Blockchain: Research and Applications 7 (2026) 100341

Contents lists available at ScienceDirect

Blockchain: Research and Applications

journal homepage: www.journals.elsevier.com/blockchain-research-and-applications

Research Article

BUS-health: Blockchain and UAV-integrated smart medical supplies

Mohtasin Golam, Md Facklasur Rahaman, Md Raihan Subhan, Dong-Seong Kim, Jae-Min Lee *

Department of IT Convergence Engineering, Kumoh National Institute of Technology, Gumi 3917, Republic of Korea

ARTICLE INFO

Keywords:
Blockchain
Bloom filter
Smart healthcare
Smart contract
Tactile Internet (TI)
Medical supplies
Unmanned aerial vehicles (UAVs)

ABSTRACT

Unmanned aerial vehicles (UAVs) have recently sparked attention in the logistics supply chain. However, using UAVs in logistics has challenges related to security, data integrity, and trustworthiness in the healthcare industry. To address these issues, this paper introduces a blockchain-integrated scheme to improve the security and trustworthiness of medical supply delivery by leveraging UAVs. Blockchain, a distributed ledger system, enables transparent and reliable participant interactions. The proposed approach employs a sophisticated two-phase verification mechanism to tackle security concerns. The initial phase employs α-hash bloom filter to verify the integrity of data and identify any unauthorized senders. In the second step, digital signature methods authenticate the sender's identity, guaranteeing the data's integrity and prohibiting unauthorized entry. Smart contracts ensure transactions maintain trustworthiness, data integrity, and security without alteration. The InterPlanetary File System (IPFS) protocol addresses storage cost issues. Introducing the 5G-enabled Tactile Internet (TI) enhances communication by being more responsive and efficient. The proposed approach creates a credit scoring mechanism for UAV role selection to improve the delivery process swiftly. The scheme surpasses traditional systems in key performance metrics, and comparing the model's validity with several existing schemes illustrates the proposed scheme's efficacy and feasibility. This scheme could efficiently tackle challenges in providing unmanned medical supplies in smart healthcare systems using blockchain, smart contracts, IPFS, and TI.

1. Introduction

The healthcare industry has experienced a substantial shift due to technological progress, moving from traditional paper records to the era of artifical intelligence (AI)-driven medical prediction [1]. The COVID-19 pandemic served as a clear indication of the weaknesses present in conventional healthcare logistics. The fundamental difficulties related to traditional healthcare logistics during pandemics were complex and diverse. Enforced lockdowns and travel restrictions, which were put in place to mitigate the transmission of the virus, frequently result in delays to transportation systems. Although telemedicine and electronic health records have made significant progress, the transportation of vital medical supplies still faces the risk of congestion and delays [2]. Moreover, the significant challenge of transporting medicine during a pandemic lies in navigating the unpredictable demand and supply chain disruptions to ensure the timely and efficient delivery of critical medical supplies [3]. East Africa, and Kenya specifically, faced significant challenges with essential medical supplies, including inadequate deliveries, ineffective logistics systems, and wastage [4]. In addition, conventional approaches frequently depend on human staff to convey medical resources, thus subjecting them to the potential hazard of getting the virus while in transit. The implementation of lockdowns resulted in road closures, travel restrictions, and staff shortages, which substantially negatively impacted the transportation of vital medical supplies, putting patient care at risk [5]. In critical, time-sensitive circumstances, delays in delivering crucial medical supplies can have devastating effects.

Beyond that, relying on human labor to manage and distribute medical resources poses substantial risks for the spread of infections and the depletion of the workforce owing to illness or quarantine measures. These constraints underscore the immediate requirement for a supply chain that is more robust and adaptable to the ever-changing demands of a pandemic situation [6]. This emphasizes the importance of employing creative strategies to anticipate and navigate global health crises. Smart technologies are transforming the logistics of pandemics by guar-

* Corresponding author.
E-mail addresses: golam248@kumoh.ac.kr (M. Golam), facklasur@kumoh.ac.kr (M.F. Rahaman), raihan@kumoh.ac.kr (M.R. Subhan), dskim@kumoh.ac.kr (D.-S. Kim), ljmpaul@kumoh.ac.kr (J.-M. Lee).

https://doi.org/10.1016/j.bcra.2025.100341
Received 29 March 2024; Received in revised form 17 January 2025; Accepted 15 April 2025

Available online 14 July 2025

anteeing the effective and secure transportation of medical supplies. The Internet of Things (IoT) combines sensor technologies to provide real-time tracking and inventory management analytics [7]. AI and blockchain technology use real-time data to perform predictive analytics and provide safe management of supply chains during pandemics [8]. Unmanned vehicles and robots are transforming the process of delivering medical supplies, reducing the risk of human exposure to potentially contaminated items [9]. By incorporating these intelligent technologies, the logistics industry may see a substantial overhaul during a pandemic, safeguarding healthcare professionals, promoting a more secure work environment, and guaranteeing the adequate transportation of essential medical resources. This facilitates the development of a healthcare logistics system that is more robust and flexible.

Unmanned aerial vehicles (UAVs) are a rapidly developing technology that will significantly transform the healthcare industry by offering a flexible and adaptable alternative to traditional ground transportation [10]. UAVs are vital for efficiently transporting medical supplies, blood products, vaccinations, and laboratory specimens, particularly in distant or inaccessible regions [11]. They exhibit unparalleled proficiency in delivering crucial medical supplies without the limitations of human interaction and road congestion, providing a scalable answer to ongoing healthcare logistical difficulties. UAVs are especially advantageous for overseeing the transportation of pharmaceuticals that are sensitive to temperature and for quickly delivering emergency medical equipment. Amid pandemics, UAVs circumvent road congestion and function in restricted areas, leading to expedited and dependable transportation of essential medical supplies to healthcare institutions [12]. The autonomous nature of UAVs minimizes the likelihood of healthcare professionals being exposed to risks, safeguarding people and guaranteeing the uninterrupted provision of vital medical services [13]. UAVs are easily adaptable to changing demands, which means they can be swiftly deployed and adjusted to provide essential supplies to regions most in need at any given moment.

Despite the transformative potential of drone-based healthcare delivery, substantial roadblocks emerge in the form of cybersecurity vulnerabilities. Significant vulnerabilities in commercial UAVs have been found by researchers, leaving them vulnerable to hacking attempts that could compromise patient privacy, flight safety, and private medical data [14]. These attacks can potentially cause financial disruptions, cargo losses, and legal issues, but more importantly, endanger patient lives through delayed or tampered medical supplies [15]. Robust security protocols are essential for drone-based medical delivery systems since the absence of such restrictions could result in unauthorized access and jeopardize security. Malicious individuals could exploit these weaknesses through path diversion attacks, resulting in erroneous or delayed deliveries of crucial medical supplies [16]. Blockchain technology effectively solves these weaknesses due to its immutability and decentralization, which offers robust protection against hackers [17,18]. Further research is necessary to investigate the successful integration of blockchain technology into this burgeoning industry, given its ability to solve these fundamental security requirements. This paper proposes blockchain technology as a potential solution due to its inherent strengths, such as immutability, ensuring data integrity, and decentralization, making it tamper-proof.

1.1. Literature review

In article Ref. [19], Cheema et al. proposed a secure drone delivery system for medical items using Ethereum technology to maintain data integrity throughout delivery. The authors improve security and identify unwanted access by using smart contracts to register and verify drones, warehouses, medical supplies and a machine-learning-based intrusion detection system. However, longer authentication periods on the public Ethereum network, increased transaction prices, and higher user numbers need greater authentication efficiency and transaction management improvements.

In Healthcare 4.0, Aggarwal et al. [20] proposed a three-tiered drone-based system for secure and discreet medical supply transfer using blockchain networks and drones. The authors improve data integrity and efficiency while permitting remote medical service access using public key infrastructure (PKI) for communication security and PoW for data verification. However, drone sensor privacy, blockchain scalability, and storage costs need improvements in sophisticated privacy-preserving methods and drone route planning algorithms.

According to Sarvesh et al. [21], the MedUAV system used blockchain technology to revolutionize emergency medical supply delivery via a decentralized autonomous organization. MedUAV enables medicinal distribution network transparency and trustworthiness by using smart contracts to document transactions on the Polygon blockchain. However, network congestion and smart contract vulnerabilities necessitate mitigation and comprehensive blockchain platform testing.

Gupta et al. [22] proposed GaRuDa, a blockchain-based drone delivery method for Healthcare 5.0 applications, which combines 5G Tactile Internet (TI) for ultra-low latency communication. GaRuDa improves healthcare delivery network connectivity and lowers expenses using InterPlanetary File System (IPFS) for data dissemination and smart contracts for automated payments. However, the infrastructure maintenance restricts drone flight durations, and data privacy issues need further study into sustainable infrastructure and privacy-preserving systems.

Alsamhi et al. [23] offered a blockchain-based architecture for pandemic drone management, ensuring secure and transparent medical supply delivery and monitoring. Despite data security and drone cooperation benefit, real-time data accuracy and scalability issues need additional study into consensus methods and drone computing.

