International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Review of Unmanned Aerial Vehicles/Urban Air Mobility Potential Cyberattacks and Authentication Models: A Way Forward

Aminu Abdulkadir Mahmoud[1], Sofia Najwa Ramli *[1,4], Mohd Aifaa Mohd Ariff [2,4], Chuah Chai Wen [3], Nordiana Rahim [1]

Submitted:13/03/2024 **Revised**: 28/04/2024 **Accepted**: 05/05/2024

Abstract: An Unmanned Aerial Vehicle (UAV) is an aircraft that operates without an onboard human pilot. It can be remotely controlled through a ground control station (GCS), remote control, or onboard computer programs. The elements onboard use a network of sensors to communicate with GCS via a wireless link and thus make the system susceptible to various cyber-attacks. These have magnified concerns, especially in recent years, due to the increased adoption of drones across multiple sectors such as governments, industries, businesses, and transport. Given the paramount need to ensure availability, integrity, and confidentiality, securing these systems is crucial. The attacks may present in forms such as jamming, denial of service, signal attack, eavesdropping, hijacking, man-in-the-middle, intrusion, and malicious application, among others, and these attacks could be mitigated using an effective authentication model. This research reviews several such models, majorly cryptographic, lightweight, and blockchain-based, proposed by different scholars. Considering the importance of blockchain, this research grouped these authentication techniques into two: blockchain and non-blockchain-based. The study shows that all the reviewed authentication techniques have certain limitations, indicating the need for enhancement. Finally, this review identifies the need to consider UAV's peculiarities, operating environment, communication channels, energy consumption (battery life), and blockchain technology to formulate an optimal authentication model.

Keywords: *Unmanned Aerial Vehicle (UAV), Urban Air Mobility (UAM), authentication, blockchain, cybersecurity*

1. Introduction

UAVs have become increasingly prevalent within both the commercial and consumer markets due to their affordability and convenience in the way they offer certain services [1]. Despite their vast advantages, these systems are faced numerous threats to people and properties [2]. Later, the maturity of the UAV development spurred the conception of Urban Air Mobility (UAM), which aims as the next-generation transportation system [3]. The economic viability of UAM cannot be over-emphasized, considering how UAVs ease the ways of doing things in many sectors. However, the infrastructures needed for the UAM to operate in the urban setting as a new transportation system are not available at the moment, and cybersecurity concerns and vulnerabilities remain a point of contention.

The secure operation of UAVs hinges upon robust cybersecurity measures. Any compromise could jeopardize ground personnel, installations, individual privacy, and even the UAVs [4]. Cyberattacks on UAVs often exploit their reliance on wireless communication, making them vulnerable to confidentiality, integrity, and availability incursions. Confidentiality can be compromised through the interception of information by malicious applications, physical hacking, eavesdropping, and personal-based intrusion. In contrast, integrity can be compromised by the fabrication/modification of information through signal attacks and hacking. Availability can be compromised through disturbance, jamming, denial of service, and natural events [4].

However, blockchain technology is highly regarded in almost every aspect of computing, requiring security, authentication, and accountability. The technology allows the anonymous nodes to operate and eliminates the need for a trusted third party (TTP) in transactions. Furthermore, its ledger accessibility is public to the participating entities, and decentralization property ensures that no single party will have a monopoly over the ledger, making it secure and impossible to temper [5].

This research conducts a review of UAV/UAM authentication models proposed by different researchers to evaluate their effectiveness and capabilities. The reviewed models/techniques were categorized as cryptographic, lightweight, and blockchain-based. Furthermore, considering the influence of blockchain, the models were regrouped into blockchain and non-blockchain categories.

[1] *Center of Information Security Research, Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia, Malaysia*
ORCID ID : 0000-0002-5220-3809
ORCID ID : 0000-0002-3615-6360
[2] *Faculty of Electrical and Electronic Engineering, Universiti Tun Hussein Onn Malaysia, Malaysia*
ORCID ID : 0000-0002-6824-3346
[3] *Guangdong University of Science and Technology, China*
ORCID ID : 0000-0003-0800-0147
[4] *Etienne Innovation Sdn. Bhd., Malaysia*
ORCID ID : 0000-0002-3615-6360
ORCID ID : 0000-0002-6824-3346
* *Corresponding Author sofianajwa@uthm.edu.my*

The study reveals that all the models carry certain limitations, which call for improvement. The review further identifies that an optimal authentication model should consider UAV's peculiarities, operating environment, communication channels, energy consumption (battery life), and blockchain technology. Based on the analysis of proposed models, the paper includes recommendations for the future direction of UAV/UAM authentication techniques. The subsequent sections of the paper address fundamentals of UAV/UAM, cyberattacks, blockchain, related work, and a conclusion with future direction.

