Computers and Electrical Engineering 99 (2022) 107847

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

A hybrid blockchain method in internet of things for privacy and security in unmanned aerial vehicles network☆

Emad H. Abualsauod

Industrial Engineering Department, College of Engineering, Taibah University, Al Madina Almonawara 41411, Saudi Arabia

ARTICLE INFO

Keywords:
Blockchain
Privacy
Internet of Things
Unmanned Aerial Vehicles
Security
Industry quality

ABSTRACT

Unmanned Aerial Vehicles (UAVs) offer a huge amount of potential in a variety of applications, including healthcare, medical, traffic monitoring, military, and industry. UAVs are deployed in association with the Internet of Things (IoT) to facilitate receivers or end-users at the end for delivering IoT services, resulting in a new research domain. The objectives of this research work are to analyze and classify the peer-reviewed research on UAV IoT frameworks and identify the solution towards challenges related to the overall security including the privacy of the frameworks. In the article, an optimum solution for various security and reliability challenges in UAV-enabled IoT applications is given using a fusion of several methods combining blockchain-based technologies. The results are obtained and compared on different parameters like overall system utility, accuracy, latency, and processing time. The proposed methodology results highlight the improvement and give novel directions toward future work.

1. Introduction

The IoT connects any device to other devices using the Internet as a medium. With the help of mechanical power, the industrial revolution enhanced production, while the next revolution made the Internet a vital tool for global communication between devices such as computers and mobile phones. IoT connected devices have unique identifiers that allow them to interact with other devices on a network of interconnected devices. Eventually, billions of devices would be connected to the Internet, enhancing people's working conditions. Huge amounts of data and codes will travel over IoT-based networks to control and smooth the operation of all connected devices in various locations and environments. With such a large amount of data coming in, there could be a problem with congestion. which can result in increased network delay and a lower delivery ratio.

UAVs offer enormous potential in the public and civil sectors, especially when integrated with the Internet of Things. These are most useful in industrial applications from controlling the disease, delivering pizza and to vacuum-cleaning up ocean waste, and many more. However, several challenges must be addressed before UAVs can be used efficiently to offer robust and dependable context-specific networks. UAV networks can range from slow dynamic to dynamic, with intermittent connectivity and a fluid architecture. UAVs have a wide range of applications such as surveying and mapping, search and rescue, reconnaissance, and IoT connecting UAVs play a big role in such applications and also extend the role in smart healthcare, city and industrial applications, and services [1].

☆ This paper is for special section VSI-suav. Reviews were processed by Guest Editor Dr. Bhisham Sharma and recommended for publication.

E-mail address: eabualsauod@taibahu.edu.sa.

https://doi.org/10.1016/j.compeleceng.2022.107847
Received 29 October 2021; Received in revised form 17 February 2022; Accepted 18 February 2022
Available online 24 February 2022

1.1. Technologies used in IoT

The major part of technologies for IoTs are Radio Frequency Identification (RFID), Barcode, Wi-Fi, wireless, Internet Protocol (IP), ZigBee, Electronic Product Code (EPC), Bluetooth, Actuators, Near-Field-Communication (NFC), Wireless Sensors Network (WSN), Artificial Intelligence (AI) and cloud computing, etc. RFID is the foundation of the IoTs and plays a big role when combined with UAVs. Such technologies discover the information of the tagged object from an internet similar to particular RFID and connect things (physical objects) to the cyber world by tagging different technologies like RFID, barcode, and NFC. Barcode is a technology that encodes numerals & alphabets by using bars and spaces. Wi-Fi communicates with devices with wireless signals whereas Bluetooth is short-range wireless communication technology. ZigBee is a protocol that enhances the features of wireless sensor networks. Near-Field Communication (NFC) is a short-range wireless technology that allows the intuitive initialization of wireless networks. The actuator is a mechanical system component that drives motions. Wireless Sensor Networks (WSNs) are devices that use a wireless link to communicate the data they collect. Artificial Intelligence is a software technology that simulates human intelligence by machines, especially computers. Cloud computing is a remotely accessed storage system. UAVs are made capable of reading these barcodes which are RFID enabled also can communicate to the sensory devices creating wireless sensor networks. But such communication linking also brings the threats related to cyber-attacks like jamming, hijacking, and poisoning of the nodes.

In the present era, security is one of the most important economic and social issues, affecting not only individuals but also institutions, government agencies, and businesses. The issue of how to protect UAV IoT devices from cyber-attacks, for the same, security stands out as the best option. It is the protection of the network system against software or hardware malfunction.

IoT devices are rapidly growing in popularity and have become an integral part of everyone's daily lives. IoT gadgets will be so widespread in the future that people will be unable to imagine their lives without them. A large number of IoT devices are connected to the Internet and transmit large amounts of data, exposing them to security threats. As a result, learning the countermeasures for protection against such crimes is an urgent need. As a result, security remains a major concern that may be addressed through coordinated efforts at all levels. The IoT delivers revolutionary technological advances to everyone's daily lives, making them easier and more comfortable. Traditional security measures will be ineffective in protecting IoT infrastructure. To defend IoT, a consistent protocol and rigid advanced security measures are now required.

1.2. Motivation of the work

UAVs carry a large amount of data through sensor devices and will become increasingly important in future scenarios. From military applications, law enforcement to daily usage the UAV vehicles demand is also rising. Governments all across the world can use blockchain to track the identities of UAVs flying over their territory. The usage of UAVs in urban contexts has accelerated in recent years as their popularity has grown.

Blockchain is new-age technology to build security among UAVs architecture, it establishes a visible and unchangeable method to aid in the mitigation of security risks [2]. With the help of blockchain UAV data storage and verification can be automated, transactions can be automated and also decision-making systems can be automated. This paper discusses the current security and privacy threats in UAV's IoT applications and the role of different technologies to handle such challenges, a novel hybrid methodology is proposed to deal with privacy and security challenges.

The remaining part of the paper is organized as follows: Section 2 describes the related work part of the manuscript Section 3. defines the materials and methods in detail with the proposed scheme. In section 4 comparative analysis and discussion is done with prior state of art followed by the future research challenges in section 5 where possible future research scenarios are discussed. Finally, Section 6 concludes the manuscript.

2. Related work

UAV networks haven't received a lot of attention in the research community, because such networks convey sensitive data and are vulnerable to a variety of attacks, security concerns are a major concern. Many solutions are proposed such as intrusion detection and response system for UAVs and ground stations that detects malicious anomalies that harm the network. A collection of detection and response approaches is proposed to monitor UAVs behaviour and classify them, based on the identified cyber-attack categorized as normal, abnormal, suspect, and malicious.

Emerging technologies, such as 4G/5G networks, have significant potential for UAVs equipped with cameras, sensors, and GPS receivers to supply IoT services from considerable heights, resulting in the creation of an airborne IoT domain. However, several difficulties must be addressed before UAVs can be used, including security, privacy, and management [3].