In response to the COVID-19 epidemic, Navaz et al. [24] suggested a blockchain-based architecture for coordinating a decentralized network of drones for public health reasons. Although it improves data security and transparency, scaling and ethical data privacy problems need careful attention and pilot tests to determine applicability and integration with drone traffic control technology.

Cui et al. [25] explored the integration of UAVs with public vehicles (PVs) for delivery purposes to improve transport system efficiency and increase public transit revenue. However, the payload capacity and range restrictions of UAVs make them unsuitable for long-distance logistical operations.

According to Verma et al. [26], VaCoChain combined consortium blockchain with 5G-enabled UAVs for faster delivery and real-time vaccination data monitoring. Despite the advantages, such as speedier delivery and counterfeit prevention, its infrastructure costs and UAV restrictions need additional study into communication security and quantum-based key distribution.

The survey results in Table 1 indicate that blockchain technology is essential for enhancing the security and dependability of healthcare delivery systems through UAVs. Besides, Ala et al. [27] developed a fuzzy multi-objective optimization model for sustainable healthcare supply chain network design, leveraging techniques such as the Multi-Objective Gray Wolf Optimizer (MOGWO), Non-Dominated Sorting Genetic Algorithm-II (NSGA-II), and epsilon constraint methods to minimize costs and environmental impacts while maximizing the social benefits under uncertainty. However, the primary drawback of their work is the lack of real-time tracking and transparency in managing healthcare supply chain operations, let alone in emergency cases in remote areas.

Wang et al. [28] developed an AI-driven secure robotic delivery system incorporating multilevel cooperative authentication (voiceprint and face recognition) and noncooperative facial recognition to enhance the security and efficiency of last-mile autonomous delivery systems, tested on a Turtlebot3 robot with lightweight machine learning algorithms like CNN-XGBoost and GhostNet. However, the limitation of this paper is the reliance on centralized servers for communication and authentication, which is vulnerable to data breaches and inefficiencies.

Table 1
Comparative survey of existing blockchain-integrated UAV-based healthcare-providing services.

Ref.	Block-chain type	Smart contract type	Encryption/de-cryption type	Authenti-cation	Hashing	Network type	Limitation	Target application
[19]	Public, private, consortium	Ethereum (EVM)	Asymmetric (PKI)	Digital sig-natures, UAV ID authentica-tion	SHA-256, Merkle Hash Tree	5G, WiFi, bluetooth	Increased authentication time with a growing number of users, transaction fees on the public Ethereum network	Medical supplies
[20]	Not specified	Ethereum (EVM), SC for identity management and privacy preservation of UAVs	Asymmetric (PKI)	Digital sig-natures, UAV ID authentica-tion	SHA-256, Merkle Hash Tree	5G, WiFi, bluetooth, radio com-munication	Scalability limitations, potential storage cost issues, privacy concerns from drone sensors	Path planning for healthcare 4.0
[21]	Public blockchain on the polygon main network	EVM-based smart contracts	Asymmetric (PKI) with digital signatures (DS)	Digital signatures (DS), UAV ID	SHA-256, Merkle Hash Tree	5G, WiFi, bluetooth	Reliant on blockchain platform performance (potential congestion) and requires further smart contract vulnerability testing	Medical supplies
[22]	Not specified	Ethereum-based smart contracts	Asymmetric public/private key infrastructure (PKI) with SHA-256	Public key infrastruc-ture (PKI)	SHA-256	5G-enabled Tactile Internet	Infrastructure maintenance cost, limited drone flying time, data privacy concerns	Healthcare 5.0
[23]	Not specified	Ethereum smart contracts	Asymmetric (PKI)	DSs using PoW with SHA-256	Secure Hash Algorithm (SHA-256) with Merkle Root Hash (MRH)	WiFi, blue-tooth, cellular (e.g., 4G, 5G), and radio com-munication	Real-time data quality of new drones, resource constraints on drones, scalability, and consensus algorithms	Combat COVID-19 and future pandemics
[26]	Public blockchain	Ethereum smart contracts using solidity	Asymmetric (PKI)	DS using public key infrastruc-ture (PKI)	SHA-256, Merkle Hash Tree	WiFi, blue-tooth, cellular communi-cation (4G/5G)	High infrastructure cost, limited UAV capacity, and range, weather dependence	Vaccine distribution

Gupta et al. [29] developed a conceptual framework for resilient information systems (RIS) integrated with AI to mitigate supply chain disruptions, leveraging AI's capabilities in data acquisition, self-learning, and scenario modeling to enhance supply chain robustness, reduce risks, and support dynamic decision-making during disruptions like COVID-19 and natural disasters. The limitation of this work is the lack of real-time, decentralized data sharing and physical adaptability to sudden disruptions in supply chain logistics.

Lau et al. [30] proposed a blockchain-based messaging and information-sharing system for the air cargo supply chain, leveraging smart contracts and a decentralized architecture to enhance communication efficiency, data transparency, and trust among stakeholders while reducing messaging transaction costs and addressing complex connectivity issues. The paper's main drawback is its focus on messaging and information sharing without addressing real-time physical delivery and dynamic response capabilities.

Koshta et al. [15] investigated the barriers to adopt delivery drones in the rural healthcare supply chain (RHSC) using the Grey-DEMATEL technique. It identifies the lack of government regulations as the most critical challenge, with limited load-carrying capacity and low flight range as prominent causal barriers. By facilitating the integration of delivery drones into RHSC, the study contributes to achieving Sustainable Development Goal 3, which aims at ensuring good health and well-being while improving healthcare delivery and accessibility in rural regions. However, the proposed system advances beyond the limitations of the referenced study by introducing a blockchain-enabled UAV optimization framework tailored for rural healthcare delivery that emphasizes real-time operational efficiency through a dynamic UAV credit scoring mechanism. This integration ensures transparency, adaptability, and enhanced reliability in addressing logistical challenges, making our framework more robust for practical deployment in complex healthcare supply chains.

Blockchain's qualities, such as immutability, smart contracts, and decentralization, provide solutions to authentication, data integrity, scalability, and privacy difficulties. It facilitates user management, minimizes transaction fees, and enables safe interchange and storage of data. Based on the survey results, the proposed approach would contribute to accomplishing these objectives. Thus, the proposed BUS-Health integrates blockchain with UAVs and TI to construct a robust medical supply scheme for smart healthcare. The fundamental contributions of this study are as follows:

- This paper proposes a blockchain-enabled UAV-integrated medical supply system for smart healthcare designed for emergencies. Furthermore, introducing the TI improves communication by increasing responsiveness and efficiency.
- The research utilizes smart contracts to provide an efficient and trustworthy transactional procedure. In addition, the contract has an access control system that assigns specific responsibilities to patients and healthcare providers.
- This research introduces a two-phase verification approach to strengthen data integrity and privacy. The role selection strategy of the UAV described in this article improves operational management efficiency.
- Finally, this study utilizes a bloom filter data structure to enhance transactional efficiency by reducing execution time over-

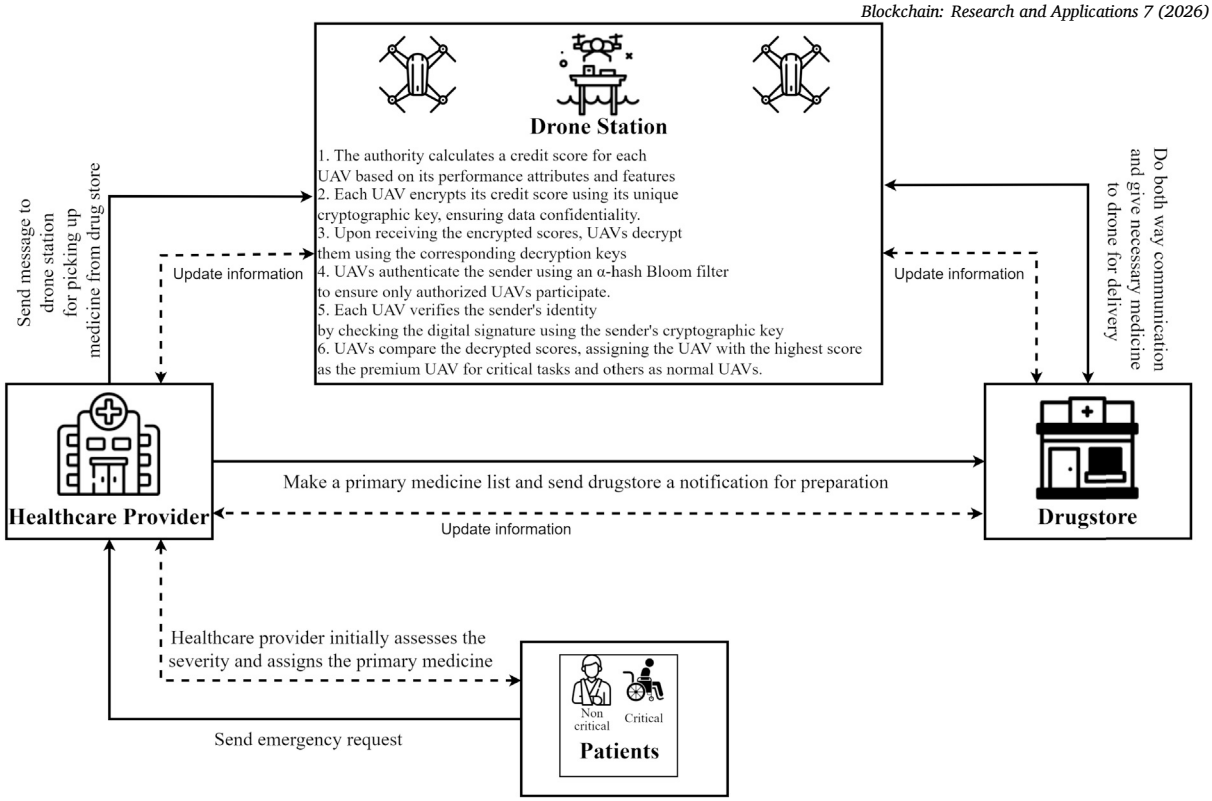

Fig. 1. Schematic representation of the blockchain-integrated unmanned aerial vehicle (UAV)-based medical delivery system.

head and proposes incorporating IPFS for data storage to overcome blockchain storage limitations.