2. Fundamentals of UAV/UAM

2.1. Unmanned Aerial Vehicles (UAVs)

UAVs can be divided into different classes, with the most common among them being fixed-wing (also referred to as lightweight unmanned airplanes) and rotary-wing (also known as multirotor, rotorcraft, or multi-copter) UAVs [5]. Fixed-wing employs Horizontal Take-Off and Landing (HTOL), while Rotary-wing UAVs utilize Vertical Take-Off and Landing (VTOL), a feature attributable to their propeller types. Rotary-wing (VTOL) is the widely used UAV because it can lift off from a stationary position without needing extra space, compared to the fixed-wing counterparts, which require a runway for take-off and landing. Additional classifications of UAVs exist as well. For instance, the Department of Defense (DoD) classifies UAVs based on speed, weight, and altitude [5]. These classifications consider several factors: purpose and application, flight performance, size and weight, power source, and safety features. Other considerations include durability and weather resistance, control and navigation systems, sensor integration, ease of use and maintenance, and cost and affordability.

2.2. Urban Air Mobility (UAM)

The UAM is envisioned to be the next generation of airborne transportation systems, leveraging unmanned aircraft for urban mobility. With plans for extensive infrastructure development and diversified operations, UAM transportation networks aim to extend their reach to most major cities [6] and [7]. Though UAM operations are similar to general UAV functionality, they have unique characteristics catered to urban and metropolitan environments, including operating at lower altitudes, and providing services such as passenger transport, goods delivery, and other service provision [3].

2.3. Unmanned Aerial Vehicles (UAVs)

UAVs require communication links to communicate with various entities and components both within and outside their systems and with other UAVs. However, there are several issues associated with UAV communication [1] and [4].

- Identification and Control: UAV communicates remotely within its components and with other UAVs, making it vulnerable to attacks by malicious actors. To prevent this kind of attack, UAVs use a unique identification code to verify the genesis of the transmission, and it is done using Radio Frequency Identification (RFID).
- Autonomous UAV: Autonomous UAVs communicate components and entities autonomously with the help of computer programs. The paths are programmed using GPS coordinates and are capable of updating their paths based on real-time data autonomously.
- UAV Swarm: A UAV swarm is called the coordinated communication and function of a group of UAVs, which requires rapid communication and coordination to avoid collisions. Communication among several UAVs can cause traffic congestion, halting all communications and reducing Shannon's capacity.
- Internet of Drones (IoDs): The IoDs communicate using a distributed sensor network and are coordinated like UAV swarms, and IoDs can provide flexibility with the mobile sensor platform. The IoDs can also help to provide unique services in locations that lack internet connectivity.

3. Cyberattacks

Cyberattacks are a significant issue that hindered the public acceptance of Unmanned Aerial Systems (UAS). UAS is a cyber-physical system whose digital components, such as sensors, software, communications, and so on, collaborate to control and monitor the physical components, such as actuators and airframes of UAVs, creating vulnerabilities [8]. These digital components are perpetually exposed to potential cyberattacks, most commonly in the forms of GPS jamming and spoofing, video interception, hijacks via communication sensor spoofing, and so on [8].

Reference [9] also highlighted that UAVs are susceptible to cyber-attacks, which pose threats to their confidentiality, integrity, and availability (CIA) triads. Within the framework of the CIA triad, securing UAVs with robust authentication processes is of paramount importance. This ensures access is granted exclusively to authorized entities and lays the groundwork for effectively implementing confidentiality and availability measures. UAVs' authenticity can be undermined by numerous threats, including but not limited to spoofing, injection, tampering, DoS, and brute-force attacks. Spoofing attacks typically create counterfeit authentication credentials, whereas injection attacks involve introducing malicious code into the UAV system. Tampering attacks seek to alter authentication mechanisms, thereby circumventing security measures. In contrast, DoS attacks aim to inundate the UAV system with excessive requests. Finally, brute-force attacks endeavor to

crack passwords or other authentication credentials by systematically checking all possible combinations [10].

Various robust authentication measures can be employed to counteract many cyberattacks on UAV systems, ranging from two-factor and biometric authentication to encryption, blockchain, and identity-based authentication. The latter utilizes a UAV's identity for authentication, considering various factors such as UAV's peculiarities, operating environment, communication channels, energy consumption, and location. Such an approach helps verify the UAV's identity, thereby ensuring that only authorized entities can access the system. Blockchain technology is favored for its added security layer, decentralized structure, and tamper-proof transaction records.

4. Blockchain Technology (BCT)

4.1. Blockchain Architecture

Blockchain has fundamentally six main layers: the data layer, network layer, consensus layer, incentive layer, contract layer, and application layer.