Authors in [4] to deal with the problem of optimized system utility created a one-side matching method with a greedy algorithm, and the results show betterment towards the increase in resource usage. Another work [5] that concentrates on the power consumption among the resources is presented where several resource blocks deployed in UAVs reduce the per cluster head load in M2M communication. This analysis clearly shows overhead reduction with UAV implementation. A novel work is done by the authors having for detecting malevolent drones and ensure public safety [6]. Authors in [7] uses linear approach with GLCM model, [8] LBP, and [9] NRLBP with again same approach whereas authors in [10] uses polynomial function CJLBP, [11] LTrP, [12] VGG19 all having polynomial model whereas Radial Basis Function (RBF) is used in [13] Alexnet, and [14] Letrist. All of these models used the same approach of getting the topographies as used in the ResNet50 model [6], with Support Vector Machine (SVM)-RBF as a classifier and compared their results in terms of accuracy with Resnet50 as shown in Fig 2. Resnet50 model used Machine Learning (ML) schemes of

SVM RBF kernel aimed at the classification of the data and proved as a better model. Blockchain-based [15] novel work is presented in the field of UAVs by the authors for providing the security under attacks. Another work in the blockchain is presented by the authors of [16] as an Unmanned Traffic Management (UTM)-Chain, a frivolous blockchain-based safety resolution for low-altitude UTM employing hyper ledger fabric. The authors in [17] proposed a solution for enhancing the privacy and security of device data on Blockchain Technology (BCT).

Nowadays, business chains and industry quality are monitored by UAVs, and blockchain as part of such a structure allows for easy identification of the point where an error has occurred, which can be caused by any cyber-attack. Cyber-physical attacks target the physical components of networked systems, such as IoT. The goal of security is to prevent unwanted access to computer networks, software, hardware, and data Table 1. shows the comparative description of different application areas that have changed with IoT involvement.

All these IoT technologies have numerous benefits but side by side there is a cyber threat also that invades user privacy and security Table 2. shows the technology specification comparison for hardware and network wise to highlight the benefits, threats, and attacks.

IoT shows a technological positive promising future where devices will intelligently connect to the network and with other devices anywhere, anytime. In the future, all devices of our daily use will be available on the Internet. The mobile phone will work as a handy remote to control all objects called IoT. A cyber attacker can use a UAV device with sensors to install the malware in IoT devices and then activate them with codes to extract personal information from a smartphone, smartwatch, or another device. The next generation's life will be dependent on cyberspace-based technology [18] mainly the security of IoT and UAVs. Virtual Circuit (VC) devices, such as UAVs, drones, and other IoT-based gadgets, have become more useful in the recent years. These devices are frequently used for aerial surveys insensitive and inaccessible places [19]. To increase the security and privacy of VC devices, a BCT-based solution for device data was deployed [20]. In [21], the authors suggest a blockchain-enabled secure data gathering structure based on a UAV swarm structure, in which data is collected from IoT devices and then transported to the nearest server via the UAV swarm. Before initiating data collection, the UAV swarm shares a common key with the IoT devices to preserve connectivity.

3. Materials and methods

Drones, also known as UAVs, offer immense promise for providing a wide range of practical solutions for smart applications all around the world. Services with cyber security in UAVs IoT frameworks and models are the primary source of concern in UAV-based

Table 1
Comparison of Applications – With and without IoT Technology

Application Area	Existing scenario	IoT Scenario	Advantages
Agriculture	In the present-day scenario of agriculture, the farmer cannot identify the disease of animals, breeds at an early stage	IoT will help the farmers to get intact information about the breeds or animals every minute	Better monitoring, direct communication between consumer and producer
Insurance company	Insurance companies are giving the same rate or premium to all the customers. Whereas some customers very often need this insurance claim.	RFID can be used in the human body or car of the customer to check heart rate, temperature, blood pressure. In-car speed, acceleration, disturbance can be measured. Based on these parameters insurance officer can decide the rate and premium of the customer	Fast access to information, Benefit the insurance company as more customers will join them
Smart Home	The only thing that is done to make our home smart is to have a fire alarm facility. Existing technology like a cell phone can be used to make home smart	IoT makes use of small sensors or RFID in things like refrigerators, lighting, living room for real-time information. If no one is in the room the lights should switch off automatically, a text message is sent to the phone if you forget to off Air Conditioning (AC) or geyser	Safety of homes. Better living saves resources
Smart grid	The conventional method of energy use	Smart energy and meters	Highly reliable, more economic and energy independent
Smart Transportation	Routine transportation system and with or without a traffic light	Ease-of-use	Smart traffic management, parking & Transportation
Smart-City	Unplanned city development. No proper management of waste management and lighting etc.	Superior city planning and rapid services delivery	Waste management, lighting, e-governance & Water supply
Health-Related	Currently, the health of a patient can be monitored if he is physically present in the hospital and continuous manual monitoring of patients is done by the nursing staff. This is not efficient as it leads to wastage of time	In IoT scenarios, mobile phones can be equipped with RFID or sensor equipment to continuously monitor the patient. This scenario will work efficiently in case of an accident	An efficient way of monitoring requires less manpower, fast monitoring, and remote monitoring
Supply chain Information	This sector of supply chain information is usually handled manually. Offline registers are maintained to store the data about the products. This system is less flexible and doesn't have flexibility	IoT can be used in any business related to the supply chain model. It is capable of retrieving all the information regarding things using the RFID mechanism	Less manpower required increases efficiency, dynamic as orders are maintained on the demand basis

Table 2
Technology specific comparison with existing threats and possible attacks

Group	Features	Benefits	Threats	Attacks
Hardware	Distinct identities and auto identification	Swift Information exchange through wireless between tags and readers	Denial of service, Tracking, Hoax/Tricking	Data-sniffing & Counter-feting
RFID	Microcontroller protocol & Radio	Consistent, Low energy consumption and cost	Packets maneuvering	Killer-Bee & scapy
ZigBee	Frequency hopping Spectrum	Safely connect 2-devices wirelessly	Denial of Service (DoS) and eavesdropping	Car Whisperer, Bluebugging
Bluetooth	Sensors & Actuators	Flexibility and Higher latency in communication	Denial of Service and Unfairness	Collision, Jamming, and Tampering
Sensor's node	Wires, Routers & Network adapters	Reliability & improved security, Ease of use	Data manipulation & Extortion hack	Fragile Link and malicious Attacks
Network	Trans receiver and Radio communication	Improved access, easy network expansion, better mobility and collaboration	Misconfiguration	Protocol tunneling
Wired				
Wireless				

IoT applications.

Smart things, transportation, communities, healthcare, personal care, homes, industries, and so on are all examples of IoT applications. Because of the sensitivity of UAV applications, security is a major concern. Appropriate safeguards are necessary to secure acquired data from hackers and fictitious activity by non-authorized users. Machine learning techniques are important in enhancing UAV security, and blockchain is a new technology for decentralized UAVs and security [22]. A fusion of solutions like ML algorithms and blockchain is proposed as a solution to enhance the security of providing services using UAVs in mentioned application areas.