The remainder of this article is as follows: Section 2 presents a detailed explanation of the proposed scheme. Section 3 presents a comprehensive analysis of the results, comparing them with previous techniques and discussing smart contract implementation. Finally, in section 4, the concluding statement is provided, and future directions are discussed.

2. Proposed methodology

This section provides a detailed overview of the proposed blockchain-based, secure UAV-assisted delivery system explicitly designed for medicare supplies in emergencies where traditional delivery is inconceivable. The proposed scheme transforms medical supply delivery in smart healthcare using a blockchain-integrated system with UAVs, as illustrated in Fig. 1. The system initiates the following workflow upon receiving a medical assistance request via a web-based or mobile application linked to the blockchain network. The healthcare provider first assesses the patient's condition to determine the severity of the emergency. Based on this assessment, the provider categorizes the patient as a critical or regular case. For critical emergencies, the healthcare provider promptly generates a list of primary required medical supplies and sends this list to the drug warehouse. Simultaneously, the drone station ($\eth_5$) is notified to deploy the fastest available drone for emergencies. A similar process is followed for non-emergency cases, but an average-speed drone is assigned instead. The drug warehouse and the $\eth_5$ confirm their tasks through the blockchain network, ensuring transparency and accountability. The drug warehouse prepares the medical supplies and confirms readiness. Upon receiving the confirmation, the $\eth_5$ dispatches the drone to collect the supplies. Once the drone has secured the medical supplies, it navigates to the patient's location using pre-determined coordinates. Throughout the flight, the drone's status and location are continuously monitored and recorded on the blockchain to ensure real-time tracking and data integrity. Upon reaching the destination, the drone confirms the delivery status and returns it to the system. The patient then verifies receipt of the medical supplies via the application, completing the transaction. Furthermore, the patients' and other entities' data are properly hashed before being fetched into the blockchain network [31].

Subsequent sections delve deeper into each phase's functionalities and workflow, comprehensively understanding the proposed scheme's operational framework. This detailed explanation underscores the proposed scheme's sophistication and effectiveness as a blockchain-based solution for secure healthcare supply.

2.1. General overview

The proposed scheme aims to efficiently and securely deliver medical supplies to emergency patients. Every entity, including drugstores, users, and UAVs, must register with a healthcare organization. The authority obtains delivery information and stores it in the IPFS using blockchain technology and a smart contract mechanism. Every UAV generates a cryptographic key and distributes it to the governing authority. The authority transmits encrypted data utilizing a shared key, decrypts the data using the identical shared key, and verifies the sender's identity using the α-hash bloom filter. Subsequently, the data is shared with the authority server Δ, where the sender's identity is verified, and the necessary data is prepared for inclusion in the blockchain. This network provides secure standards for drugstores, users, and UAVs to register with a central healthcare authority, guaranteeing authentication and authorization. The system employs encryption and shared keys to ensure security. Every UAV creates a distinct shared key for encrypting delivery data, which is subsequently sent to the Δ of the regulating authority for verification.

2.2. Integration of blockchain, TI, and UAV delivery

Combining blockchain technology, TI, and UAV delivery systems represents a significant development in smart healthcare, allowing for agile, adaptive, and highly portable healthcare solutions. UAVs are essential in this system since they communicate via low-power channels for immediate contact and assistance in healthcare services. Blockchain technology provides a decisive solution by reducing unwanted access and security breaches via improved security standards [32]. This ensures the safety of UAV operations and builds confidence in the system, especially in payment procedures related to UAV deliveries. A 5G-enabled TI is suggested to enhance the low latency and communication overhead. The combination of low latency and high reliability guarantees that healthcare applications stay operational and responsive, critical for timely healthcare delivery and intervention. The smart healthcare framework utilizes each technology's distinct advantages to improve the provision and adaptability of healthcare services, especially in remote locations or emergency scenarios. The approach handles significant concerns in healthcare logistics, such as security weaknesses and the need for swift response, using the collective capabilities of blockchain, TI, and UAV technology.

2.3. Architectural model

The proposed scheme's architectural design comprises three distinct phases: UAV registration, UAV role selection, and two-phase verification. Each phase plays a crucial role in the system's overall operation.

2.3.1. UAV registration

To ensure secure communications, each UAV must complete a registration process in the proposed architecture and obtain a private key. The key is derived from several elements, including the UAV's MAC address ($\widehat{mac}_{\partial}$), timestamp ($\tau_{\check{s}}$), and a randomly created salt hash ($\hat{S}_{h^\circ}$). Salt hashing prevents pre-computed hash attacks by ensuring unique salts produce distinct private keys, even if two UAVs have the same MAC addresses and timestamps. This enhances password security against brute-force efforts. The hash, denoted as (h°), signifies the generated hash. The following mathematical equation concisely defines the procedures included in generating a private key:

$$h^\circ = \mathbb{H}(\widehat{mac}_{\partial} \parallel \tau_{\check{s}} \parallel \hat{S}_{h^\circ}) \tag{1}$$

In this equation, ($\mathbb{H}$) signifies a cryptographic hash function that transforms the input of the UAVs ($\widehat{mac}_{\partial}$), ($\tau_{\check{s}}$), and ($\hat{S}_{h^\circ}$) by merging them through the operation of concatenation represented by ($\parallel$). Moreover, a private key (ρ_k) is derived from (h°), and a corresponding public key (ϱ_k) is derived from (ρ_k), ensuring a robust mechanism for UAV identity verification and secure communication.

To facilitate delivery operations, the Δ stores the delivery area's coordinates, specifically the longitude ($\overleftarrow{lon}$) and latitude ($\overrightarrow{lat}$) of the delivery location, ($\hat{S}_{h^\circ}$), $\widehat{mac}_{\partial}$, and ϱ_k. The Δ then generates a trust token for that area, which is utilized for communication purposes. The establishment of the trust token generation process can be expressed as follows:

$$(\mathfrak{T}) = \delta(\iota_{[\overleftarrow{lon},\overrightarrow{lat}]}, \hat{S}_{h^\circ}, \widehat{mac}_{\partial}, \varrho_k) \mid \delta : (x,y)^* \mapsto (x,y)^\iota \tag{2}$$

In this equation, (δ) represents the trust token generation that combines the mentioned elements to produce the trust token ($\mathfrak{T}$). Let us assume (ι) is the set of coordinates (x, y) on the elliptic curve. In addition, the Δ securely stores this data in the ledger using a smart contract, and a (ϱ_k) is utilized as an identifier for the UAV. The trust token is vital in establishing a secure communication framework for UAVs and facilitating the efficient delivery of medical supplies. Deploying a security-centric system is crucial in the healthcare industry, as the timely and safe conveyance of medications leads to patient care outcomes.

2.3.2. UAV role selection

Before commencing the delivery process, the authority determines each UAV's specific function based on its capabilities, such as maximum speed, payload capacity, battery power, CPU, RAM, and other relevant factors. The evaluation employs a credit scoring mechanism, quantifying each UAV's performance potential by assigning a weighted significance (ω) to these attributes, providing a quantifiable indicator of its performance capabilities. The credit score ($\mathfrak{c}_s$) of a UAV is computed using a mathematical formula that integrates these parameters, reflecting their contributions to efficient and successful deliveries. The following equation is utilized to compute the credit score:

$$\mathfrak{c}_s = \omega_1 \cdot \nu_{max} + \omega_2 \cdot \rho_{cap} + \omega_3 \cdot \beta_{pow} + \omega_4 \cdot \mathbb{C} + \omega_5 \cdot \mathfrak{R} + \sum_{i=1}^{n} \omega_{o_i} \cdot O_i \tag{3}$$

These weights ($\omega_1, \omega_2, \omega_3, \omega_4, \omega_5$, and ω_{o_i}) are allocated according to maximum speed ($\nu_{\max}$), load capacity (ρ_{cap}), battery power (β_{pow}), CPU processing power ($\mathbb{C}$), and RAM ($\mathfrak{R}$), which ascertains the relative significance of each capability in accomplishing the delivery task. O_i denotes the i-th additional significant component taken into account in calculating the credit score, together with the related weight (ω_{o_i}) of an object. The summation of ($\omega_{o_i} \cdot O_i$) includes all supplementary aspects beyond the fundamental capabilities, providing a comprehensive evaluation of the UAV's performance potential.