1. **Data layer:** In this Layer, the data is timestamped and stored within each block's block body and header. The current block header contains the hash of the next block's header and the previous block's hash, while the next block carries the hash of the current block's hash. This linking mechanism creates a chain of blocks, similar to a linked list data structure [5] and [11].
2. **Network Layer:** The Network Layer oversees verifying blockchain transactions and distributing the ledger throughout the network. When a transaction is created, it is sent to nearby nodes for verification based on specific requirements. If the transaction is deemed valid, it is shared with other nodes. However, it is rejected and not recorded if it fails to meet the requirements. This process ensures that only legitimate transactions are added to each node's ledger [5].
3. **Consensus Layer:** This layer uses different consensus algorithms to validate the blocks, order the blocks, and ensure that each node agrees. This is crucial in blockchain operation as the consensus between the participants is the key to avoiding some protocols to ensure consensus among the participating entities. The consensus mechanisms are Practical Byzantine Fault Tolerance (PBFT), Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of State (DPoS), and other consensus algorithms are also used [5].
4. **Incentive Layer:** This layer is responsible for giving the miners rewards (economic gain) in return for the processing power they have invested to mine the blocks. This incentive is in the form of digital currency and aligns with the work done [5].
5. **Contract Layer**: The layer provides programmability to the blockchain and allows for the inclusion of scripts, smart contracts, and algorithms, enabling the execution of complex transactions on the blockchain. Smart contracts are a set of predefined rules executed automatically when certain conditions are met, and they facilitate transactions between two parties involved in the contract [5].
6. **Application Layer:** This layer is the topmost layer of the blockchain, and it is where the blockchain is applied in various fields such as healthcare, transportation, financial institutions, and IoT, among others [5].

4.2. Blockchain Architecture

There are three types of blockchain, and these include public blockchain, private blockchain, and consortium blockchain.

1. **Public Blockchain:** This type of blockchain is open to the public and accessible to anyone interested in transactions. Any party that is validated will receive the transaction's ledger and reward where it is merited. The public blockchain uses Proof of Stake (PoS) and Proof of Work (PoW) to make the transaction successful [11]. In a public blockchain, anyone can participate, cryptocurrency is required, decentralization is high, low throughput, and high energy consumption. This type of blockchain is the most widely used and used by most of the papers reviewed in this research.
2. **Private Blockchain:** This type of blockchain is restricted, and access can only be granted by the system administrator. Its features include full privacy, better scalability, faster speediness, high efficiency, and faster transaction. This kind of blockchain is used by private organizations enterprises where only preselected members can participate in the network [5] and [11].
3. **Consortium Blockchain:** This type of blockchain can organize and manage blockchain networks to share information, improve existing workflows, and ensure transparency and accountability [11]. This research intends to use two private blockchain networks to manage and collaborate as a consortium blockchain to achieve its objectives.

5. Review of Related Work

This research reviews various UAV authentication models and techniques proposed by numerous researchers. These models primarily fall into three categories: lightweight-based, cryptographic-based, and blockchain-based, each to ensure authentication, intrusion detection, and privacy preservation. Given the significant role of blockchain technology in authentication and accountability, the study divides the examined authentication models into non-blockchain-based and blockchain-based authentication models.

5.1. Non-Blockchain-based Authentication Models

This section discusses lightweight, cryptographic, and other non-blockchain-based models and techniques proposed by various researchers. Their goal is to bolster security and efficiency across multiple applications of UAVs through effective authentication. This segment examines the methods, contributions, and limitations of these models.

Reference [12] employed Elliptic Curve Cryptography (ECC), digital signature, and hash function for UAV authentication and traceability to ensure integrity, confidentiality, anonymity, availability, privacy, and defense against repudiation, DoS, and spoofing attacks. The scheme has four entities, i.e., the Trusted Authority (TA) center, which provides public key and private key to the registrants, manufacturer (UAV), player (mobile device) operator of UAV, and GCS. The integrated mentioned techniques used digital signature to ensure non-repudiation between the entities in each phase. And private key is used to sign and transmit a message, and the receiver uses the sender's public key to verify the received message. The scheme is remarkable in tackling repudiation, DoS, and spoofing attacks, ensuring mutual authentication and confidentiality of UAV communication. Its computational cost is also impressive compared to other schemes. But still, much needs to be done to improve the efficiency of the authentication process and further reduce computational costs.

On the other hand, [13] introduced a framework named "SENTINEL" for secure UAV authentication on the IoDs. The framework uses Message Authentication Code (MAC), Elliptic Curve Digital Signature Algorithm (ECDSA), Password Key Derivation Function 2 (PKDF2), and HMAC-SHA-256 techniques to achieve its purpose. It has four identified entities, which include a drone (UAV), Ground Station (GS), Certificate Authority (CA), and operator. The framework used CA to register entities and provide them with the certificate of registration, and these entities use mutual authentication to verify each other before performing any transaction. The framework is relatively lighter and provides mutual authentication between entities using the flight session key. The work also has a faster execution time compared to other schemes on average. However, the authentication procedure needs to be improved to consider the irregularities of the entities involved and identify their possible points of attack.

Reference [14] proposed an improvement over [13]'s framework. Their lightweight authentication protocol safeguards the IoDs in Flying Ad-Hoc Networks (FANETs) against security vulnerabilities, ensuring message integrity, authenticity, and authorization among the participating entities. The protocol is termed as "Hash Message Authentication Code/Secure Hash Algorithmic (HMACSHA1)" and has three identified entities, i.e., drone, Certificate Authority (CA), and Ground Station (GS). Its execution is divided into five phases: registration, key agreement, drone-to-drone authentication, dynamic drone addition, and drone revocation/reissue phases. A cryptographic hash function is used for data protection from adversaries, and a timestamp is used to identify each transmitted message with a predefined time threshold prior to communication with GS. The proposed protocol is commendable in terms of security and privacy preservation, and its capability was verified through Random Oracle Model (ROM) and ProVerit 2.0. The result shows a performance improvement compared to [13] work and other protocols. Similarly, the authentication process still needs to be improved, like that of [13].