3.1. Sensor clusters in harsh terrains

To handle the problem in a distributed manner, the authors of [4] created a one-side matching method and a greedy algorithm to maximize the data collection utility. The scenarios were simulated in both a grid and a random topology, with UAVs and sensor clusters deployed over a 10 km by 10 km area. Simulations show that UAVs are not always matched with the closest sensor clusters, that the suggested greedy algorithm's solution is best, and that sensed data may be collected effectively.

Table 3 presents the implementation of the greedy algorithm and accordingly raises the system utility and the results achieved reflect that there is increased performance is with the number of clusters. The grid topology implementation analysis for the collection of data where greedy algorithms appear to be far better for the implementation of handling the data collection issue. With the increase in deployment of clusters in the area, greedy algorithms performance also gets improved.

3.2. M2M with UAV methodology

Authors in [5] proposes a new architecture for cluster-based mechanisms with power-efficient Machine-to-Machine (M2M) communication. Many UAVs are defined as airborne base stations in the approach, and they are utilised to collect data from Cluster Heads (CHs), which are a collection of M2M clusters. To reduce the transmit power that CHs used while sustaining the rate necessities of M2M devices, an effective resource and scheduling division technique for CH-UAV communications is provided [16].

The experimental setup consists of resource blocks deployment with 6 and 24 in UAVs, Fig. 1 clearly shows that the number of resource blocks deployed in UAVs reduces the per cluster head load in M2M communication. With the increase of resource blocks, the power consumption of each cluster decreases. This analysis clearly shows that implementing UAVs reduces overhead.

3.3. Resnet50 model

Another study [23] reveals that while drones have many advantages, they also bring substantial obstacles and public concerns that

Table 3
Grid Topology Implementation

Grid Topology Sensor Clusters	25	30	35	40	Algorithms
Approx. System Utility (Mbps)	2.03	2.4	2.77	3.1	**Greedy**
	1.8	2	2.2	2.7	**Random**
	2	2.23	2.6	3	**One-Side**

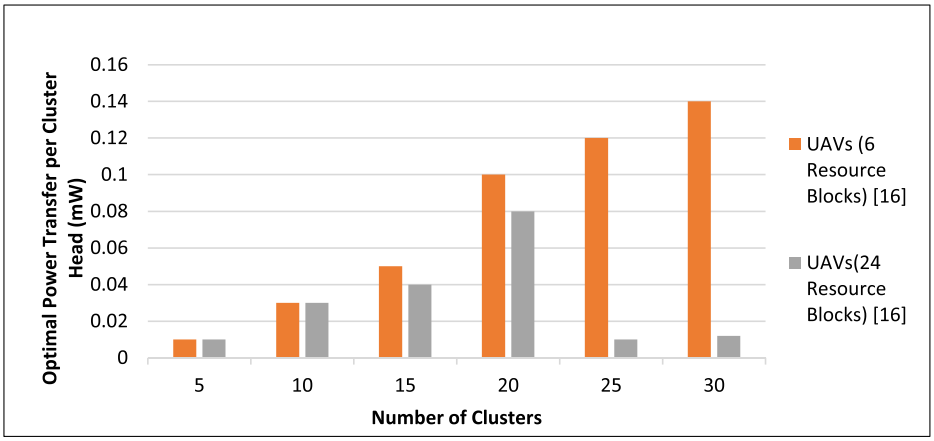

Fig. 1. UAVs performance with resource blocks

must be addressed. A framework for detecting malevolent drones and ensuring public safety is presented as a solution. The proposed model is put to the test on 400 photos that include scale variation, compression, background congestion, blurriness, and poor brightness, among other issues. After obtaining topographies using the ResNet50 model, the data is classified using a Support Vector Machine (SVM) Radial Basis Function (RBF) kernel. This technique had the highest classification precision in the confusion matrix when compared to other more recent models [6].

Fig. 2. presents a comparative study where the Resnet50 model, and is compared with different models having the same SVM classifier, models are categorized into three sections linear, polynomial, and RBF based. Obtained results clearly show that the proposed Resnet50 model gives more accuracy during communication.

3.4. UAV Ad hoc network with blockchain

The communication between UAVs and ground stations can be protected using several security practices such as Named Data Networking (NDN), artificial intelligence, blockchain, and machine learning models. NDN allows for quick and effective distribution of content in mission-critical Unmanned Aerial Vehicle Ad hoc Networks (UAANETs); though, its in-network storing method introduces a novel safety task known as content poisoning. Poisoned content can contaminate router caches and separate effective content in the network, resulting in degradation of service or denial of services attack [15]. To efficiently find poisoned content, an innovative and methodical background that blends Interest Key Content Binding (IKCB), advancing policy, and on-demand authentication is presented Proposed algorithm 1. shows the poisoned content determination IKCB strategy.

Several security threats due to poisoned content are hijacking, alteration attacks led to corrupted content, inauthentic content, and fake content.

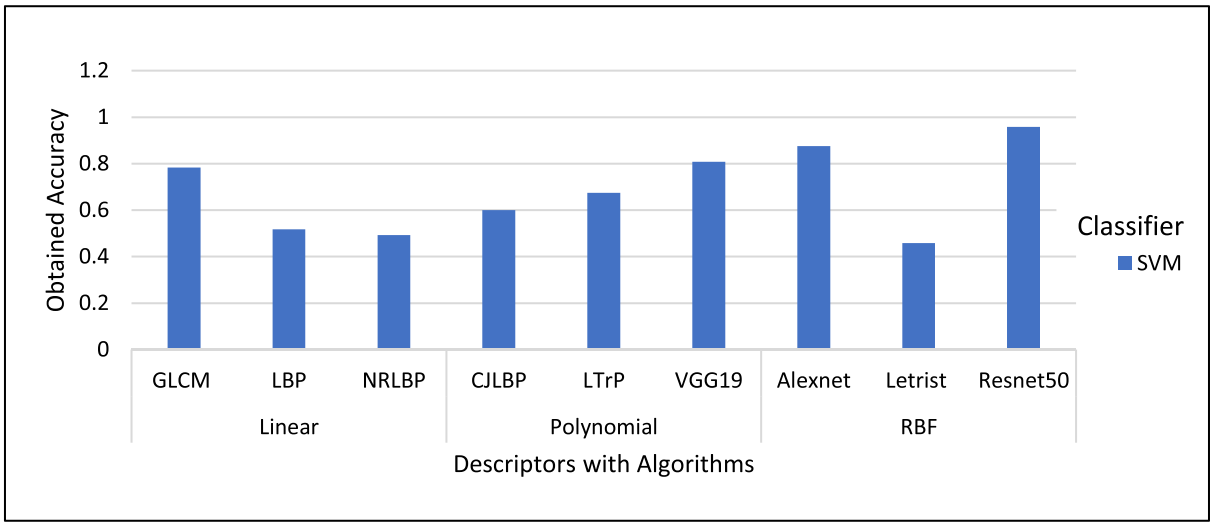

Fig. 2. UAVs performance with descriptors

According to the proposed mechanisms and Interest Key Binding (IKB) latency measurements, legitimate content takes an average of 110 milliseconds to retrieve, but the suggested approach takes just about 15 milliseconds. The average latency of the mechanism aiming towards the 81st–85th content is around 158 milliseconds, which is higher than IKB but lower than the total average latency. According to the findings, the attacker sends out corrupted dynamic material that is undetectable during the standard phase, thus the re-released attention executes on-request sign authentication, with the fiasco conclusion recorded in the FIB entry's previous sign authentication.