Before providing the $\mathfrak{c}_s$, the UAV encrypts it using its ϱ_k. Let the encrypted score be represented by ε_s:

$$\varepsilon_{s_i} = \epsilon_{\varrho_k}(\mathfrak{c}_{s_i}),\ \forall i \in (\check{n} - 1) \tag{4}$$

In this context, $\epsilon_{\varrho_k}(\cdot)$ denotes the UAV's encryption operation, wherein its (ρ_k) encrypts the ($\mathfrak{c}_s$), guaranteeing its anonymity and rendering it challenging to decrypt without the corresponding (ϱ_k). The total number of UAVs is denoted by $\check{(n)}$. The parameters ε_s are shared among the UAVs, and once a UAV receives an ε_s, it uses a (ϱ_k) to decrypt it and get the other UAV's original $\mathfrak{c}_s$. Let ϑ_{s_i} be the decrypted data,

$$\vartheta_{s_i} = \theta_{\varrho_k{}^{-1}}(\mathfrak{c}_{s_i})\ \forall i \in (\check{n} - 1) \tag{5}$$

In this context, $\theta_{\varrho_k{}^{-1}}(\cdot)$ denotes the decryption function using the corresponding (ϱ_k^{-1}) to decrypt the received encrypted score (ε_s). The UAV subsequently verifies the sender's authenticity using a α-hash bloom filter. Let f° represent the filtered data. The calculation can then be derived as

$$f_i^\circ = \bigwedge_{\forall i \in \alpha} \alpha - hash(\varrho_{k_i}^{\upsilon})\ \forall i \in (\check{n} - 1) \cap f^\circ \in (0,1) \tag{6}$$

In this context, the UAV is denoted by the (υ) symbol. After successfully validating, υ verifies the sender's validity by evaluating the signature using the sender's ϱ_k. By implementing a uniform procedure, the verified result, represented as ν_{s_i}, can be expressed as follows:

$$\nu_{s_i} = \wp_{\varrho'_{k_i}}(\mathfrak{c}_{s_i}, \theta_{\varrho_k{}^{-1}}(\mathfrak{c}_{s_i})),\ \forall i \in (\check{n} - 1) \cap \nu_{s_i} \in \{true, false\} \tag{7}$$

In this context, $\wp(\cdot)$ represents the signature verification function, while ι denotes the list of devices stored in the blockchain when each υ is registered. After gathering all the scores, the most superior (υ)'s were identified. Given that $\mathfrak{c}_{s_{\max}}$ represents the maximum attainable score, the following equation can be obtained:

$$\mathfrak{c}_{s_{max}} = \max_{\forall i \in \overline{\upsilon}}(s_i) \tag{8}$$

Upon determining that the $\mathfrak{c}_{s_{\max}}$ of a υ reaches the threshold of maximum score within the collective network, the υ is designated as the premium UAV $\upsilon_{\text{premium}}$; conversely, UAVs with a lower score are elected as the role of normal UAV υ_{normal}. This selection process for UAVs incorporates blockchain technology and cryptographic approaches to guarantee

that only authorized and capable UAVs participate in delivery operations. This technology enhances security, reliability, and operational efficiency by implementing digital signatures for score verification and recording registered devices on the blockchain.

Algorithm 1: UAV role selection in BUS-Health.

$\mathfrak{c}_s \leftarrow 0$
while $i \in m$ **do**
  $\mathfrak{s} \leftarrow \mathfrak{s} + (\mathfrak{r}_i \times \omega_i)$
end while
$\mathfrak{s}_e \leftarrow \emptyset$
while $i \in (n-1)$ **do**
  $\varepsilon_s \leftarrow \mathfrak{s}_e \cup \xi \varrho_k(\mathfrak{s}_i)$
end while
ϑ transmits $\mathfrak{s}_e$
wait()
$\mathfrak{s}_e \leftarrow \emptyset$
while $i \in (n-1)$ **do**
  $\vartheta_{s_i} \leftarrow \mathfrak{s}_d \cup \zeta(s_{ei})$
end while
$s \leftarrow \emptyset$
while $i \in (n-1)$ **do**
  $f_i^\circ \leftarrow \bigwedge_{j \in \alpha} ß\mathfrak{f}_j(\sigma_i)$
  if $f_i^\circ == 1$ **then**
    $\mathfrak{c}_s \leftarrow \mathfrak{s} \cup \mathfrak{s}_i$
  end if
end while
$\mathfrak{c}_{s_{max}} \leftarrow \max(\mathfrak{s})$
$\upsilon \leftarrow (\mathfrak{s} == \mathfrak{s}_{\max})$?premium : normal

2.3.3. Two-phase verification

The BUS framework integrates a robust two-phase verification mechanism to ensure resistance against intrusion. Initially, a sender must pass through the $\alpha - hash$ bloom filter, a probabilistic data structure designed to efficiently verify membership within (υ) and Δ without maintaining exhaustive records. The filter is a preliminary gatekeeper, mitigating the computational overhead by pre-filtering invalid entities while preserving scalability. Subsequently, valid senders undergo the signature verification process to establish their authenticity. For entities such as (υ) that do not possess a comprehensive list of ($\mathfrak{d}$), the system bypasses the bloom filter and straight executes signature verification. This layered approach ensures that only authorized entities can access the network. Attackers seeking to compromise (υ)'s or ι devices must present a legitimate network identity to bypass these verifications, rendering unauthorized access practically unfeasible. Integrating the α-hash bloom filter with signature verification enhances the security and efficiency of the system, aligning with the objectives of establishing a dependable and scalable network defensive mechanism.

An α-hash bloom filter (where $\alpha = 1, 2, 3, \ldots$) is required to verify $\mathfrak{E}$ validity based on the pre-generated data table based on the device list ($\mathfrak{d}$). Let τ be the pre-generated data table:

$$\tau = \bigcup_{\forall i \in \mathfrak{d}} \bigcup_{\forall i \in \alpha} ß_\alpha(\mathfrak{d}_i^{\mathfrak{t}}) \tag{9}$$

In this context, α represents the total number of filters employed in α-hash bloom filter, $\mathfrak{t}$ indicates the device type (i.e., 0 for IoT devices, 1 for UAVs, 2 for Δs), and ß denotes the function of a bloom filter.

To mitigate false positives $\not{p}$, the size of the data table and the number of filters are adjusted. Let η be the total number of $\mathfrak{d}$:

$$\eta = -\frac{\mathfrak{b} \times ln(\not{p})}{(ln(2))^2} \tag{10}$$

Here, $\mathfrak{b}$ represents the number of bits in the α-hash bloom filter.

Following the process, the υ generates the operational data Θ,

$$\Theta = \left\langle \Theta_{id}, \Theta_{\widehat{mac}_\partial, \mathfrak{d}^{\mathfrak{t}}, \mathfrak{l}_r} \right\rangle \tag{11}$$

The radius of the specified place is denoted by r, and the position of the υ is denoted by $\mathfrak{l}_r$, which includes the $\left\langle \overrightarrow{lon}, \overrightarrow{lat} \right\rangle$ coordinates.

Finally, the verification of an entity $\mathfrak{E}_{x'}$ involves passing through the α-hash bloom filter. Let the $ß_\alpha$ function be a α-hash bloom filter that inputs an entity's identifier (or message) $\mathfrak{E}_{x'}$ to determine whether x' is likely to be a member of a set $\hat{\mathbf{S}}$ of permitted entities:

$$ß_\alpha = \bigwedge_{i=1}^{\alpha} \wp\left\{\mathfrak{E}_{x'}(\alpha)\right\} \ \forall i \in \alpha \cap x' \in \{0,1\} \tag{12}$$

In this context, the function $x' \in \{0,1\}$ determines whether the entity belongs to the approved set where 1 or (true) means x' belongs to the $\hat{\mathbf{S}}$, and 0 or (false) means the vice-versa.

After the α-hash bloom filter, the $\mathfrak{E}$ undergoes a digital signature verification process. The secondary verification phase involves cross-referencing an entity's digital signature with a predefined list of authorized devices on the blockchain to confirm its authenticity. This procedure guarantees that only authorized companies with blockchain-validated identification may engage in the network's operations, hence maintaining the security and trustworthiness of the UAV network, especially in healthcare logistics.