Reference [15] presented a lightweight trust-based adaptive identity strategy for UAV authentication in FANETs using ECC. The strategy focuses on securing communication, reducing energy consumption, and minimizing identity authentication frequency between UAVs and Ground Control Station (GCS). The scheme uses the concept of selecting a UAV with the highest trust value from the UAV swarm to authenticate with GCS, which will represent the UAVs. The scheme has four phases: security requirements, the most trusted UAV selection, UAV identity privacy protection, and GCS privacy identity protection. It also involves the choice of local trust value, global trust value, and comprehensive trust value. Analysis using Random Oracle Model (ROM) shows that the scheme provides message identity authentication, privacy protection, traceability, unlinkability, and protection against replay, modification, impersonation, and man-in-the-middle attacks. However, despite the contributions made by this scheme, still more needs to be done concerning the nature and peculiarities of the entities involved for proper identity authentication to reduce the complexity further.

Finally, [16] introduced a mutual authentication scheme to address UAVs' security and privacy concerns and ensure efficient communication in FANETs. The scheme uses a session key authentication protocol and has three identified entities which include Trusted Server (TS), End User (EU), and UAV. It initiates secret key generation and registers participants (EU and UAVs) at TS offline and provides them with credentials. These registered entities will use the credentials to get access to participate in the FANETs transaction seamlessly. The mutual authentication scheme proposed in the paper uses batch authentication techniques to minimize the communication and computation overheads in the resource-constrained FANETs. The proposed scheme ensures that only authenticated UAVs can communicate with each other, which enhances the security of the FANET. Nevertheless, the authentication process of the scheme is deficient, as admitted by the author, and it could be improved using blockchain.

In addition to the aforementioned studies, this review examines other non-blockchain-based authentication model papers. A summary of all non-blockchain-based articles reviewed can be found in Table 1.

The non-blockchain-based models proposed in the reviewed papers successfully address several issues, despite the challenges highlighted in Table 2. The reviewed papers on non-blockchain-based authentication models focus primarily on addressing impersonation, intrusion, spoofing, and privacy preservation. However, the literature does not extensively tackle other attack types like denial of service, eavesdropping, and those targeting communication channels. Moreover, only a fraction of the papers discusses factors such as computational cost, time, and energy requirements, which are pivotal in designing efficient and scalable authentication systems. As such, there remains ample opportunity for further enhancement in these areas to ensure the practicality and feasibility of the proposed model implementation.

Table 1. Summary of Non-Blockchain Proposed Models

Author	***Property/Security Feature Tested***	***Method/Technique***	***Strength/Contribution***	***Weakness/Limitation***
C. L. Chen et al. [12]	Privacy preservation	Privacy preservation, Elliptic Curve Cryptography (ECC), and digital signature.	Mutual authentication provides security against DoS, spoofing, and repudiation attacks. Confidentiality and integrity, computational cost.	The authentication process needs to be improved.
Cho et al. [13]	Level of security of the proposed authentication framework.	Message Authentication Code (MAC), Elliptic Curve Digital Signature Algorithm (ECDSA). Password-based Key Derivation Function 2 (PBKDF) and HMAC-SHA256.	Security and privacy preservation, mutual authentication, and faster execution time compared with other existing protocols.	The authentication process needs to be improved.
Jan et al. [14]	Replay attack, impersonation attack, and man-in-the-middle attack.	Hash Message Authentication Code/Secure Hash Algorithmic (HMACSHA), FANETs, Random Oracle Model (ROM).	Secure communication for UAV, showing some relatively good performance. Security and privacy preservation.	The authentication procedure is not adequately defined.
Kwon et al. [18]	Impersonation attack, man-in-the-middle attack.	Elliptic Curve Cryptography (ECC) and Analysis using Real-or-Random (RoR), Burrows-Abadi-Needham (BAN) logic, and Automated Validation of Internet Security and Protocols and Applications (AVISPA).	Mutual authentication has a lower computational cost than the initial mutual authentication phase. The system is found to be more efficient for the UAM environment when compared with other related work.	The authentication process and the model's resistance against cyber-attacks need to be improved.
Al-Adhami et al. [19]	Confidentiality, integrity, and authenticity.	Secure communication pathways, SHA-1 and Advanced encryption method, DES, Geffe Genetics (GG), RNA-RADG-CBC	Security of UAV communication channels.	The research focused on UAVs' communication channels only.
Tian et al. [20]	Reliability and security of mutual authentication mechanism.	(RRCBC) encryption algorithm. Physical Unclonable Function (PUF), Fuzzy extractor, Unique key, session key, and secret key	Mutual authentication, multi-domain secure communication, and ensures anonymity.	High computational cost
Du et al. [15]	Lightweight design and security of mutual authentication mechanism.	A lightweight mutual authentication based on adaptive strategy, Flying Ad-hoc Networks (FANETs), ECC	Privacy protection, resistance replays attack, man-in-the-middle attack, and impersonation attack. Relatively low computational cost compared with other schemes.	Consideration is not given to the nature of the environment and the entities involved.
Rajasekaran et al. [16]	Mutual authentication, anonymous authentication, and location privacy.	Mutual authentication scheme for privacy in UAV (FANETs), Session key authentication protocol	Privacy preservation and mutual authentication. Resistant against known attacks and relatively low computational cost.	The authentication process is not well clear.