3.5. Blockchain-based secure unmanned traffic management

The authors of [16] proposed an Unmanned Traffic Management (UTM) Chain, a frivolous blockchain-based safety resolution for low-altitude UTM employing hyper ledger fabric. UAVs are designed to work within the constraints of computing and storage resources. Hijacking, GPS spoofing, and jamming are all possible attacks on UAVs.

Performance Evaluation of the proposed solution is calculated using equations 1 and 2 are mentioned as:

$$DelayinTransaction = SystemThreshold * ConfirmationTransactionTime - SubmissionTransactionTime \quad (1)$$

$$DelayforRead = ResponseTimeofTransaction - SubmissionTimeforTransaction \quad (2)$$

According to Table 4, the peer's average and maximum CPU use are 7.32 percent and 11.34 percent, discretely. Likewise, the peer's extreme and average memory usages are 81.4 MB and 95.5 MB, discretely. The assembling node's normal CPU and memory utilization were 75.2 MB and 7.53 percent, respectively, indicating that the blockchain network uses fewer resources, is more consistent, and provides a positive user experience.

3.6. Blockchain technology for UAV data

In recent years, the use of equipment like drones, UAVs, and other IoT-based equipment has increased substantially. The principal application for this equipment is aerial measuring in complex and distant ranges. The fact that aggravation and data control issues have grown up to an extent as technology has improved. The authors [17] proposed a solution for enhancing the privacy and security of these device data on BCT. The basic information regarding the instruction to the vehicle (equipment), authenticity, reliability, and vehicle responses is saved in a cloud platform that employs Pentatope-based Elliptic curve cryptography and SHA to protect data privacy. To facilitate smooth BCT transactions, the data is kept on an Ethereum-based public blockchain. The proposed approach is put to the test in a virtual car monitoring system using an IoT-based application.

The graph in Fig. 3 shows that the blockchain increases the latency and processing time which increases overall time consumption, as there is now more latency and processing time due to the involvement of the blockchain.

3.7. Proposed hybrid ML blockchain model

For the implementation of the proposed hybrid method for imparting security in UAVs for IoT services FlyNetSim, an integrated UAV-Network Simulator is selected with python language used for the implementation. Multiple distributed sensors are built over the simulator, the blockchain system is designed as a testbed as a deployment scenario using multiple ML algorithms k-Nearest Neighbours (KNN), Naïve Bayes (NB) with multiclass classifier Onevsrest is embedded in blockchain scenario using API followed by Python scikit library as shown in Fig. 4. Hash functions provide security encryption with blocks in order to implement security and privacy in multiple header blockchain structures. Several of the ML methods discussed are included in the transactions. UAVs with blockchain provide authentication and authorization procedures as well as asymmetrical encryption algorithms, which help to achieve data privacy protection in drone network security.

The proposed methodology is compared over different parameters like system utility, latency, and processing time with overall attack detection accuracy specified in Table 5.

Table 5 presents the success rate of the model where privacy and preservation ratios can be seen with the great reduction in attack rate, it shows how the attacks are now reduced in percentage with such implementation.

Typically, UAVs process the data using complex machine learning techniques on a centralized server. All of the conservative cyberattacks can be used to transfer and store data in UAVs. Despite their massive influence, UAVs rely heavily on intelligent systems that employ machine learning methodologies to make decisions in the absence of people. A distributed machine learning system based on blockchain is presented to improve the reliability of UAVs.

Fig. 5 shows the FlyNetSim simulation over the NS-3 environment, Applications (AP) acting as a base station in the form of sensor devices and multi-UAV nodes connected over the network.

Table 4
Number of users impact on delay

Number of Users	30	50	Transaction Type
Approximate Average Latency	412	454	Invoke
	121	134	Query

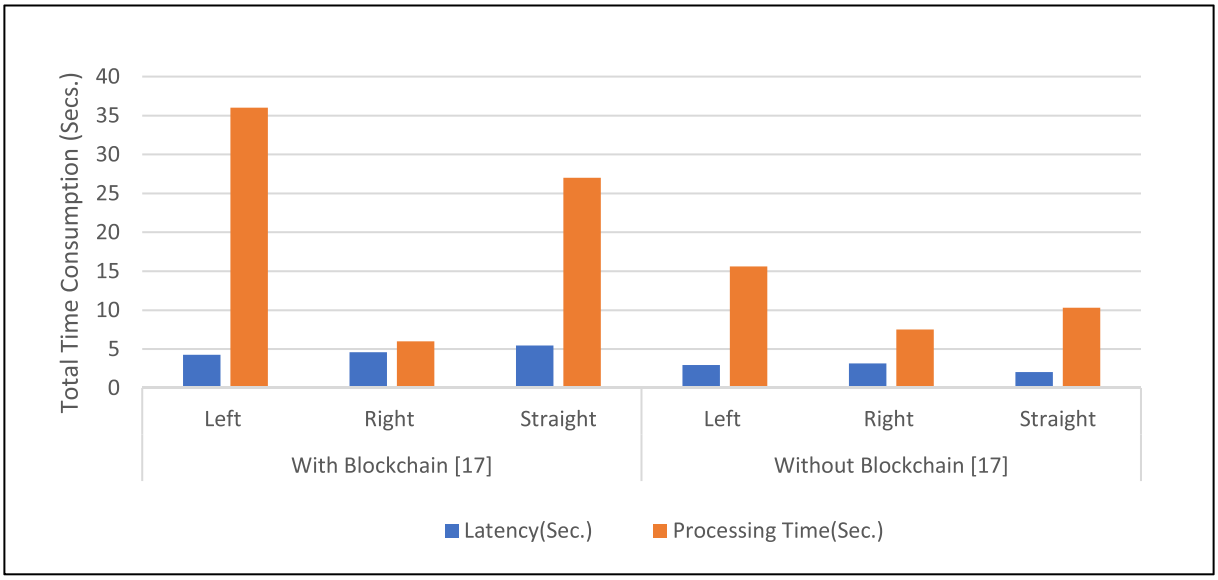

Fig. 3. Time consumption with and without Blockchain

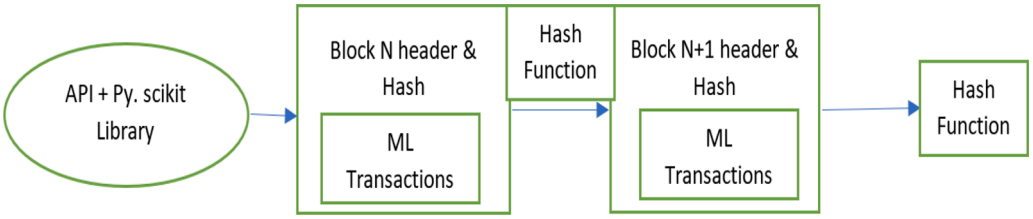

Fig. 4. ML embedded blockchain structure

Table 5
The success rate of the proposed model

Percentage	Privacy	Preservation	Attacks Rate
Success Rate (%)	85	94	10

Proposed Algorithm 1

Determined if there is a local Cluster Space (CS) that is non-omitted by Attention.
Reinstate the replica.
Validating cached content signatures
If there is a local CS
omitted content.
If fails
The router removes information from the CS and notifies the local First Index Base (FIB), which stores the authentication result.
Forwarding access from a Pending Interest Table (PIT) except for the marked poisoned faces, all of the following hops are put out according to interest.
If the upstream data packet matches the formal renewed interest, check the Publisher Public Key Digest (PPKD) as described in the IKCB.
If the aspect after which the data packet arrived has freshly conveyed poisoned insides, perform on-demand signature verification.
If the preceding verification was successful, move downstream and cache the material.
If not, reject the information and alert the local FIB to save the outcome.

