VAHAK: A Blockchain-based Outdoor Delivery Scheme using UAV for Healthcare 4.0 Services

Rajesh Gupta*, Arpit Shukla†, Parimal Mehta‡, Pronaya Bhattacharya §, Sudeep Tanwar¶, Sudhanshu Tyagi‖, Neeraj Kumar**
*†‡§¶Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad, Gujarat, India
‖**Thapar Institute of Engineering & Technology (Deemed to be University), Patiala (Punjab), India
Emails:*18ftvphde31@nirmauni.ac.in, †18bce370@nirmauni.ac.in, ‡16bce118@nirmauni.ac.in,
§pronoya.bhattacharya@nirmauni.ac.in, ¶sudeep.tanwar@nirmauni.ac.in, ‖s.tyagi@thapa.edu, **neeraj.kumar@thapar.edu

***Abstract*—Unmanned aerial vehicle (UAV) is used in various smart applications, such as defense, civilian, and healthcare services. As data in these applications flow through an open channel, i.e., the Internet, so security and privacy always a challenging issue. Though many solutions exist for this problem in literature, but these solutions are not adequate to handle security, privacy, latency, and efficient real-time delivery of healthcare services remotely over the wireless communication channel. Moreover, the existing UAV systems have security, reliability, latency, and storage cost issues, which restricts their applicability shortly. Motivated from these facts, this paper proposes *VAHAK*, an Ethereum Blockchain (BC) based secure outdoor healthcare medical supplies using UAVs. *VAHAK* provides reliable communication between the UAVs and the entities in a decentralized manner, which ensures the early delivery of required medical supplies to the critical patients. In *VAHAK*, security, privacy, and reliability issues have been resolved using Ethereum smart contract (ESC), while storage cost issues are handled with IPFS protocol. The security vulnerabilities of the *VAHAK* are tested on *MyThril* open-source tool. *VAHAK* is efficient in terms of data storage cost as it uses the InterPlanetary File System (IPFS) for healthcare record storage and 5G-enabled Tactile Internet (TI) for communication, respectively. Finally, *VAHAK* performance evaluation demonstrates its effectiveness as compared to the traditional systems where it outperforms the existing schemes with respect to various performance evaluation metrics, such as scalability, latency, and network bandwidth.**

***Index Terms*—Blockchain, UAV, Healthcare, Outdoor Delivery, Smart Contracts, Security**

I. Introduction

Healthcare is the prime concern for the overall growth of any nation, as it delivers medical care services to the people around the world with a vision to achieve a healthy and wealthy life. Therefore, the healthcare industry has changed dramatically over the years as technology upgraded. With the advent of modular IT systems, the healthcare industry has revolutionized from 1.0 to 4.0 [1]. Healthcare 1.0 started in the early 1970s, where medical records were manually organized and maintained. In the mid-1990s, multiple IT systems were beginning to get interconnected, and Electronic Health Records (EHRs) called Healthcare 2.0 [2], [3]. Then, the year ranging from 2005-2015 was known for Healthcare 3.0 as EHR systems were interconnected, the Human Genome Project concluded, and medical sensors like wearables and implantables became more frequent. Nowadays, with the usage of latest technologies, real-time data collection with faster connection speeds, and AI for data analysis/insights, healthcare has become more predictive and personalized to the patient is the era of Healthcare 4.0 [4].

Though healthcare has improved a lot in many areas, such as telemedicine, telesurgery, record keeping, and disease prediction [5]. But, the delivery system/supply chain remains a challenging issues for the healthcare industry [6]. The healthcare supply chain is different from other industries as it not only does the carriage of materials but has to deliver quickly to save the life of an individual. Traditional healthcare supply chain systems delivered medicines through road transport infrastructure, which has many limitations, such as road traffic, congested roads, and long-distance to cover. Statistics given in [7] show that *20%* of emergency patients' deaths were caused by traffic jams. So, the efficient transformation in the delivery system is required, as it is the second most considerable expense for the industries [8].