Table 2. Summary of security issues addressed by Non-Blockchain-based reviewed papers

Contribution/Resistance Against Attacks/Complexities	Percentage of research that addressed the issue
Replay	45.5%
Man-in-the-middle	45.5%
Denial of Service (DoS)	9.1%
Eavesdropping	27.3%
Modification	45.5%
Spoofing	54.6%
Impersonation	100%
Intrusion	100%
Privacy Preservation	54.6%
Communication Channels	18.2%
High Computational Cost	27.3%
High Computational Time	27.3%
Energy Requirement	18.2%

5.2. Blockchain-based Authentication Models

This section discusses UAV authentication models based on blockchain technology, as proposed by various researchers.

Reference [21] proposed a lightweight blockchain-based authentication mechanism for IoT systems, which ensures mutual authentication and access control. The mechanism decentralizes its function via fog computing and a public blockchain, restricting communication to only authenticated entities by the blockchain. It uses Elliptic Curve Digital Signature Algorithm (ECDSA) for generating public and private keys. It operates on two primary layers: the device layer and the fog layer, with three types of communication (device-fog, fog-fog, and device-device). The device layer is where an IoT device is registered and deployed, while the fog layer is a blockchain-enabled network of fog nodes that work together in coordination. The mechanism leverages blockchain and fog computing, provides mutual authentication and security against known attacks, and performs relatively well compared to other schemes. Despite its notable features, the authentication procedure did not consider the vulnerabilities and points of attack of the entities involved, the channels in which they communicate, and the model's evaluation procedure is not clearly defined.

Later, [22] proposed a blockchain-empowered policy enforcement system designed to restrain unauthorized access to private and restricted areas, ensure policy compliance, and facilitate collision-free flights. The proposed method has three layers, a physical layer that deals with drone management and a service management layer that manages drone service and is responsible for providing drone services to customers/clients upon request. This will, in turn, communicate to a blockchain network and service enforcement layer, where private blockchain is used to enforce compliance based on smart contracts. A drone operator can initiate a flight by sending a request to the system with their digital signature. The system would then use the blockchain to verify the signature and authenticate the identity of the operator. Similarly, when a service provider wants to offer drone-based services, they would need to provide their digital signature to the system, which would be used to authenticate their identity. This authentication process ensures that only authorized entities are allowed to participate in the system, reducing the risk of unauthorized drone flights or services and keeping records of all transactions. Nevertheless, the work lacks a thorough evaluation of its authentication and verification performance to ascertain its efficiency.

Reference [23] introduced a blockchain-based architecture to secure data dissemination within the IoDs ecosystem to ensure data confidentiality, integrity, and authenticity. The proposed architecture separates the data portion of the blockchain (block ledger) from the block header and stores it off-chain using public blockchain and cloud infrastructure. New drone registration is necessary for legitimate access control, identity management, and traceability, and interactions occur as blockchain transactions. A lightweight consensus mechanism is used that involves stochastic selection and transaction signing to ensure each drone has control of its block. Additionally, the architecture addresses the increasing storage requirements by using data compression with the shrinking block mechanism, providing secure data dissemination at a low overhead cost compared to other approaches.

Another research proposed by [25] involves a stateless blockchain for UAV networks that employ triply aggregable sub-vector commitment for authentication and a dynamic proof of trust consensus mechanism. The system has two phases and four roles, where a blockchain client program is deployed to register UAVs and initialize the network. The registration server constructs security parameters using the Hyperelliptic Curve Public Key Cryptosystem (HECC). According to simulation results, the system performs better than some authentication methods in terms of single-point authentication, latency, and impersonation detection but has a relatively high computational cost.

Additionally, [17] introduced an innovative, blockchain-based, task-oriented authentication model. This model aims to ensure stable networks and provide authenticated and secured communication within dynamic and complex networks. Utilizing a lightweight authentication protocol, the model facilitates both group and intra-group mutual authentication in a UAV environment. The authentication process is divided into group and intra-group authentication, employing a two-stage framework and two lightweight authentication protocols. A trust management component assesses the trustworthiness of a UAV based on its historical behavior and performance. It then assigns a trust score, determining the UAV's authentication level for subsequent tasks. Despite offering a secure, reliable, and customizable authentication mechanism for task-oriented UAV groups, the model's efficacy in resisting known cyberattacks has not been adequately evaluated.

In addition to the papers discussed above, several other blockchain-based authentication models were reviewed, as summarized in Table 3.