The entity $\mathfrak{E}$ first undergoes verification using the α-hash bloom filter to preliminarily check if it belongs to the set of authorized entities. Each entity $\mathfrak{E}_x$ generates a digital signature $\mathfrak{D}_\infty$ using its private key ρ_k:

$$\mathfrak{D}_\infty = \text{Sign}_{\rho_k}(\mathfrak{E}_x) \tag{13}$$

The entity transmits the data along with its digital signature $\mathfrak{D}_\infty$. Upon receiving the data, the system performs a secondary verification by cross-referencing the digital signature $\mathfrak{D}_\infty$ with a predefined list of authorized entities stored on the blockchain. The function $\wp(\cdot)$ verifies the digital signature using the corresponding public key ϱ_k:

$$\wp(\mathfrak{D}_\infty, \mathfrak{E}_x, \varrho_k) = \text{Verify}_{\varrho_k}(\mathfrak{D}_\infty) \tag{14}$$

This function checks if $\mathfrak{D}_\infty$ is a legitimate signature for $\mathfrak{E}_x$ using ϱ_k. If the verification is successful, the entity $\mathfrak{E}_x$ is confirmed as authorized, and the data is accepted. If not, the data is discarded. For the signature verification $\wp(\cdot)$ phase, the entity's $\mathfrak{D}_\infty$, and (ϱ_k) represents the corresponding to the (ρ_k) used for signing. The function validates if $\mathfrak{D}_\infty$ is a legitimate signature for x' using (ϱ_k).

$$\wp(x_i') = \bigwedge_{i=1}^{x'} \theta_{\varrho_k^{-1}}\left(\mathfrak{D}_\infty, x'\right) \ \forall i \in \wp \cap x' \in \{0,1\} \tag{15}$$

The formalization highlights the significance of validating digital signatures, ensuring that a signature $\mathfrak{D}_\infty$ is the authentic result of signing x' using the (ρ_k) linked to (ϱ_k). A successful verification affirms the message's integrity and the sender's validity, guaranteeing safe communications and transactions, particularly inside the BUS-Health network.

2.4. 5G-TI-enabled UAV delivery

This section provides a comprehensive overview of the 5G-TI UAV communication. 5G-TI integration significantly improves the connectivity for UAVs, enabling real-time, ultra-reliable, low-latency (URLLC) data transfer essential for the delivery of emergency medical supplies. 5G-TI allows UAVs to obtain precise destination coordinates in degrees, minutes, and seconds (DMS) format, enhancing the navigation accuracy. For example, when a UAV (υ) is designated for delivery, it is provided with the precise destination coordinates in the DMS format, such as 63°34'14.3"N, 3°10'16.6"E. Real-time monitoring enabled by 5G-TI allows continuous updates on (υ) location and estimated delivery time, ensuring any deviations are promptly addressed. The (υ) status changes dynamically throughout the delivery process. Initially, the status is updated from $idle$ to $in-transit$ once the flight begins. Upon reaching the destination, the status is successfully delivered if the difference between

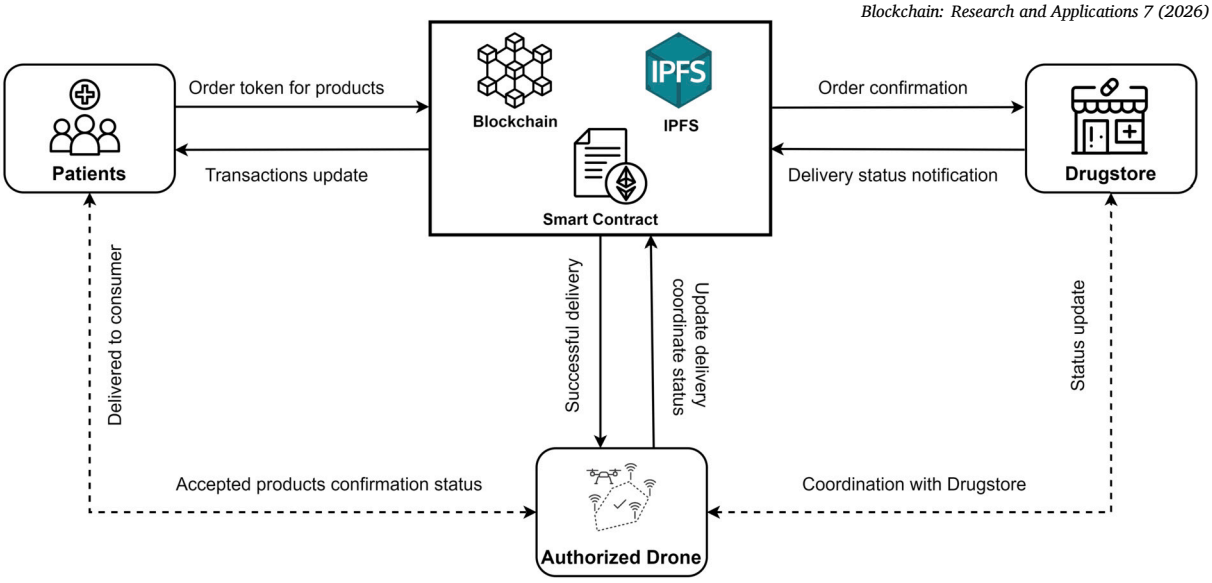

Fig. 2. Smart Contract-Enabled Transactional Process.

the estimated delivery time and the current time is zero, and after completing the delivery, the (υ) returns to $\mathfrak{d}_s$, where its status is updated back to idle.

Throughout the operation, 5G-TI enables (υ) to attain flying speeds roughly 100 times quicker than 4G-satellite channels. This is due to the increased channel capacity provided by 5G-TI. The round-trip time (RTT) latency is reduced to only 0.001 seconds [33]. The URLLC data transmission allows (υ)s to consistently send route information to the $\mathfrak{d}_s$ without delay. Upon reaching their destination, the (υ)s ensure the safe delivery of medical supplies. The 5G-TI infrastructure allows for rapid (υ) selection, completing this process within less than 20 ms [26]. The $\mathfrak{d}_s$ supervises (υ) flight operations throughout transit using the 5G-TI channel's high bandwidth and low latency to ensure accurate control and coordination. This sophisticated communication system guarantees the prompt and dependable transportation of critical medical supplies, improving the efficiency and efficacy of healthcare logistics.

2.5. Transactional process

Algorithm 2: Order and delivery of Medicare.

Input: OrderDetails, CustomerAddress, SupplierInfo, DroneInfo
procedure ORDER AND DELIVERY(OrderDetails, CustomerAddress, SupplierInfo, DroneInfo)
  OrderID ← SmartContract.CREATEORDER(OrderDetails)
  ASSEMBLEORDER(OrderID, SupplierInfo)
  if AUTHORIZEDDRONE(DroneInfo) **then**
    DELIVERORDER(OrderID, CustomerAddress, DroneInfo)
    SmartContract.UPDATESTATUS(OrderID, Delivered)
    PaymentStatus ← SmartContract.PROCESSPAYMENT(OrderID)
    DeliveryStatus ← Success
  else
    DeliveryStatus ← Drone Authorization Failed
    PaymentStatus ← Payment Not Processed
  end if
  return (DeliveryStatus, PaymentStatus)
end procedure

The proposed scheme comprises three primary entities: consumers (patients), suppliers (healthcare organizations), and UAVs, collaborating byusing blockchain technology to enable secure transactions, as depicted in Fig. 2. Initially, the consumer orders necessary product supplies stored on the blockchain using a smart contract to guarantee transparency and immutability. Suppliers acknowledge the order and are notified to assemble the required medical supplies and store them in a specified drugstore. Authorized drones collect products from the specified drugstore and transport them to the consumer's location, using appropriate technology to ensure safe delivery. After successful delivery, the status will be updated using a smart contract, and the payment will be executed to reward all parties involved. In the proposed blockchain-based UAV-integrated medical supply system, smart contracts and IPFS are essential components that ensure efficient, secure, and transparent operations. Smart contracts are utilized to facilitate and automate transactions, maintaining trustworthiness, data integrity, and security without alterations. These contracts handle tasks such as registering and verifying entities (like UAVs, drugstores, and users), managing the delivery process, and processing payments, ensuring that all interactions are securely recorded on the blockchain. Each UAV generates a cryptographic key for secure data transmission and verifies its identity using a two-phase verification process involving α-hash bloom filters and digital signatures, ensuring that only authorized UAVs participate in delivery operations. Meanwhile, the IPFS protocol addresses storage cost issues by storing large amounts of data off-chain, thereby overcoming the limitations of blockchain storage. The IPFS protocol is integrated into the system to securely store delivery information, such as coordinates and cryptographic keys, ensuring data integrity and accessibility while reducing on-chain storage requirements. This combined use of smart contracts and IPFS enhances the system's overall efficiency, scalability, and security, providing a robust solution for the timely and reliable delivery of medical supplies.

It is worth mentioning that the proposed scheme provides distinctive and non-financial incentives to different actors. For instance, the healthcare organization could employ a scoring system to incentivize successful product delivery by the UAV. This system facilitates communication and transactions among the customer, supplier, and drone to ensure the efficient and safe delivery of medicinal products. The explanation of the execution process is illustrated in Algorithm 2, with the most straightforward structural description.

3. Performance evaluation

The evaluation involves a two-step process. Firstly, the efficiency of the α-hash bloom filter is assessed using Python in a standard computing environment, comparing it against linear search, binary search [34], and chameleon hashing based on different metrics such as time complexity, space complexity, and verification speed. Then, the implementation and

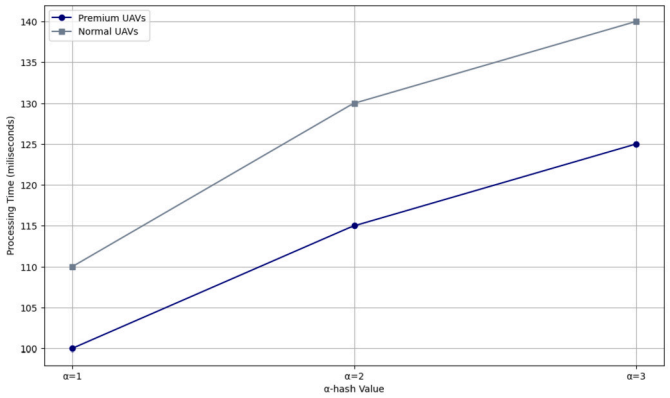

Fig. 3. Required time for verification process using α-hash Bloom Filter in role selection for different types of UAVs.