One plausible solution to the above-illustrated issues is to change the mode of transportation itself. UAVs can be preferred for the healthcare supplies in a much faster way. Moreover, it can fly either autonomously with the help of digital circuitry installed in it or with a remote controller. An ambulance drone was made at TUDelft and showed a 93% faster response time in rural areas and 32% in urban areas than conventional methods [9]. Though drones have become more mainstream but the Cybersecurity of UAVs is still a nightmare. Researchers from Johns Hopkins University identified flaws in the commercial drones such as vulnerabilities to hijacking, man-in-the-middle, and injection attacks [10]. This has raised various concerns about the security and reliability of adopting drones for healthcare-related deliveries.

However, the issues mentioned above have not been taken into consideration much by the researchers. For example, in [11] and [12], the authors have given the prototype of an emergency air ambulance, which can reach to the required venue faster than a conventional ambulance. Moreover, it is integrated with all-purpose medical facilities that support the team working at a specific hospital. They have used *IEEE 802.15.4* (ZigBee) protocol [13] over the GSM communication channel to transfer data from air ambulance to the hospital. But, the authors have not given much importance to the com-

munication network properties, such as bandwidth, latency, and security. In [14], the authors have developed a quad-copter prototype, i.e., aero ambulance similar to [11] and [12], but not as a support to the conventional ambulance, instead as an independent entity. They have used it to transport blood from blood banks to hospitals and hospital to hospital with faster delivery. But, they have not looked into security issues like drone hijacking and GPS spoofing.

BC and smart contract (SC) seem to be the technological solutions to overcome the security mentioned above issues [15]. Motivated from these facts, this paper proposes an Ethereum BC-based SCs for healthcare supply using UAVs called *VAHAK* that ensures the transaction reliably and security. It is a peer-to-peer (P2P) distributed scheme in which each peer has a copy of the entire BC, which has no chance of single-point failure [16], [17]. *VAHAK* also ensures the trust between all stakeholders via the immutability and transparency of records. Ethereum SCs are self-executable, self-verifiable, self-enforceable, and self-validated the transactions between system entities [18]. In *VAHAK*, some important information, such as timestamp, location, delivery status, and package transported, is stored into the BC and make it visible to all peers [19]. Thus, it reduces the security concerns of UAV by tracking it's every moment in the chain of blocks. Further, if the drone starts going off-route, we can rely on an SC to make it return to base.

To monitor the real-time position of the drone as it flies to the recipient, *VAHAK* uses 5G-enabled Tactile Internet(TI), which is ultra-fast with $< 1ms$ latency, highly reliable as its downtime is less than 3s per year, and its bandwidth can go up to 10Gbps [20]. Moreover, it helps to deliver medicines faster in critical conditions. To store the data on the BC is quite costly because of its limited storage. So, in *VAHAK*, we have used Interplanetary File System (IPFS), a distributed data storage that increases the throughput and reduces the latency in data access and synergizes well with the BC technology [21]. IPFS uses a Merkle Directed Acyclic Graph (DAG) to ensure immutability of added MP_i of i^{th} patient, with version control for updates. It is resistant to security attacks that can be performed on MP_i, ensuring privacy.

A. Research Contribution

Following are the research contributions of this paper.

- An Ethereum SC-based secure approach is proposed to track the delivery of healthcare supplies by UAVs.
- A IPFS-based decentralized and distributed data storage approach for *VAHAK* is designed for fast and reliable data access.
- Performance evaluation of the proposed scheme by considering latency, reliability, and data storage cost.

B. Organization

The rest of the paper is organized as follows. Section II presents the system model and problem formulation. Section III describes the proposed approach. Results and discussion are presented in Section IV, and finally, the paper is concluded in Section V.

II. System Model and Problem Formulation

This section presents the problem formulation and an overview of the *VAHAK* system.