Table 3. Summary of Blockchain Proposed Models

Author	***Property/Security Feature Tested***	***Method/Technique***	***Strength/Contribution***	***Weakness/Limitation***
Khalid et al. [21]	Data confidentiality, data integrity, and authentication.	Public blockchain, and Elliptic Curve Digital Signature Algorithm (ECDSA).	Provides authentication and security against known attacks and performs relatively well compared to other schemes. Mutual authentication and access control.	The authentication procedure needs improvement, and the evaluation procedure is unclear.
Aujla et al. [26]	Secure communication (authentication & encryption), secure sharing of information, replay attack, DoS attack, and secure storage.	Consortium Blockchain, and PoW consensus mechanism.	Provide security against spoofed signal attacks, GPS signal attacks, and device-to-device communication attacks.	High computational cost, and energy is not given consideration.
Rahman et al. [22]	Blockchain-based policy enforcement, secured data sharing, and authentication & authorization.	Mechanism to ensure privacy and restrict unauthorized access and Private Blockchain	Authentication and drone flight compliance with a smart contract using blockchain.	The performance of the system was not adequately evaluated to ascertain its efficiency.
Golam et al. [27]	Security, scalability, and efficiency.	User authentication mechanism to checkmate unauthorized access. Public Blockchain, and IoMT	Provides security in the military network and prevents cyberattacks and reduces data transmission delay and enhances the validation process.	The proposed technique considers only device-to-device communication in the military network.
Singh et al. [23]	The paper did not specify the tested features.	Architecture for distributed access control and identity management for IoD. Blockchain, public key, and compression mechanism.	Provides security against GPS spoofing, Hardware trojans, and falsified information.	The authentication procedure needs to be improved. It has high computational cost.
Han et al. [28]	Identity management, authentication, and security.	Consortium blockchain, and consensus mechanism (PBFT).	It has advantages in UAV identity management, UAV authentication, scalability, and secure transmission of communication data. Solve a single point of failure problem.	High computational cost and high authentication time.
Javed et al. [29]	Authentication of drones, certification management, secure communication, access control, and non-repudiation.	Hyperelliptic Curve Cryptography (HECC), Blockchain concept as a Certificate Authority (CA), and a Transaction as Certificate (TC) to facilitate transactions in blockchain without CA or TTP.	Security against replay, device impersonation, man-in-the-middle, malicious deployment, DoS, and de-synchronization attacks.	High computational cost, the research did not consider energy consumption and the diversities of the participating entities and their peculiarities.
Kong et al. [25])	Mutual authentication between UAV and base station, secure communication, resistance against replay attacks, man-in-the-middle	A blockchain-based proof of trust authorization consensus mechanism.	Performs well in terms of single-point authentication, latency, and impersonation detection.	High computational cost

	attacks, DoS attacks, security, and computational efficiency.			
Andola et al. [30]	Authentication and authorization of drones, secure communication, and privacy preservation.	Non-Interactive Zero Knowledge Proof (NIZKP), Bilinear map, Unforgeability Signature (Un-Sig), Unlikability in Ciphertext (UN-C).	Distributed authentication and non-disclosure of the identity of the sender and receiver.	High computational cost
A. Chen et al. [17]	Task-oriented authentication, blockchain-based authentication, secure data transmission, authentication efficiency, and tamper-proof-authentication.	A lightweight authentication protocol for group and intra-group mutual authentication in a UAV environment. ECC, ECDHE, AES, ECDLP	The analysis demonstrated that the proposed model offered a lightweight and secured authentication for task-oriented UAV groups.	The scheme is not properly evaluated to ascertain its actual performance.

The blockchain-based models proposed in this study demonstrate a promising approach to addressing various problems, notwithstanding the identified challenges, as summarized in Table 4. This study reviewed and analyzed ten (10) blockchain-based model papers. Their strategies for handling security attacks and complexities suggest significant advancements compared to non-blockchain-based models. As demonstrated in Table 4, all ten papers addressed impersonation and intrusion, signifying these issues' importance within the realm of blockchain-based models. Furthermore, every paper tackled privacy preservation and modification issues, while over 80% managed replay, man-in-the-middle attacks, denial of service (DoS) attacks, and eavesdropping.

However, as inferred from Table 4, less emphasis is given to communication channels that are susceptible to most of the stated attacks and energy requirements. Addressing the security of communication channels is crucial because they can be vulnerable to various types of attacks, such as eavesdropping, data tampering, unauthorized access, signal jamming, and other forms of communication-based threats. Ensuring the security of these channels would guarantee the integrity, confidentiality, and availability of transmitted data within the UAVs/UAM system. Nevertheless, these aspects received less attention in the reviewed papers. While the papers addressed high computational costs and time, and 86% managed spoofing, protecting communication channels and energy efficiency aspects remain relatively under-researched.

In summary, the result implies that the literature provides substantial coverage to most types of attacks and complexities in blockchain-based models, particularly in modification and privacy preservation. However, it also reveals the relatively less attention given to securing communication channels and energy requirements in the UAVs/UAM environment.