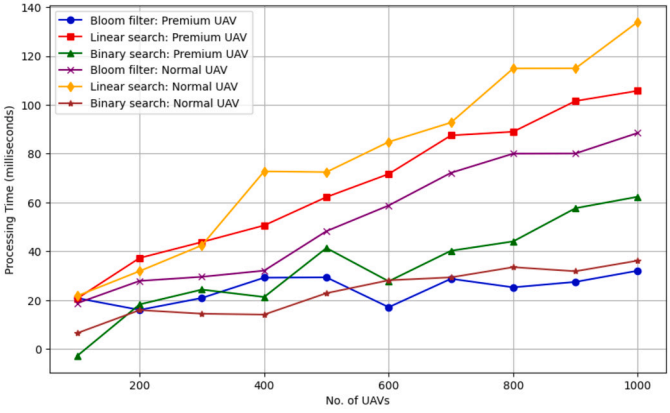

Fig. 4. Processing time required for UAV data verification in various filtering methods.

functionality of smart contracts are evaluated, simulating various scenarios to test robustness, reliability, and efficiency, ensuring secure and efficient transactions within the blockchain network. This detailed approach comprehensively assesses both the verification mechanism and smart contract implementation.

The α-hash bloom filter is a significant method for verifying the genuineness of UAVs, guaranteeing network security, and ensuring that only authorized UAVs are considered in role selection [35]. The processing time graph indicates that increased complexity in the Bloom Filter results in longer processing durations, possibly owing to the additional computational load imposed by a greater number of hash functions. Nevertheless, the minimal incremental time required implies that the system maintains efficiency despite the growing complexity. Premium UAVs have faster processing speeds across all α values, indicating superior computational capability compared to normal UAVs, as illustrated in Fig. 3. This distinction is crucial because it emphasizes the system's ability to adapt to different degrees of technical complexity within the UAV swarm. The bloom filter's efficiency and resilience are apparent in its effective management of computational needs for role selection, as seen by the graph's gradual incline, particularly for Premium UAVs.

Fig. 4 illustrates a positive correlation between the number of UAVs and the processing time for bloom filter, sequential search, and binary search algorithms. The graph demonstrates how processing time for bloom filters, sequential searches, and binary searches increase with the number of UAVs. However, the proposed approach surpasses other authentication schemes, such as linear search and binary search. Bloom filters are vital in medical data processing, mainly when dealing with extensive datasets such as patient records or prescription information. Their ability to perform hash functions and bit lookup more quickly makes them perfect for membership testing. Bloom filters prioritize existence checks, verifying the presence of specific data or drug interactions rather than their precise location. In addition, they provide space efficiency by utilizing a compressed bit array, resulting in space savings compared to linear or binary search methods. Binary and linear search algorithms are well-suited for accurately identifying elements and their positions in sorted data structures or small datasets. However, when dealing with extensive datasets, they may require a significant amount of memory due to the necessity of storing genuine data items. This leads to a poor result compared to the proposed α-hash bloom filter used in this work.

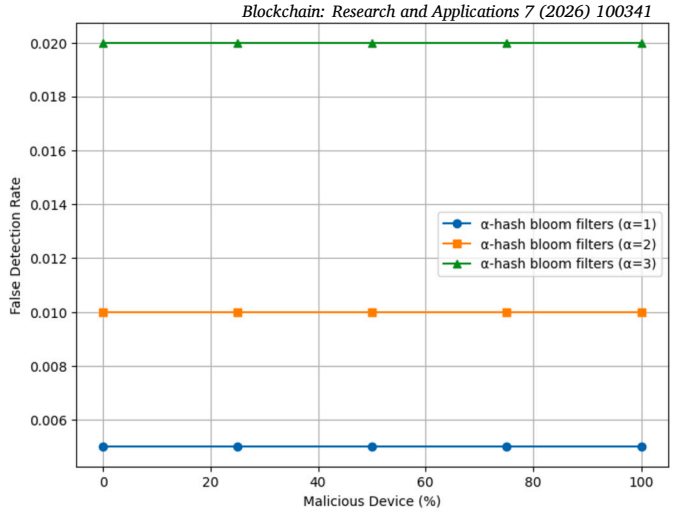

Fig. 5. The false detection rate in a α-hash bloom filter while validating various percentages of malicious devices.

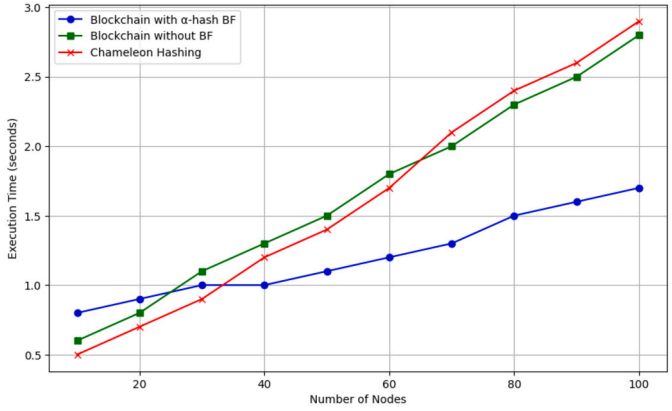

Fig. 6. Comparison of execution time between α-hash bloom filter with existing traditional methods for data verification.

The issue of false positives associated with the bloom filter is a significant concern. A simulation involving 100 devices showed in Fig. 5 that the false detection rate of α-hash bloom filters remains consistently stable, regardless of the varying percentages of malicious devices. The graph displayed three varied α numbers inside the filters. Although there are inconsistencies, the rate of false-positive results remains stable, demonstrating that variations in the increasing devices do not affect the α value or substantially impact the performance. The α-hash bloom filters have the highest false-positive rate of approximately 0.02 for $\alpha = 3$ values. The results demonstrate that BUS-Health successfully verifies devices and safeguards against malicious ones. Furthermore, increasing the value of α does not impact the false-positive rate in the α-hash bloom filters, as the contrast of the false rate is not massive.

Fig. 6 compares the execution time required in BUS-Health with the other existing methods (traditional blockchain and chameleon hashing [36]). Regardless of the scenario, the execution duration consistently

Table 2
Comparison of different filtering techniques for data verification.

Metric	Chameleon hashing	Linear search	Binary search	α-hash Bloom filter
Time complexity	Moderate	High	Very high	Low (depending on filter size)
Space complexity	Moderate	High	High	Low (depending on filter size)
Verification speed	Very fast	Slow	Fast	Very fast
Collision resistance	Moderate	High (depends on hash function)	High (depends on data structure)	High (depends on hash functions used)
False-positive rate	Low	None	None	Low (configurable)
Ease of implementation	Moderate	Easy	Moderate	Moderate
Scalability	High	Low	Moderate	Very high
Data integrity	High (due to hashing)	Moderate (depends on hash function)	Moderate (depends on data structure)	High (due to probabilistic guarantees)
Authentication	Built-in with hashing	Not inherently built-in	Not inherently built-in	Built-in with hashing

Table 3
Comparison of different existing schemes with the proposed work.

Schemes	[19]	[22]	[23]	[24]	[25]	[26]	Proposed work
Mutual authentication	✓	×	×	✓	×	×	✓
Storage efficiency	×	✓	✓	✓	×	✓	✓
Decentralised authority	✓	✓	✓	✓	×	✓	✓
Traceability	×	✓	✓	×	×	✓	✓

rises with an increased number of nodes. Traditional blockchains require nodes to authenticate every transaction, which can be laborious and time-consuming. BUS-Health is a blockchain that employs a bloom filter to alleviate the load on nodes during cryptographic verification, diminishing the overall verification duration. This procedure avoids unnecessary transactions, hence decreasing the overall execution time. Initially, BUS-Health may have a longer processing time than typical blockchains since it has to handle the extra workload of managing the bloom filter. However, as the number of nodes increases, the advantages of the bloom filter become more apparent, alleviating the burden on each node and steadily enhancing the execution time. BUS-Health accelerates transactions and checks data while maintaining an acceptable rate of false positives. Chameleon hashing is unsuitable for BUS-Health because it is vulnerable to pre-image attacks and has a lower processing performance.

In the BUS-Health system, the α-hash bloom filter outperforms chameleon hashing [36], linear search, and binary search [34] due to its superior technical attributes illustrated in Table 2. It offers constant time complexity for verification, leading to fast processing speeds essential for real-time healthcare logistics. The low space complexity, dependent on filter size, ensures efficient storage. Furthermore, the high collision resistance and a configurable low false-positive rate ensure accurate and reliable data verification, and high scalability allows it to handle increasing data volumes and network nodes efficiently. Additionally, the α-hash bloom filter supports inherent authentication through hashing, enhancing data privacy, and integrity, which is crucial for maintaining the trustworthiness of medical data. These features make the α-hash bloom filter the optimal choice for BUS-Health, ensuring efficient, secure, and scalable data verification.