A. System Model

Fig. 1 shows the BC-based secure delivery scheme using UAV for Healthcare 4.0 called as *VAHAK*, which comprises of four entities, such as $\{E_P, E_H, E_W, E_{UAV}\} \in E$. UAVs ($E_{UAV}$) that deliver the medical supplies, hospital (E_H) that diagnoses the patient and classifies the E_P medical supply request as critical (C) or non-critical (NC), warehouse or pharmacy (E_W) from which the medicine is supplied to the UAVs for delivery, and the patient (E_P) who has called for the help. The communication transactions of E are stored in the

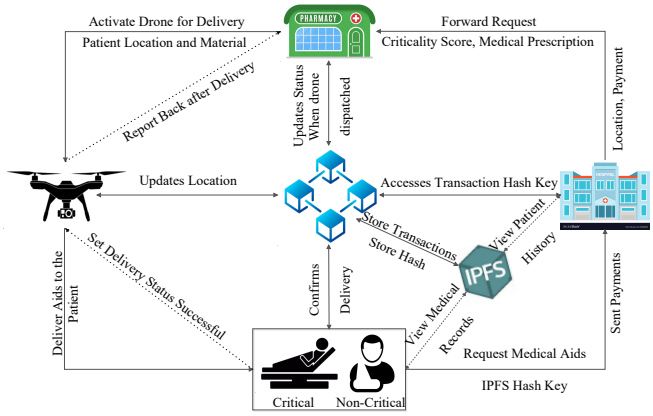


Fig. 1: *VAHAK* System Model.

chain of blocks to show the current status of each delivery to all the stakeholders. To make sure that the status displayed is the real-time status (without any delay), the drones and other entities are connected to the Internet using 5G-enabled TI, which ensures an ultra-low latency and ultra-high reliability. Moreover, storing data on BC directly is extremely costly, so instead, we are using IPFS to store data and its generated hash in the BC for later access. TI will help to reduce the round trip latency of accessing IPFS for data storage and store the hash back to the BC.

B. Problem Formulation

In *VAHAK*, there are four entities $\{E_P, E_H, E_W, E_{UAV}\} \in E$ that exchanges medical data through BC. The patient entity E_P is defined as $\{P_1, P_2, \ldots . P_n\}$ having their medical health records $H_R = \{P_{h1}, P_{h2}, \ldots, P_{hn}\}$. Similarly, the hospital entity $E_H = \{H_1, H_2, \ldots, H_k\}$ are associated with a set of m doctors $\{D_1, D_2, \ldots, D_m\}$. These entities and their associated relations are subject to the following constraints.

$$n, m, k > 0 \tag{1}$$

$$\forall P_i \;\; \exists H_k : (P_i \xrightarrow{®} H_h) \tag{2}$$

where, constraint (2) specifies that for every patient P_i there is a mapping with at least one H.

H_R are stored in distributed IPFS with hash keys

$\{H_K^1, H_K^2, \ldots, H_K^n\}$ where $K \in \{1, 2, \ldots, n\}$. Each key H_K^i is mapped with at most one E_H. Now, a patient P_i has a medical prescription (MP), stored in IPFS with the following attributes.

$$MP_i = \{H_K^i, ID(P_i), ID(D_m), ID(H_j), P_D^i, T\}$$

Any i^{th} patient can suffer from *C* diseases denoted as $\{P_{D_1}, P_{D_2}, \ldots, P_{D_c}\}$. The patient enters all associated disease record as an attribute P_D^i in MP_i, which is shared with H_j via BC.

Any P_i can view it's MP from IPFS by unlocking it with H_k^i. Then, MP_i is mapped with H_j through a mapping relation $R_{PH}, represented as follows. MP_i \rightarrow H_j$. Based on the received request, H_j classifies MP_i as critical (C) or Non-Critical (NC), denoted as M_C^i and M_{NC}^i. For critical illness of the patient, payment settlement can be deferred for a time-interval T_C^i as it is an emergency situation. For non-critical cases, immediate payment settlement is required through wallets W_{H_j} and W_{P_i}. These actions are subject to the following constraints.

$$W_{P_i} > 0, \quad if \;\; P_i \in M_{NC}^i \tag{3}$$

$$T_C^i < T_{max} \tag{4}$$

$$\forall M_P^i \in \{M_C^i, M_{NC}^i\} \tag{5}$$

The H_j sends an inventory request I_R to the entity E_W. In case of critical illness, a token $T(M_C^i)$ is generated and forwarded to E_W. For non-critical illness, the payment receipt is executed through SC, denoted as $P(M_{NC}^i)$ is stored in E_W.