In machine learning, accuracy is measured as the percentage of accurate predictions compared to the total number of predictions Equation 3. shows the mathematical equation where TP is True Positive, TN is True Negative, FP as False Positive, and FN as False Negative.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{3}$$

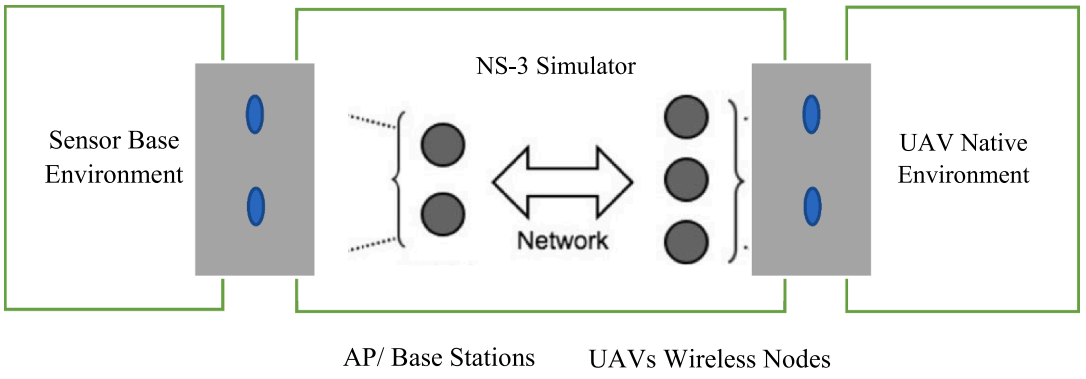

Fig. 5. Multi UAVs Simulation Environment

Precision is a metric for determining the amount to which true positives are correct and calculated as shown with equation 4.

$$Precision = \frac{TruePositives}{TruePositives + FalsePositives} \tag{4}$$

The percentage of successful identification of malicious occurrences is represented by the True Positive Rate (TPR) and calculated as presented in equation 5.

$$TPR = \frac{TruePositives}{TruePositives + FalseNegatives} \tag{5}$$

From the calculations performed the results obtained from the simulators are shown in Fig. 6, where the percentage of different parameters are shown over the three mentioned algorithms selected for the experimentation over the blockchain.

For multi-UAV intelligent decision-making, this technique has the latent to dramatically increase data integrity and storage [24]. The proposed model shows the overall accuracy, precision, and true positive rate of more than 99%.

UAVs are fast evolving and encouraging a wide range of societal uses. Despite this, they are nevertheless subject to a range of security vulnerabilities that put public safety at risk. Security becomes considerably more difficult when they are connected to the Internet since their data stream is exposed to attackers. The significant topic for small unmanned aerial schemes for beyond-line-of-sight actions in precise low-altitude airspace is Unmanned Traffic Management (UTM). Serious security vulnerabilities could lead to fatal consequences if the flight pathway links among drones and ground stations or stations are not protected [16].

The literature study suggests that blockchain is a revolution for UAVs, implementation of UAV raises the processing and increases the latency but threat to cyber-attacks get reduced. Implementation analysis results also show that ML algorithms are also becoming part of UAVs structures to deal with various challenges including cyber threats. As a solution there can be a fusion of ML algorithms

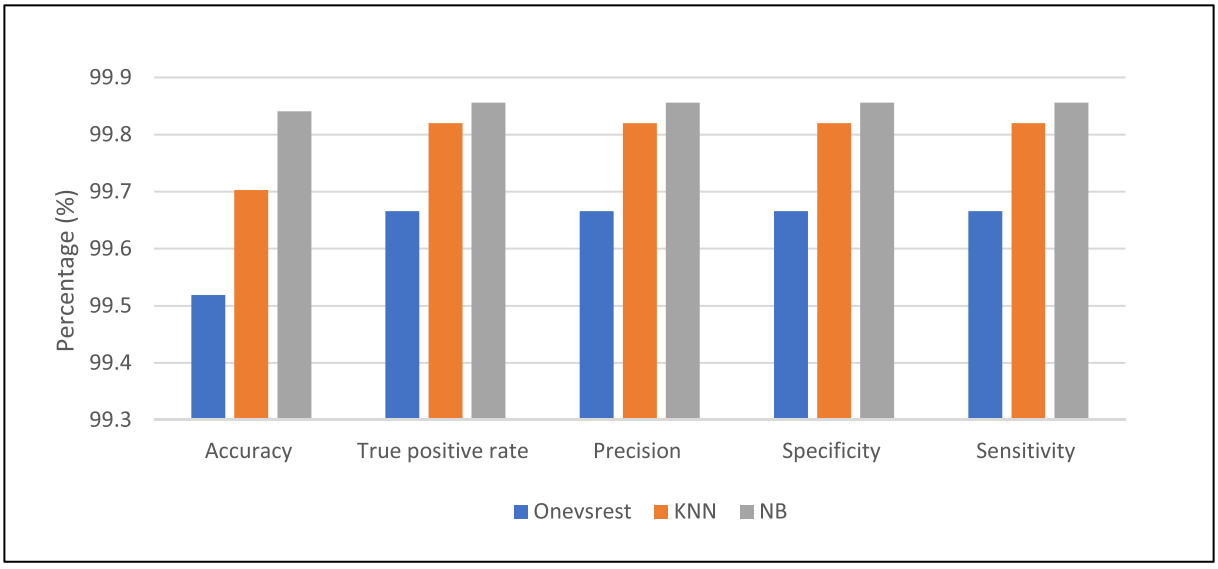

Fig. 6. Proposed model metrics over the machine learning algorithms

with more base stations of UAVs to reduce the cluster overheads [16], and will be implemented with a blockchain solution that helps to deal with security and privacy issues.

4. Comparative analysis and discussion

In the proposed model, multiple nodes are set up in the simulation environment, and mentioned ML techniques are deployed over the nodes, these nodes are simulated as sensor clusters and compared with work in [4]. The proposed approach shows that with the increase in the number of clusters system utility increases as shown in Fig. 7. As the deployment of clusters increases the system utility, a clear rise can be seen. So, it can be presumed that blockchain implementation with ML helps to increase the system's effectiveness.