The comparison of the proposed scheme with existing authentication schemes is presented in Table 3, focusing on key parameters such as mutual authentication, storage efficiency, decentralized authority, and traceability. The analysis demonstrates that the proposed work excels in all these parameters. Unlike existing schemes, the proposed scheme uniquely integrates mutual authentication, efficient storage, decentralized authority, and traceability. This highlights the proposed scheme's advanced capabilities and comprehensive approach, ensuring robust and scalable authentication without the need for a centralized trusted authority, which is a significant enhancement over the compared schemes.

3.1. Smart contract implementation and validation

The simulations were performed within the Remix IDE to examine the integrity of the smart contracts thoroughly. This involved comprehensively analyzing the deployed code and debugging processes and carefully assessing transaction logs, outputs, events, and exceptions. These validation techniques guaranteed that the functionality matched precisely with the expected requirements.

The contract employs an access control mechanism, allowing patients' and healthcare providers' distinct roles. Patients can register in the system, providing essential personal and medical information such as name, age, contact details, and medical condition history. This registration process ensures that each patient's data is securely stored on the blockchain, accessible only to authorized entities. Upon registration, patients are assigned the "PATIENT-ROLE," granting them specific privileges within the system.

Similarly, healthcare providers, represented by hospitals or clinics, can register by providing details like the hospital's name and location. Upon registration, they are assigned the "HEALTHCARE-PROVIDER-ROLE," enabling them to participate in emergency support requests and provide medical assistance.

One of the system's core functionalities is handling emergency support requests. Patients, upon encountering a medical emergency, can trigger a request for assistance. This request, denoted by the "EmergencyRequest" struct, captures critical details such as the patient's address, the nature of the condition (classified as either critical or non-critical), and an initial prescription. This information is vital for healthcare providers to assess the situation's urgency and provide appropriate care.

Upon receiving an emergency request, healthcare providers can categorize the condition based on its severity, prescribe an initial drug, and confirm the delivery of medical assistance. These actions, facilitated by functions like "categorizeCondition," "prescribeInitialDrug," and "confirmDelivery," enable healthcare providers to coordinate effectively in responding to emergencies while maintaining transparency and accountability.

Several benefits can be achieved through the implementation of this decentralized healthcare system. Firstly, patient data is securely stored on the blockchain, ensuring privacy and integrity. Secondly, the system facilitates swift communication and collaboration between patients and healthcare providers, enabling prompt responses to medical emergen-

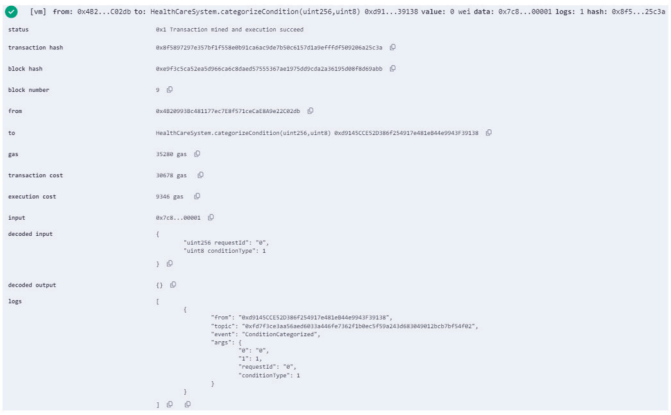

Fig. 7. Patient condition assessment by healthcare provider.

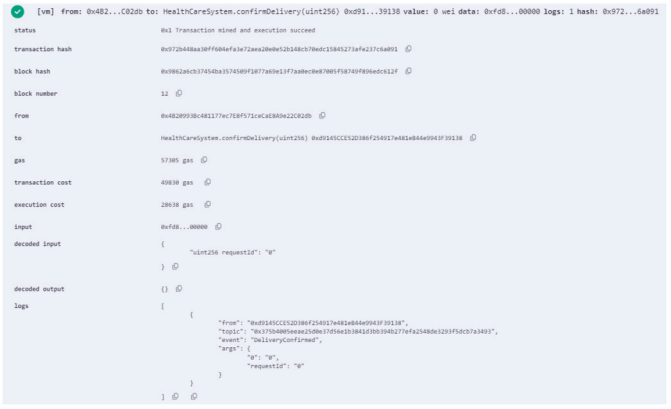

Fig. 8. Necessary drug delivery confirmation.

Fig. 9. Primary drug suggestion by healthcare provider.

cies. Thirdly, the transparent nature of blockchain technology enhances trust among stakeholders, promoting accountability and efficiency in delivering healthcare services. Figs. 7–11 depict the entire sequence of the system's procedure.

3.2. Discussion

The proposed system ensures compliance with aviation and healthcare regulations by incorporating mechanisms for UAV registration and certification, while data privacy is safeguarded through encryption and the blockchain's immutable ledger, aligning with existing standards. Although the initial startup costs for infrastructure, including UAVs, blockchain setup, and 5G-enabled TI, are considerable, these are offset by long-term operational efficiencies and cost savings achieved through

Fig. 10. Emergency medicine request by patient.

Fig. 11. Registration of patient and healthcare provider and their role finalization.

reduced reliance on human labor and minimized risks of infection during pandemics. Additionally, the proposed system considers that user-friendly web and mobile applications enable healthcare providers to manage requests and deliveries efficiently, with minimal disruption to current workflows. Training programs for staff and continuous support further ensure smooth adoption and operation. The system is designed to scale effectively, employing load balancing and dynamic resource allocation to prevent performance bottlenecks. Furthermore, integrating AI algorithms for multi-UAV coordination and optimized path planning ensure that the network remains efficient and responsive, even as the scale of operations expands. Moreover, to address privacy and security concerns, advanced cryptographic encryption techniques could be used to provide more robust security for protecting every entity's privacy.

4. Conclusions and future work

This paper explores using blockchain technology and UAVs to enhance smart healthcare logistics supply chains. The objective is to tackle concerns about the system's reliability, transactional credibility, data accuracy, and security in delivering medical supplies. The proposed solution involves using blockchain technology, smart contracts, and a scoring system for UAVs via smart contracts to improve transparency and accountability. It includes 5G-enabled TI to enhance communication efficiency. The study illustrates that combining blockchain with UAV-based medical supply delivery offers a reliable, secure, and efficient solution for medical logistics difficulties. The two-phase verification method proposed in this approach guarantees system integrity, which is essential in a medical setting. The impact of the bloom filter verification procedure is investigated by simulating an α-hash bloom

filter in Google Colab. The comparative analysis highlights the model's merits compared to conventional healthcare logistics approaches, especially regarding transactional security, data integrity, and communication credibility. In the future, advanced AI algorithms could be employed for effective multi-UAV path planning in conjunction with an encryption system to guarantee the maximum data privacy of the patient. Smart healthcare should prioritize the patient's needs over the healthcare organization. Implementing this will enhance the efficiency of the medical supply chain, accelerate emergency delivery, optimize transportation routes, and bolster the privacy and security of user data.

CRediT authorship contribution statement

Mohtasin Golam: Writing – original draft, Conceptualization, Writing – review & editing, Validation, Methodology. **Md Facklasur Rahaman:** Conceptualization, Validation, Methodology, Writing – review & editing. **Md Raihan Subhan:** Writing – review & editing, Formal analysis, Resources, Conceptualization. **Dong-Seong Kim:** Writing – review & editing, Validation, Supervision. **Jae-Min Lee:** Supervision, Writing – review & editing, Validation.

Funding

This research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF), funded by the Ministry of Education (2018R1A6A1A03024003) 20%. It was also supported by the Innovative Human Resource Development for Local Intellectualization Program through the Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (IITP-2025-RS-2020-II201612) 20%, and by the IITP-ICAN (ICT Challenge and Advanced Network of HRD) grant funded by the Korea government (MSIT) (IITP-2025-RS-2022-00156394) 20%. Additional support was provided by the MSIT, Korea, under the ITRC (Information Technology Research Center) support program (IITP-2025-RS-2024-00438430) supervised by IITP 20%, as well as the Gyeongsangbuk-do RISE (Regional Innovation System & Education) project (Idea Start-up Valley unit) 20%.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] G. Rong, A. Mendez, E.B. Assi, et al., Artificial intelligence in healthcare: review and prediction case studies, Engineering 6 (3) (2020) 291–301, https://doi.org/10.1016/j.eng.2019.08.015.

[2] A. Dorofeev, V. Kurganov, N. Fillipova, et al., Ensuring the integrity of transportation and logistics during the covid-19 pandemic, Transp. Res. Procedia 50 (2020) 96–105, https://doi.org/10.1016/j.trpro.2020.10.012.

[3] M. Karatas, L. Erişkin, E. Bozkaya, Transportation and location planning during epidemics/pandemics: emerging problems and solution approaches, IEEE Trans. Intell. Transp. Syst. 23 (12) (2022) 25139–25156, https://doi.org/10.1109/tits.2022.3166724.