However, E_W consists of l warehouses $\{W_1, W_2, \ldots, W_l\}$. I_R is forwarded to any b^{th} warehouse in W_l. Any b^{th} warehouse maintains a priority queue Q_W^i, which consists of all requests stored according to the criticality score of P_D^i. M_{NC}^i can be stored in first-come-first-serve fashion. The request is packetized with an associated header $H(M_C^i)$ and $H(M_{NC}^i)$, respectively, with the following attributes.

$$H(M_C^i) = \{SA(W_l^i), DA(P_i), CS(P_D^i)\} \tag{6}$$

$$H(M_{NC}^i) = \{W_l^i, SA(W_l^i), DA(P_i), CS(P_D^i)\} \tag{7}$$

$$CS(H(M_c^i)) > H(M_{NC}^i) \tag{8}$$

The aggregated packets $\{Q_1, Q_2, \ldots, Q_p\}$ are sent to E_P via UAV entity E_{UAV} consisting of set of h UAV's $\{UAV_1, UAV_2, \ldots, UAV_h\}$. All UAVs are considered to exhibit fairness policy, i.e., all of them offer the same set of storage and computing services. Any p^{th} aggregated packet can be assigned to any available UAV_h.

$$\forall UAV_h \;\; \exists UAV_a : assign(UAV_a, CS(P_D^i)) \tag{9}$$

where $assign(a, b)$ is a function that assigns a critical Q_b to UAV_a. Any h^{th} UAV has the following parameters.

$$UAV_h = \{Q_{type}, \zeta_p, \lambda(\zeta_p), \tau, T_\lambda, T_\vartheta\} \tag{10}$$

where $Q_{type} \in \{H(M_C^i), H(M_{NC}^i)\}$, and ζ_p denotes the carried payload by h^{th} UAV, $\lambda(\zeta_p)$ specifies the encapsulated UAV header, τ denotes the set of operational states *IDLE, BUSY, IN-TRANSIT, DELIVERED, FAILED*, T_λ is the timestamp information of processing $\lambda(\zeta_p)$, and T_ϑ denotes the timestamp information of Q_p delivered to P_i. Initially during transit $T_\vartheta = 0$.

Initially, UAV_h will be in *IDLE* state and after receiving the packet from Q_W^i, it identifies the Q_{type} and adds $\lambda(\zeta_p)$ at T_λ. Also, the state information changes to *BUSY* during the processing. Once the UAV attaches the header, it is ready for transit towards the destined $DA(P_i)$ as specified in Q_p. The state now changes to *IN-TRANSIT* over the 5G-enabled TI communication channel.Then, the Q_p is received by P_i and UAV_h changes τ to *DELIVERED*. T_ϑ is updated to current timestamp, i.e., $T_\vartheta = T_{curr}$. In case of non-conformance of delivery due to channel security and privacy issues, UAV_h updates the state to *FAILED* at timestamp T_f. A proposed formal security verification is carried out at E_W. During return of UAV_h back to E_W, it changes its state back to *IN-TRANSIT*. On successful return, header information is removed from UAV_h header and state is marked to *IDLE* for subsequent allocation of other Q_p.