In Resnet 50 model approach [6] using SVM RBF to predict the accuracy is specified in Fig. 2, when compared with the proposed methodology blockchain with multiple ML algorithms have improved the attack detection accuracy specified in Fig. 8. Most of the used classifier is SVM for the experimentation whereas in the proposed methodology KNN with NB are used and overall increased accuracy can be seen in Fig. 8.

These different UAV nodes transfer data among each other, the power consumption among the nodes is also optimized and can be seen in Fig. 9. Despite using the different machine learning algorithms with the simulation of blockchain the proposed model in Fig. 7 shows that time consumption remains optimal during communication among the nodes. The next parameters are considered latency and processing time over which the performance of the proposed model is tested. Under this parameter blockchain and ML deployed proposed methodology shows a better result in terms of latency and processing time and is also termed as more secure.

As illustrated in Fig. 9, three nodes are implemented under simulation to verify the total processing time and latency. The simulation shows that because of ML algorithms blockchain performance gets better which results in reduced latency and processing time. From Fig. 9 it can be realized that latency varies in range from 3.8 to 4 secs whereas processing time varies from 9 to 15 secs.

UAVs hold a lot of promise for enabling new applications in a range of industries, including armed, security, medication, and surveillance, as well as traffic monitoring. UAVs furnished with cameras, sensors, and GPS receivers have a lot of promise in offering IoT facilities, especially in the industrial and healthcare domains, appreciation of emerging technologies like 4G/5G networks. However, several challenges must be addressed before UAVs may be used effectively, including security, privacy, and management. This article examines the implementation of numerous UAV models that make use of IoT technology, as well as answers to fleet management issues such as aerial networking, privacy, and security.

To support and enable security and effectiveness in terms of utility and accuracy in UAVs, a framework based on the merging of blockchain and machine learning has been presented. The application of blockchain technology in the Internet of Things can overcome security risks. The ability of blockchain security to recover from many cyber-attacks is one of its primary features, its structure is a digital log file that is saved in a chain of blocks and encrypted so that it cannot be changed, and it reduces the risk of a cyber-attack bringing down the entire network. It is the most up-to-date technology that may assist industries improve data security, traceability, privacy, accountability, anonymity, integrity, transparency, resilience, and authentication, as well as long-term sustainability and operational efficiency.

5. Future research challenges

IoT is the latest technological innovation in the world and this technology is making life smarter, simpler, and faster. IoT systems are implanted with sensors, software, and electronics to exchange data and information**.** Implementation of IoT can be seen with the development in agriculture, smart cities, smart transportation, smart-grid, etc. IoT technology brings a revolutionary change in an existing scenario which has an advantage over conventional technology.

Today's privacy, as well as the IoT security of the future, has become a primary concern. It is critical to counter cyber attacks in order to provide effective security. Major Cyber-attacks were seen in financial institutions but now hacking of websites and networks is increasing rapidly for ransom. 95% of cyber-attacks on business networks are the result of successful spear phishing [25].

Security is also required against malicious software like ransomware, trojans, virus, worms, and bots that hack and control the computers and things attached to the network. The number of ransomware families increased by 752% [7]. The impact of cyber-attacks is not only limited to data disruption of computers but can disrupt the banking, rail & air traffic control systems even stock markets.

Hospital care has become dependent on information technology over the previous few years. For privacy, reliability, and effective healthcare delivery, healthcare systems must be secure. Because it is a soft target and a rich data source, the healthcare industry has become a popular target for cyber-attacks. They contain IoT devices and sensitive data, healthcare facilities that are vulnerable to cyber-attacks.

Cyber-attacks have an impact on the national economy and policymakers should realize its consequence in absence of preparedness for cyber-attacks. The futuristic development process is fully dependent on computers and every user should know criminal brain science. Besides this, proper implementation of laws, rules, and regulations under security has not been fully implemented led to an increase in cybercrimes.

There is a need for secure, stable, compatible IoT networks that maintain privacy, longevity, and confidentiality. Following are key challenges among the IoT and UAVs that can act as the future research direction.

