in the internet of things with decentralized blockchain-based security, IEEE Internet of Things Journal 8 (8) (2020) 6406–6415.

[33] T.-H. Kim, R. Goyat, M. K. Rai, G. Kumar, W. J. Buchanan, R. Saha, R. Thomas, A novel trust evaluation process for secure localization using a decentralized blockchain in wireless sensor networks, IEEE access 7 (2019) 184133–184144.

[34] Y. Xu, J. Ren, G. Wang, C. Zhang, J. Yang, Y. Zhang, A blockchain-based nonrepudiation network computing service scheme for industrial iot, IEEE Transactions on Industrial Informatics 15 (6) (2019) 3632–3641.

[35] R. Clarke, L. B. Moses, The regulation of civilian drones' impacts on public safety, Computer law & security review 30 (3) (2014) 263–285.

[36] R. N. Akram, K. Markantonakis, K. Mayes, O. Habachi, D. Sauveron, A. Steyven, S. Chaumette, Security, privacy and safety evaluation of dynamic and static fleets of drones, in: 2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC), IEEE, 2017, pp. 1–12.

[37] R. Goyat, G. Kumar, M. K. Rai, R. Saha, R. Thomas, T. H. Kim, Blockchain powered secure range-free localization in wireless sensor networks, Arabian Journal for Science and Engineering 45 (8) (2020) 6139–6155.

[38] M. Hema Kumar, V. Mohanraj, Y. Suresh, J. Senthilkumar, G. Nagalalli, Trust aware localized routing and class based dynamic block chain encryption scheme for improved security in wsn, Journal of Ambient Intelligence and Humanized Computing 12 (5) (2021) 5287–5295.

[39] J. Yang, S. He, Y. Xu, L. Chen, J. Ren, A trusted routing scheme using blockchain and reinforcement learning for wireless sensor networks, Sensors 19 (4) (2019) 970.

[40] G. Ramezan, C. Leung, Wireless communications and mobile computing, vol. 2018, article id 4029591, Wireless Communications and Mobile Computing (2018).

[41] K. Haseeb, N. Islam, A. Almogren, I. U. Din, Intrusion prevention framework for secure routing in wsn-based mobile internet of things, Ieee Access 7 (2019) 185496–185505.

[42] M. A. Uddin, A. Stranieri, I. Gondal, V. Balasurbramanian, A lightweight blockchain based framework for underwater iot, Electronics 8 (12) (2019) 1552.

[43] Z. Cui, X. Fei, S. Zhang, X. Cai, Y. Cao, W. Zhang, J. Chen, A hybrid blockchain-based identity authentication scheme for multi-wsn, IEEE Transactions on Services Computing 13 (2) (2020) 241–251.

[44] S. Hong, P2p networking based internet of things (iot) sensor node authentication by blockchain, Peer-to-Peer Networking and Applications 13 (2) (2020) 579–589.

[45] G. Rathee, M. Balasaraswathi, K. P. Chandran, S. D. Gupta, C. Boopathi, A secure iot sensors communication in industry 4.0 using blockchain technology, Journal of Ambient Intelligence and Humanized Computing 12 (1) (2021) 533–545.

[46] Y. Tian, Z. Wang, J. Xiong, J. Ma, A blockchain-based secure key management scheme with trustworthiness in dwsns, IEEE Transactions on Industrial Informatics 16 (9) (2020) 6193–6202.

[47] S. I. Khan, F. Ullah, B. J. Choi, Drone-as-a-service (daas) for covid-19 self-testing kits delivery in smart healthcare setups: A technological perspective, ICT Express (2022).

[48] S. Rathore, B. W. Kwon, J. H. Park, Blockseciotnet: Blockchain-based decentralized security architecture for iot network, Journal of Network and Computer Applications 143 (2019) 167–177.

[49] W. She, Q. Liu, Z. Tian, J.-S. Chen, B. Wang, W. Liu, Blockchain trust model for malicious node detection in wireless sensor networks, IEEE Access 7 (2019) 38947–38956.

[50] Y. Ren, Y. Liu, S. Ji, A. K. Sangaiah, J. Wang, Incentive mechanism of data storage based on blockchain for wireless sensor networks, Mobile Information Systems 2018 (2018).

[51] P. Danzi, A. E. Kalør, Č. Stefanović, P. Popovski, Delay and communication tradeoffs for blockchain systems with lightweight iot clients, IEEE Internet of Things Journal 6 (2) (2019) 2354–2365.

[52] Y. Liu, K. Wang, Y. Lin, W. Xu, Lightchain: a lightweight blockchain system for industrial internet of things, IEEE Transactions on Industrial Informatics 15 (6) (2019) 3571–3581.

[53] X. Liang, X. Du, G. Wang, Z. Han, A deep reinforcement learning network for traffic light cycle control, IEEE Transactions on Vehicular Technology 68 (2) (2019) 1243–1253.

[54] A. Rovira-Sugranes, A. Razi, Optimizing the age of information for blockchain technology with applications to iot sensors, IEEE Communications Letters 24 (1) (2019) 183–187.

[55] G. Kolumban-Antal, V. Lasak, R. Bogdan, B. Groza, A secure and portable multi-sensor module for distributed air pollution monitoring, Sensors 20 (2) (2020) 403.

[56] H. S. Munawar, Z. Gharineiat, S. Imran Khan, A framework for burnt area mapping and evacuation problem using aerial imagery analysis, Fire 5 (4) (2022) 122.

[57] P. Sharma, Sharma pk, park jh, Blockchain based hybrid network architecture for the smart city, Future Gener. Comput. Syst 86 (2018) 650–655.

[58] K. He, Z. Wang, D. Li, F. Zhu, L. Fan, Ultra-reliable mu-mimo detector based on deep learning for 5g/b5g-enabled iot, Physical Communication 43 (2020) 101181.

[59] A. Akram, R. H. Jhaveri, M. Alazab, H. Chi, Bc-iodt: blockchain-based framework for authentication in internet of drone things, in: Proceedings of the 5th International ACM Mobicom Workshop on Drone Assisted Wireless Communications for 5G and Beyond, 2022, pp. 115–120.

[60] J. Liang, Z. Xu, Y. Xu, W. Zhou, C. Li, Adaptive cooperative routing transmission for energy heterogeneous wireless sensor networks, Physical Communication 49 (2021) 101460.

[61] W.-C. Chien, H.-H. Cho, C.-F. Lai, F.-H. Tseng, H.-C. Chao, M. M. Hassan, A. Alelaiwi, Intelligent architecture for mobile hetnet in b5g, IEEE Network 33 (3) (2019) 34–41.

[62] Z. Abubaker, N. Javaid, A. Almogren, M. Akbar, M. Zuair, J. Ben-Othman, Blockchained service provisioning and malicious node detection via federated learning in scalable internet of sensor things networks, Computer Networks 204 (2022) 108691.