III. *VAHAK*: The Proposed Approach

This section describes the working of *VAHAK*, a BC-based secure delivery scheme for healthcare supplies. *VAHAK* is secure and eliminates the need for trusted third-party systems between the communicating parties. It also reduces the shipment cost and improves the latency and throughput of the system using *IPFS protocol* for data storage. The BC-based secure delivery scheme *VAHAK* is shown in Fig. 2, which is divided into four different working layers: (i) data collection, (ii) data process, (iii) transport, and (iv) application layers. The data exchange is uniformly transacted among the different sublayers in JavaScript Object Notation (JSON) format. JSON offers more readability, map-data structure, aligned code-structure, and light-weight data exchange solution than XML. The details about these layers are explained in subsequent subsections.

A. Application Layer

It consists of a patient who needs medical aid, and a caregiver or bystander can also be a part of this layer. The patient, the caregiver, or the bystander can put their request for healthcare aids from this layer. This layer also gives the location where the required supplies get delivered by UAVs and must be in the proximity of E_W. The $P_i \in E_P$, communicates with the $H_K \in E_H$ by sharing its IPFS H_{Key}^i and also describes the situation for which the medical aid is needed as per Algorithm 1. In our system, one E_P can request only one E_H at a time, but can forward its request to any of the available H_k. In other view, multiple E_P can send their requests to one single E_H. So, the complexity of Algorithm 1 is $O(n \times k)$. A SC is created between each layer to establish trust between entities. Here, in *VAHAK*, the SC between patient and the hospital is built, which takes care of the healthcare supply request (by E_P) and also validates it. When the SC is verified and validated the E_P request, then, it stores the location of P_j, H_{Key}^i to access their medical

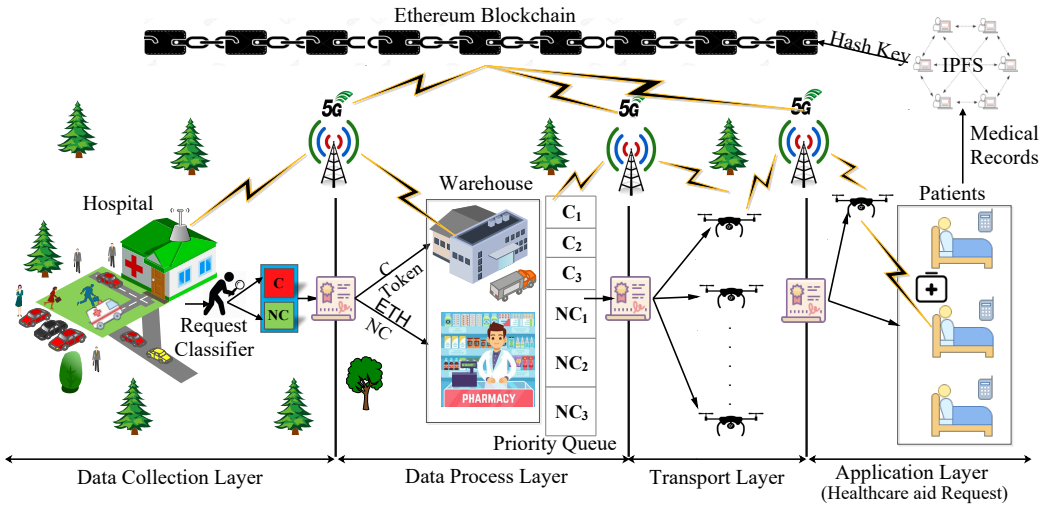


Fig. 2: *VAHAK* System Architecture.

records, and other details of the P_j in the BC as a transaction. Each party (E) to the SC can view its data in IPFS and the communication transactions at any time.

In *VAHAK*, we have used open-source technology to create and deploy SCs is Ethereum BC and Solidity language. After placing a request ($R_{Patient}$), the P_j will receive the medical supplies delivered by UAV and set the status as received in the BC.