- **Insecure firmware/software of IoT devices**

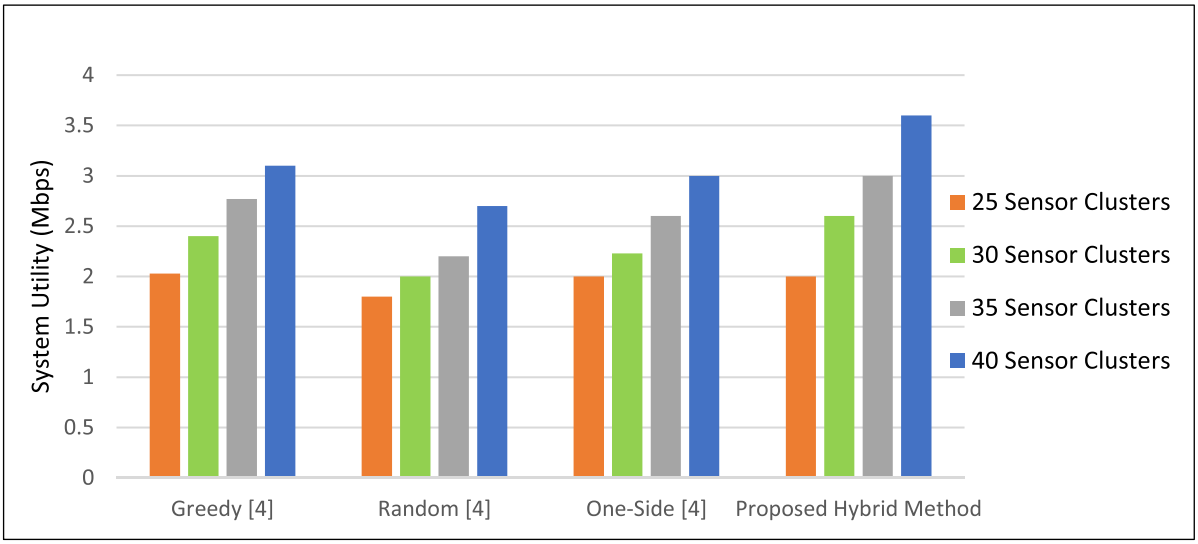

Fig. 7. System Utility of Proposed Method

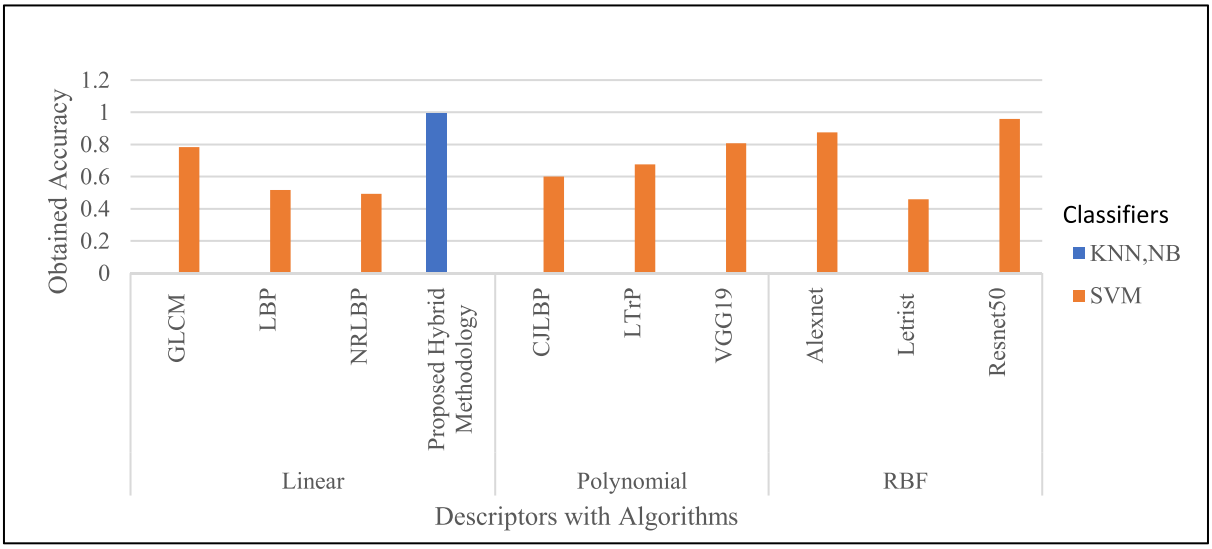

Fig. 8. Proposed model performance with descriptors

A major challenge is malicious software hosted through firmware in IoT devices and can cause security defiance due to weak codes. Frequent updates of firmware and security patches are required. The distribution of a secure firmware update to IoT devices is required, to provide a trusted network to ensure quick firmware updates blockchain technology can be used [26].

- **IoT UAVs with blockchain structure**

Blockchain is different model architecture, implementation with UAVs and IoT framework is a new challenge. It is necessary to explore secure data capture techniques, which can be subjected to future works.

- **IoT UAVs diversity**

IoT applies to different application areas and it becomes difficult for UAVs to serve in such a diverse environment. There are three critical challenges in this area first scalability, which necessitates a scalable network architecture, second intelligence which necessitates a global computing plane and third variety, which necessitates the provision of a diverse set of applications [27].

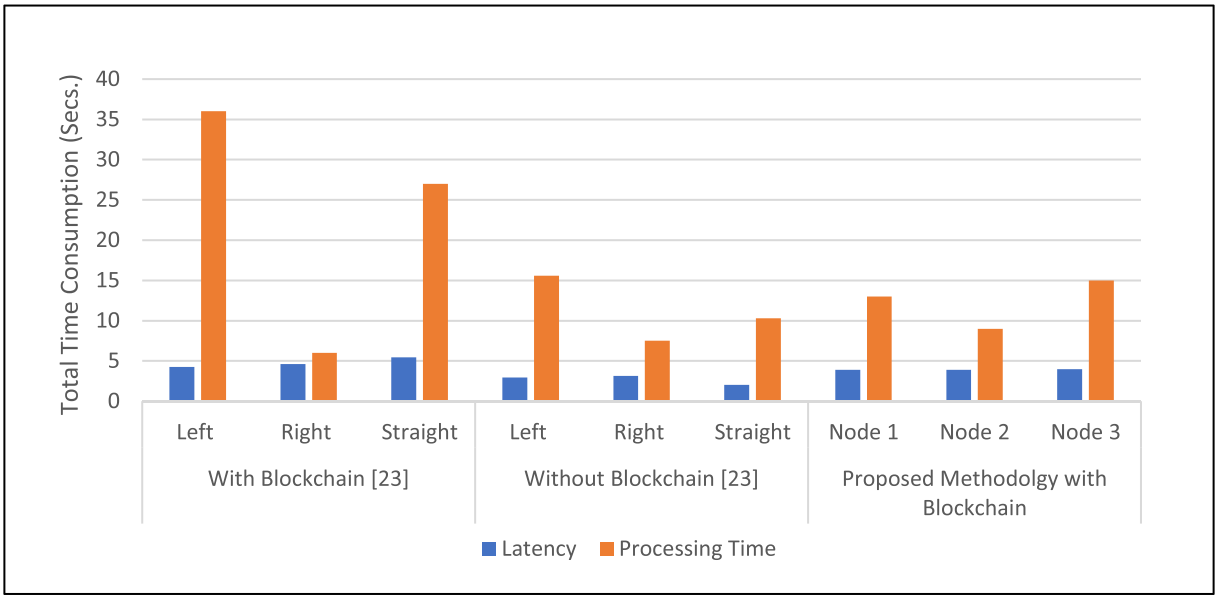

Fig. 9. Latency and processing time with the proposed methodology

- **Congestion control in UAVs**

  It is challenging to build a congestion control protocol that is applicable for all types of applications in UAVs, due to the application particular nature of wireless sensor networks. Congestion avoidance and control primarily try to reduce packet loss that occurs due to congestion, while also ensuring that all network flows receive equal bandwidth allocation [28].

- **Insecure interfaces**

This is the major challenge to IoT devices as insecure interfaces can compromise by malicious nodes in the network and these interfaces are a point of vulnerability that poses threat to working devices.

- **Privacy violation on cloud**

The data from IoT devices is stored in the cloud, where privacy may be violated by malicious service providers on back-end storage. Data privacy is the main challenge for the IoT network layer as sender and receiver communication should be secure.

- **Session hijacking**

Hacker keeps session going with fake messages and it causes denial-of-service in the IoT environment. Attacks against cloud components, on the other hand, might result in enormous losses for cloud service providers and users. By providing the recent threat environment and important cloud attack instances, a complete detection approach is required [29].

- **Buffer overflow attack**

Nodes on the network need to keep some storage space for coming information packets. Hackers may send incomplete packets that lead to a Denial of Service (DoS) attack by rejecting other packets as buffer space already consumed.

- **Routing and collision avoidance in UAVs**

  Routing strategies intend to provide the UAVs with collision-free environments and also to discover not only the optimum as well as the smallest path. Routing strategies are extremely important in the building of a secure path that takes the least amount of time to reach the ultimate destination. Routing is still one of the challenging areas to investigate to find an appropriate path for UAVs [30].

- **Routing Protocol for Low-Power and Lossy Networks (RPL) routing attack**

The IPv6 routing protocol is very vulnerable in an IoT context, and in a Sinkhole attack, a malicious device will be able to tamper

with other nodes' data, causing messages to be dropped and causing delays.

Conclusion

The present research focuses on data privacy issues, data preservation in IoT devices, UAVs, and blockchain technology. Implementation analysis of several security solutions for UAV collaborative applications is performed in terms of ML and blockchain. An effort has been done to present a progressive way of comprehending the numerous tendencies in these methods and highlighting the advantages and limitations that are defined in the design and development of UAV-based applications. A huge number of studies and experiments are carried out to identify the scope of blockchain and machine learning techniques for ensuring security in UAVs. It can be stated that machine learning methods define a critical part in smartly enhancing UAV security, but the blockchain is a relatively new technology for decentralized UAVs and security. By using the hybrid blockchain model with machine learning the overall reliability towards the security of information with the quality of information can be improved. The results obtained demonstrate that ML in collaboration with blockchain can serve the secure and reliable data communication purpose for several UAVs application areas including IoT, such models can support diverse applications especially in healthcare and industries where security and quality can't be compromised.