Table 4. Summary of security issues addressed by Blockchain-based reviewed papers

Contribution/Resistance Against Attacks/Complexities	Percentage of research that addressed the issue
Replay	80%
Man-in-the-middle	80%
Denial of Service (DoS)	80%
Eavesdropping	80%
Modification	100%
Spoofing	86.7%
Impersonation	100%
Intrusion	100%
Privacy Preservation	100%
Communication Channels	33.3%
High Computational Cost	53.3%
High Computational Time	53.3%
Energy Requirement	26.7%

6. Conclusion and Future Direction

This study categorizes the reviewed papers into two main groups: non-blockchain and blockchain-based authentication models. Each proposed model or technique's

contributions, limitations, and efficacy were analyzed, focusing on its ability to address or resolve specific problems or issues. Across all papers reviewed, noticeable advancements were achieved in mitigating known cyberattacks (including replay, man-in-the-middle, DoS, impersonation, intrusion, modification, eavesdropping, and more), managing computational complexities, and optimizing energy consumption. Moreover, blockchain-based models were found to be more effective in resisting attacks, preserving privacy, and resisting attacks on communication channels. Therefore, the research recommends using blockchain-based authentication models for UAVs/UAM to ensure secure and authenticated communication, reliability, availability, and confidentiality.

6.1. Acknowledgment

This research is supported by Universiti Tun Hussein Onn Malaysia (UTHM) through TIER 1 (vot Q139).

References

[1] N. Barrera, Unmanned Aerial Vehicles. New York: Nova Science Publisher, 2021.

[2] M. Alwateer, S. W. Loke, and N. Fernando, "Enabling drone services: drone crowdsourcing and drone scripting," IEEE access, vol. 7, pp. 110035–110049, 2019, doi: https://doi.org/10.1109/ACCESS.2019.2933234.

[3] A. C. Tang, "A review on cybersecurity vulnerabilities for urban air mobility," in AIAA Scitech 2021 Forum, 2021, p. 0773. doi: https://doi.org/10.2514/6.2021-0773.

[4] M. Ináncsi, "Cybersecurity Challenges of the Civilian Unmanned Aircraft Systems," 2022, doi: https://doi.org/10.32567/hm.2022.2.14.

[5] T. Alladi, V. Chamola, N. Sahu, and M. Guizani, "Applications of blockchain in unmanned aerial vehicles: A review," Vehicular Communications, vol. 23, p. 100249, 2020, doi: https://doi.org/10.1016/j.vehcom.2020.100249.

[6] M. C. Ertürk, N. Hosseini, H. Jamal, A. Şahin, D. Matolak, and J. Haque, "Requirements And Technologies Towards Uam: Communication, Navigation, And Surveillance," in 2020 Integrated Communications Navigation and Surveillance Conference (ICNS), IEEE, 2020, pp. 2C2-1. doi: https://doi.org/10.1109/ICNS50378.2020.9223003.

[7] McKinsey & Company, "Study on the societal acceptance of Urban Air Mobility in Europe," Cologne, Germany, May 2021. Accessed: Jul. 04, 2023. [Online]. Available: https://www.easa.europa.eu/en/full-report-study-societal-acceptance-urban-air-mobility-europe.

[8] R. Altawy and A. M. Youssef, "Security, privacy, and safety aspects of civilian drones: A survey," ACM Transactions on Cyber-Physical Systems, vol. 1, no. 2, pp. 1–25, 2016, doi: https://doi.org/10.1145/3001836.

[9] H. Wang, H. Zhao, J. Zhang, D. Ma, J. Li, and J. Wei, "Survey on unmanned aerial vehicle networks: A cyber physical system perspective," IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1027–1070, 2019, doi: https://doi.org/10.1109/COMST.2019.2962207.

[10] Y. Mekdad et al., "A survey on security and privacy issues of UAVs," Computer Networks, vol. 224, p. 109626, 2023, doi: https://doi.org/10.1016/j.comnet.2023.109626.

[11] P. Paul, P. S. Aithal, R. Saavedra, and S. Ghosh, "Blockchain Technology and its Types—A Short Review," International Journal of Applied Science and Engineering (IJASE), vol. 9, no. 2, pp. 189–200, 2021.

[12] C.-L. Chen, Y.-Y. Deng, W. Weng, C.-H. Chen, Y.-J. Chiu, and C.-M. Wu, "A traceable and privacy-preserving authentication for UAV communication control system," Electronics (Basel), vol. 9, no. 1, p. 62, 2020, doi: https://doi.org/10.3390/electronics9010062.

[13] G. Cho, J. Cho, S. Hyun, and H. Kim, "SENTINEL: A secure and efficient authentication framework for unmanned aerial vehicles," Applied Sciences, vol. 10, no. 9, p. 3149, 2020, doi: https://doi.org/10.3390/app10093149.

[14] S. U. Jan, F. Qayum, and H. U. Khan, "Design and analysis of lightweight authentication protocol for securing IoD," Ieee access, vol. 9, pp. 69287–69306, 2021, doi: https://doi.org/10.1109/ACCESS.2021.3076692.