Algorithm 1 Patient request to hospital for medicine

Input: R, MP_i, H_k, H^i_{Key}
Output: E_P request (R) is valid or not,
Request-type is {C, NC}, such that
$R \in \{R_{Patient}, R_{Hospital}, R_{Warehouse}, R_{Authority}, R_{UAV}\}$.

```
procedure PATIENT_REQUEST( R, MP_i)
    if (R ∈ R_Patient) then
        H_k ← REQUEST_HEALTH_SUPPLY(ID(P_i), H^i_Key)
        while (Items_Left > 0) do
            H_k ← ADD_PRESCRIPTION_ITEMS (MP_i)
        end while
    else
        R_Authority ← REQUEST_REGISTRATION (R, P_n)
    end if
    while (TRUE) do
        if (No_Item_Left) then
            R_Patient ← CS_Aggregated
            ETH_Tx_Fee ← CALCULATE_BILL(P^i_D)
        else
            CS(P^i_D) ← GENERATE_CS(P^i_D)
            CS_Aggregated ← CS_Aggregated + CS(P^i_D)
        end if
    end while
    H_i ← REQUEST_CLASSIFY (CS_Aggregated)
    R_Patient→Type → {C, NC}
    R_Validate ← VALIDATE_PRESCRIPTION (MP_i, H^i_Key)
    R_Patient→Valid → VALID(0:FALSE, 1:TRUE)
    if (R_Patient→Type == NC) then
        R_Hospital ← TRANSFER(R_Patient, ETH_Tx_Fee)
    end if
end procedure
```

B. Data Collection Layer

It consists of E_H and its staff where H_j receives the medical supply request from the patient at the application layer as $R_{Patient}$ as shown in Algorithm 1. H_i uses the H_{Key} of P_i to access the patient's medical records that are stored on the IPFS data storage system. Based on the P_i past records, H_i will validate the $R_{Patient}$ and classify it into C or NC based on the level of criticality (i.e., based on their $CS_{Aggregated}$). The CS is ranging from 0 to 1, where 0 is the least critical value, and the values above the 0.75 will be considered as critical. If the P_i is critical, then the H_k will pass a token as payment for the transaction to the next layer, i.e., data process layer and medical supplies to be delivered to P_i against the $R_{Patient}$ immediately without any delay. Then, the critical P_i will be given a fixed period to pay the due amount for the received healthcare supplies.

If the $R_{Patient}$ is *NC*, then, the hospital first ask for the payment from the P_i before processing the order. Once the hospital receives the payment (*in ETH*), then $R_{Patient}$ will be passed to the next layer, i.e., the data process layer with its payment receipt as shown in Algorithm 2. The SC between the hospital and the warehouse is used to ensure the consistency and reliability of the supply chain, as the next part of the process will only be initiated once the payment has been transferred to the entity E_W in the data process layer. The SC will stores the payment receipt, patient location, and healthcare supplies as a block in the Ethereum BC.

C. Data Process Layer

It consists of E_W, which stores healthcare supplies like first-aid kits, vaccines, medicines, or insulin. It also maintains a multi-level priority queue (PQ) based on the criticality score ($CS_{Aggregated}$) of the request received from the data collection layer. There are two levels in the PQ, i.e., C and NC. Moreover, the R_i from H_j at data collection layer is stored into the PQ according to $CS_{Aggregated}$. The requests at C-level are stored in order based on their $CS_{Aggregated}$ as per the Insertion sort technique, and at NC-level, the requests are being stored in the first-come-first-serve manner.

Algorithm 2 Hospital to warehouse communication

Input: $R, MP_i, H_k, DA(P_i), CS_{Aggregated}$
Output: $DeliveryInitiation\{0 : Successful, 1 : Unsuccessful\}$

```
procedure SUPPLY_DELIVERY_REQUEST( R, MP_i, E_P)
    if (R ∈ R_Hospital) then
        R_Warehouse ← REQUEST_SUPPLIES(MP_i, R_Patient)
        if (R_Patient→Type == C) then
            R_Warehouse ← GENERATE_TOKEN
                          (R_Patient, R_Hospital, MP_i)
            R_Patient ← GRANT_PERIOD(ETH_Tx_Fee, T)
        else
            R_Warehouse ← TRANSFER(R_Hospital, ETH_Tx_Fee)
        end if
    else
        R_Authority ← REQUEST_REGISTRATION (R_Hospital)
    end if
    R_Warehouse ← ADD_TO_PQUEUE (R_Patient)
    while (TRUE) do
        if (UAV_AVAILABLE() = = TRUE) then
            R_UAV ← INITIATE_DELIVERY(MP_i, UAV_h)
            BREAK()
        end if
    end while
end procedure
```