Declaration of Competing Interest

The corresponding author states that there is no conflict of interest.

References

[1] Skorobogatov G, Barrado C, Salamí E. Multiple UAV systems: a survey. Unmanned Syst 2020;8(02):149–69.
[2] Alladi T, Chamola V, Sahu N, Guizani M. Applications of blockchain in unmanned aerial vehicles: a review. Vehicular Commun 2020;23:100249.
[3] Lagkas T, Argyriou V, Bibi S, Sarigiannidis P. UAV IoT framework views and challenges: Towards protecting drones as "Things. Sensors 2018;18(11):4015.
[4] Pang Y, Zhang Y, Gu Y, Pan M, Han Z, Li P. Efficient data collection for wireless rechargeable sensor clusters in Harsh terrains using UAVs. In: 2014 IEEE Global Communications Conference; 2014. p. 234–9.
[5] Soorki MN, Mozaffari M, Saad W, Manshaei MH, Saidi H. Resource allocation for machine-to-machine communications with unmanned aerial vehicles. In: 2016 IEEE Globecom Workshops (GC Wkshps); 2016. p. 1–6.
[6] Rezende E, Ruppert G, Carvalho T, Ramos F, de Geus P. Malicious software classification using transfer learning of resnet-50 deep neural network. In: 2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA); 2017. p. 1011–4.
[7] Zhang J, Li G-L, He S-W. Texture-based image retrieval by edge detection matching GLCM. In: 2008 10th IEEE International Conference on High Performance Computing and Communications; 2008. p. 782–6.
[8] Wu X, Sun J. Joint-scale LBP: a new feature descriptor for texture classification. The Visual Computer 2017;33(3):317–29.
[9] Ren J, Jiang X, Yuan J, Wang G. Optimizing LBP structure for visual recognition using binary quadratic programming. IEEE Signal Process Lett 2014;21(11):1346–50.
[10] Song T, Li H, Meng F, Wu Q, Cai J. LETRIST: locally encoded transform feature histogram for rotation-invariant texture classification. IEEE Trans Circuits Syst Video Technol 2018;28(7):1565–79.
[11] Murala S, Maheshwari RP, Balasubramanian R. Local tetra patterns: a new feature descriptor for content-based image retrieval. IEEE Trans Image Process: Publ IEEE Sig Process Soc 2012;21(5):2874–86.
[12] Nguyen DT, Zong Z, Ogunbona P, Li W. Object detection using non-redundant local binary patterns. In: 2010 IEEE international conference on image processing; 2010. p. 4609–12.
[13] Shijie J, Ping W, Peiyi J, Siping H. Research on data augmentation for image classification based on convolution neural networks. In: 2017 Chinese automation congress (CAC). IEEE; 2017. p. 4165–70.
[14] Carvalho T, De Rezende ERS, Alves MTP, Balieiro FKC, Sovat RB. Exposing computer generated images by eye's region classification via transfer learning of VGG19 CNN. In: 2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA); 2017. p. 866–70.
[15] Lei K, Zhang Q, Lou J, Bai B, Xu K. Securing ICN-based UAV ad hoc networks with blockchain. IEEE Commun Mag 2019;57(6):26–32.
[16] Allouch A, Cheikhrouhou O, Koubàa A, Toumi K, Khalgui M, Nguyen Gia T. UTM-chain: blockchain-based secure unmanned traffic management for internet of drones. Sensors 2021;21(9):3049.
[17] Ch R, Srivastava G, Gadekallu TR, Maddikunta PKR, Bhattacharya S. Security and privacy of UAV data using blockchain technology. J Inf Secur Appl 2020;55:102670.
[18] Ullah F, Ali Babar M. The journal of systems and software. architectural tactics for big data cybersecurity analytics systems: a review. J Syst Softw 2019;151:81–118.
[19] Cyveillance. (2015). The cost of phishing: understanding the true cost dynamics behind phishing attacks. Retrieved from https://docs.apwg.org/sponsors_technical_papers/WP_CostofPhishing_Cyveillance.pdf.
[20] Viriyasitavat W, Da Xu L, Bi Z, Sapsomboon A. Blockchain-based business process management (BPM) framework for service composition in industry 4.0. J Intell Manuf 2020;31(7):1737–48.
[21] Islam A, Shin SY. Bus: A blockchain-enabled data acquisition scheme with the assistance of uav swarm in internet of things. IEEE Access 2019;7:103231–49.
[22] Syed F, Gupta SK, Hamood Alsamhi S, Rashid M, Liu X. A survey on recent optimal techniques for securing unmanned aerial vehicles applications. Trans Emerg Telecommun Technol 2021;32(7):e4133.
[23] Abbasi K, Batool A, Fawad, Asghar MA, Saeed A, Khan MJ, ur Rehman M. A vision-based amateur drone detection algorithm for public safety applications. In: 2019 UK/China Emerging Technologies (UCET); 2019. p. 1–5.
[24] Khan AA, Khan MM, Khan KM, Arshad J, Ahmad F. A blockchain-based decentralized machine learning framework for collaborative intrusion detection within UAVs. Comput Netw 2021;196:108217.
[25] Awotunde JB, Folorunso SO, Bhoi AK, Adebayo PO, Ijaz MF. Disease diagnosis system for IoT-based wearable body sensors with machine learning algorithm. In: Kumar Bhoi A, Mallick PK, Narayana Mohanty M, de Albuquerque VHC, editors. Hybrid artificial intelligence and IoT in healthcare. Singapore: Springer; 2021. p. 201–22.
[26] Bettayeb M, Nasir Q, Abu Talib M. Hyperledger-Based Secure Firmware Update Delivery for IoT Devices. In: The 7th annual international conference on Arab women in computing in conjunction with the 2nd forum of women in research; 2021. p. 1–5.
[27] Liu Y, Dai H-N, Wang Q, Shukla MK, Imran M. Unmanned aerial vehicle for internet of everything: opportunities and challenges. Comput Commun 2020;155:66–83.

[28] Sharma B, Srivastava G, Lin JCW. A bidirectional congestion control transport protocol for the internet of drones. Comput Commun 2020;153:102–16.
[29] Bhardwaj A, Mangat V, Vig R, Halder S, Conti M. Distributed denial of service attacks in cloud: state-of-the-art of scientific and commercial solutions. Comput Sci Rev 2021;39:100332.
[30] Sharma B, Obaidat MS, Sharma V, Hsiao KF. Routing and collision avoidance techniques for unmanned aerial vehicles: analysis, optimal solutions, and future directions. Int J Commun Syst 2020;33(18):e4628.

Emad Hashiem Abualsuod is an Assistant Professor in the Industrial Engineering Department at Taibah University in Saudi Arabia. He also served as the vice dean for development/quality and the chairman of the Industrial Engineering Department for the College of Engineering at Taibah University. His research interests include quality management, industrial applications, comprehensive airspace, project engineering, lean management, QoS, and IoT.