[15] X. Du, Y. Li, S. Zhou, and Y. Zhou, "ATS-LIA: A lightweight mutual authentication based on adaptive trust strategy in flying ad-hoc networks," Peer Peer Netw Appl, vol. 15, no. 4, pp. 1979–1993, 2022, doi: https://doi.org/10.1007/s12083-022-01330-7.

[16] A. S. Rajasekaran, A. Maria, F. Al-Turjman, C. Altrjman, and L. Mostarda, "Anonymous mutual and batch authentication with location privacy of UAV in FANET," Drones, vol. 6, no. 1, p. 14, 2022, doi: https://doi.org/10.3390/drones6010014.

[17] A. Chen, K. Peng, Z. Sha, X. Zhou, Z. Yang, and G. Lu, "ToAM: a task-oriented authentication model for UAVs based on blockchain," EURASIP J Wirel Commun Netw, vol. 2021, pp. 1–15, 2021, doi: https://doi.org/10.1186/s13638-021-02039-6.

[18] D. Kwon et al., "Design of secure handover

authentication scheme for urban air mobility environments," IEEE Access, vol. 10, pp. 42529–42541, 2022, doi: https://doi.org/10.1109/ACCESS.2022.3168843.

[19] A. Al-Adhami, R. K. Hasoun, E. K. Gbashi, and S. Hassan, "A secure communication protocol for civil drones," Indonesian Journal of Electrical Engineering and Computer Science, vol. 27, no. 3, pp. 1490–1501, 2022, doi: http://doi.org/10.11591/ijeecs.v27.i3.pp1490-1501.

[20] C. Tian, Q. Jiang, T. Li, J. Zhang, N. Xi, and J. Ma, "Reliable PUF-based mutual authentication protocol for UAVs towards multi-domain environment," Computer Networks, vol. 218, p. 109421, 2022, doi: https://doi.org/10.1016/j.comnet.2022.109421.

[21] U. Khalid, M. Asim, T. Baker, P. C. K. Hung, M. A. Tariq, and L. Rafferty, "A decentralized lightweight blockchain-based authentication mechanism for IoT systems," Cluster Comput, vol. 23, no. 3, pp. 2067–2087, 2020, doi: https://doi.org/10.1007/s10586-020-03058-6.

[22] M. S. Rahman, I. Khalil, and M. Atiquzzaman, "Blockchain-powered policy enforcement for ensuring flight compliance in drone-based service systems," IEEE Netw, vol. 35, no. 1, pp. 116–123, 2021, doi: https://doi.org/10.1109/MNET.011.2000219.

[23] M. Singh, G. S. Aujla, and R. S. Bali, "Derived blockchain architecture for security-conscious data dissemination in edge-envisioned Internet of Drones ecosystem," Cluster Comput, vol. 25, no. 3, pp. 2281–2302, 2022, doi: https://doi.org/10.1007/s10586-021-03497-9.

[24] L. Kong, B. Chen, and F. Hu, "Blockchain-Assisted Adaptive Reconfiguration Method for Trusted UAV Network," Electronics (Basel), vol. 11, no. 16, p. 2549, 2022, doi: https://doi.org/10.3390/electronics11162549.

[25] L. Kong, B. Chen, F. Hu, and J. Zhang, "Lightweight Mutual Authentication Scheme Enabled by Stateless Blockchain for UAV Networks," Security and Communication Networks, vol. 2022, 2022, doi: 10.1155/2022/2330052.

[26] G. S. Aujla, S. Vashisht, S. Garg, N. Kumar, and G. Kaddoum, "Leveraging blockchain for secure drone-to-everything communications," IEEE Communications Standards Magazine, vol. 5, no. 4, pp. 80–87, 2021, doi: https://doi.org/10.1109/MCOMSTD.0001.2100012.

[27] M. Golam, R. Akter, E. A. Tuli, D.-S. Kim, and J.-M. Lee, "Lightweight Blockchain Assisted Unauthorized UAV Access Prevention in the Internet of Military Things," in 2022 13th International Conference on Information and Communication Technology Convergence (ICTC), IEEE, 2022, pp. 890–894. doi: https://doi.org/10.1109/ICTC55196.2022.9953024.

[28] P. Han, A. Sui, and J. Wu, "Identity Management and Authentication of a UAV Swarm Based on a Blockchain," Applied Sciences, vol. 12, no. 20, p. 10524, 2022, doi: https://doi.org/10.3390/app122010524.

[29] S. Javed et al., "An efficient authentication scheme using blockchain as a certificate authority for the internet of drones," Drones, vol. 6, no. 10, p. 264, 2022, doi: https://doi.org/10.3390/drones6100264.

[30] N. Andola, Raghav, V. K. Yadav, S. Venkatesan, and S. Verma, "SpyChain: A lightweight blockchain for authentication and anonymous authorization in IoD," Wirel Pers Commun, vol. 119, pp. 343–362, 2021, doi: https://doi.org/10.1007/s11277-021-08214-8.