[4] J.O. Onyango, Supply chain solutions for essential medicine availability during covid-19 pandemic, J. Humanit. Logist. Supply Chain Manag. 14 (1) (2024) 118–133, https://doi.org/10.1108/jhlscm-05-2022-0056.

[5] Z. Xu, A. Elomri, L. Kerbache, et al., Impacts of covid-19 on global supply chains: facts and perspectives, IEEE Eng. Manag. Rev. 48 (3) (2020) 153–166, https://doi.org/10.1109/emr.2020.3018420.

[6] T.-M. Choi, Risk Analysis in Logistics Systems: A Research Agenda During and After the Covid-19 Pandemic, Transp. Res. Part E Logist. Transp. Rev. 145 (2021) 102190, https://doi.org/10.1016/j.tre.2020.102190.

[7] G. Zhang, N.J. Navimipour, A comprehensive and systematic review of the iot-based medical management systems: applications, techniques, trends and open issues, Sustain. Cities Soc. 82 (2022) 103914, https://doi.org/10.1016/j.scs.2022.103914.

[8] D.C. Nguyen, M. Ding, P.N. Pathirana, et al., Blockchain and ai-based solutions to combat coronavirus (covid-19)-like epidemics: a survey, IEEE Access 9 (2021) 95730–95753, https://doi.org/10.1109/access.2021.3093633.

[9] Y. Shen, D. Guo, F. Long, et al., Robots under covid-19 pandemic: a comprehensive survey, IEEE Access 9 (2020) 1590–1615, https://doi.org/10.1109/access.2020.3045792.

[10] D. Hawashin, M. Nemer, S.A. Gebreab, et al., Blockchain applications in uav industry: review, opportunities, and challenges, J. Netw. Comput. Appl. 230 (2024) 103932, https://doi.org/10.1016/j.jnca.2024.103932.

[11] Z. Lv, D. Chen, H. Feng, et al., Digital twins in unmanned aerial vehicles for rapid medical resource delivery in epidemics, IEEE Trans. Intell. Transp. Syst. 23 (12) (2021) 25106–25114, https://doi.org/10.1109/tits.2021.3113787.

[12] J. Euchi, Do drones have a realistic place in a pandemic fight for delivering medical supplies in healthcare systems problems?, Chin. J. Aeronaut. 34 (2) (2021) 182–190, https://doi.org/10.1016/j.cja.2020.06.006.

[13] R.M. Triche, A.E. Greve, S.J. Dubin, Uavs and their role in the health supply chain: a case study from Malawi, in: Proceedings of the 2020 International Conference on Unmanned Aircraft Systems (ICUAS), IEEE, 2020, pp. 1241–1248, https://doi.org/10.1109/icuas48674.2020.9214064.

[14] Y. Mekdad, A. Aris, L. Babun, et al., A survey on security and privacy issues of uavs, Comput. Netw. 224 (2023) 109626, https://doi.org/10.1016/j.comnet.2023.109626.

[15] N. Koshta, Y. Devi, C. Chauhan, Evaluating barriers to the adoption of delivery drones in rural healthcare supply chains: preparing the healthcare system for the future, IEEE Trans. Eng. Manag. 71 (2022) 13096–13108, https://doi.org/10.1109/TEM.2022.3210121.

[16] J.-P. Yaacoub, H. Noura, O. Salman, et al., Security analysis of drones systems: attacks, limitations, and recommendations, Internet Things 11 (2020) 100218, https://doi.org/10.1016/j.iot.2020.100218.

[17] R. Akter, M. Golam, V.-S. Doan, et al., Iomt-net: blockchain-integrated unauthorized uav localization using lightweight convolution neural network for Internet of military things, IEEE Internet Things J. 10 (8) (2022) 6634–6651, https://doi.org/10.1109/jiot.2022.3176310.

[18] M. Facklasur Rahaman, M. Golam, M. Raihan Subhan, et al., Meta-governance: blockchain-driven metaverse platform for mitigating misbehavior using smart contract and ai, IEEE Trans. Netw. Serv. Manag. 21 (4) (2024) 4024–4038, https://doi.org/10.1109/TNSM.2024.3419151.

[19] M.A. Cheema, R.I. Ansari, N. Ashraf, et al., Blockchain-based secure delivery of medical supplies using drones, Comput. Netw. 204 (2022) 108706, https://doi.org/10.1109/tnsm.2024.3419151.

[20] S. Aggarwal, N. Kumar, M. Alhussein, et al., Blockchain-based uav path planning for healthcare 4.0: current challenges and the way ahead, IEEE Netw. 35 (1) (2021) 20–29, https://doi.org/10.1016/j.comnet.2021.108706.

[21] E. Sarvesh, J. Jose, S. Chitrakala, Meduav: drone-based emergency medical supply system using decentralized autonomous organization (dao), Proc. Comput. Sci. 230 (2023) 737–748, https://doi.org/10.1109/mnet.011.2000069.

[22] R. Gupta, P. Bhattacharya, S. Tanwar, et al., Garuda: a blockchain-based delivery scheme using drones for healthcare 5.0 applications, IEEE Internet Things Mag. 4 (4) (2021) 60–66, https://doi.org/10.1109/iotm.001.2100045.

[23] S.H. Alsamhi, B. Lee, M. Guizani, et al., Blockchain for decentralized multi-drone to combat covid-19 and future pandemics: framework and proposed solutions, Trans. Emerg. Telecommun. Technol. 32 (9) (2021) e4255, https://doi.org/10.1002/ett.4255.

[24] A.N. Navaz, M.A. Serhani, H.T. El Kassabi, et al., Trends, technologies, and key challenges in smart and connected healthcare, IEEE Access 9 (2021) 74044–74067, https://doi.org/10.1109/access.2021.3079217.

[25] S. Cui, Y. Yang, K. Gao, et al., Integration of uavs with public transit for delivery: quantifying system benefits and policy implications, Transp. Res., Part A, Policy Pract. 183 (2024) 104048, https://doi.org/10.1016/j.tra.2024.104048.

[26] A. Verma, P. Bhattacharya, M. Zuhair, et al., Vacochain: blockchain-based 5g-assisted uav vaccine distribution scheme for future pandemics, IEEE J. Biomed. Health Inform. 26 (5) (2021) 1997–2007, https://doi.org/10.1109/jbhi.2021.3103404.

[27] A. Ala, A. Goli, S. Mirjalili, et al., A fuzzy multi-objective optimization model for sustainable healthcare supply chain network design, Appl. Soft Comput. 150 (2024) 111012, https://doi.org/10.1016/j.asoc.2023.111012.

[28] W. Wang, P. Gope, Y. Cheng, An ai-driven secure and intelligent robotic delivery system, IEEE Trans. Eng. Manag. 71 (2022) 12658–12673, https://doi.org/10.1109/TEM.2022.3142282.

[29] S. Gupta, S. Modgil, R. Meissonier, et al., Artificial intelligence and information system resilience to cope with supply chain disruption, IEEE Trans. Eng. Manag. 71 (2021) 10496–10506, https://doi.org/10.1109/TEM.2021.3116770.

[30] C.W. Lau, J. Liu, X. Ma, Blockchain-based messaging and information sharing systems for air cargo supply chains, IEEE Trans. Eng. Manag. 71 (2023) 9019–9034, https://doi.org/10.1109/TEM.2023.3314733.

[31] J. Jayabalan, N. Jeyanthi, Scalable blockchain model using off-chain ipfs storage for healthcare data security and privacy, J. Parallel Distrib. Comput. 164 (2022) 152–167, https://doi.org/10.1016/j.jpdc.2022.03.009.

[32] M. Golam, R. Akter, R. Naufal, et al., Blockchain inspired intruder uav localization using lightweight cnn for Internet of battlefield things, in: Proceedings of the MILCOM 2022-2022 IEEE Military Communications Conference (MILCOM), IEEE, 2022, pp. 342–349, https://doi.org/10.1109/milcom55135.2022.10017795.

[33] S. Tanwar, S. Tyagi, I. Budhiraja, et al., Tactile Internet for autonomous vehicles: latency and reliability analysis, IEEE Wirel. Commun. 26 (4) (2019) 66–72, https://doi.org/10.1109/mwc.2019.1800553.

[34] D. Upadhyay, N. Gaikwad, M. Zaman, et al., Investigating the avalanche effect of various cryptographically secure hash functions and hash-based applications, IEEE Access 10 (2022) 112472–112486, https://doi.org/10.1109/access.2022.3215778.

[35] M. Golam, J.-M. Lee, D.-S. Kim, A uav-assisted blockchain based secure device-to-device communication in Internet of military things, in: Proceedings of the 2020 International Conference on Information and Communication Technology Convergence (ICTC), IEEE, 2020, pp. 1896–1898, https://doi.org/10.1109/ictc49870.2020.9289282.

[36] F. Li, H. Xu, Q. Song, et al., Blma: editable blockchain-based lightweight massive iiot device authentication protocol, IEEE Internet Things J. 10 (24) (2023) 21633–21646, https://doi.org/10.1109/JIOT.2023.3308725.