D. Transport Layer

This layer is responsible for transporting the healthcare supplies via UAVs over the 5G-enabled TI communication channel [22]. Every E_W is connected to the UAV station through which delivery can be initiated. The UAVs can be in one of the following states, i.e., {*IDLE, BUSY, IN-TRANSIT, DELIVERED, FAILED*} during the process. Initially the *IDLE* UAV is being selected for the transport purpose by the E_W at timestamp T. Then, E_W attaches the packet header, i.e., $H(M_C^i) or H(M_{NC}^i)$ along with the healthcare supply of the selected R_i according to *VAHAK* priority queue and the state will change to *BUSY*. Then, the UAV is loaded and ready to take off towards the $DA(P_i)$ and the state changes to *IN-TRANSIT*. Its current location is continuously updated in the BC for security and tracking purposes. Through this, all the entities (E) come to know where actually the drone is (in real-time) and can be immediately notified if the drone is acting suspiciously (state changes to *FAILED*). When the UAV delivers the healthcare supplies to P_i at timestamp T_i, and both UAV and patient will confirm the delivery status via SC and the state changes to *DELIVERED*. Then UAV returns to its base station and sets its state to *IDLE* for the next task.

IV. Formal Security Verification of *VAHAK*

This section focuses on the several security features of ESC, for instance, tx.origin, re-entrancy, tx order dependence, and time-stamp dependence. It is important to verify the security vulnerabilities of ESC before its final deployment in the BC as it immutable and cannot be changed afterwards. Hence, the security vulnerabilities of *VAHAK* is tested over the *MyThril* open-source tool [23]. It is used to detect various security bugs or vulnerabilities using various analysis techniques, such as taint analysis, consoles analysis, and control flow checking. Compared to other open source tools, *MyThril* offers symbolic code-executions for EVM bytecodes [24]. The proposed SC in *VAHAK* are analyzed for security vulnerabilities using *MyThril* tool. As output, it returned a message *"No issues were detected"* which is shown as a snapshot in Fig. 3.

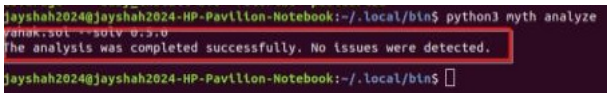


Fig. 3: Formal security verification of *VAHAK*

V. Results and Discussion

In this section, we evaluate the performance of *VAHAK* with respect to the scalability, bandwidth, latency, and data storage cost. The detailed explanation is as follows.

A. Bandwidth

The bandwidth utilization of IPFS data storage protocol is compiled by simulating the IPFS node for one hour duration in real-time. Fig. 4a shows the relative comparison of network bandwidth utilization by *VAHAK* with other traditional schemes. The network bandwidth of Ethereum is around 200Kbps to 300Kbps [25]. *VAHAK* outperforms in bandwidth utilization in range 51Kbps to 80 Kbps.

B. Scalability

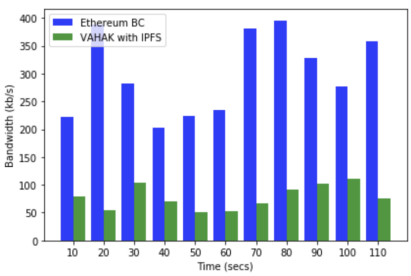
Fig. 4b shows the improved scalability based on the transaction time and the number of blocks mined during the Healthcare supplement processing of the *VAHAK* vs. the traditional approaches (both BC-based and non-BC based). In *VAHAK*, the 5G-enabled TI is used as communication medium to ensure the ultra-high reliability (i.e., *99.999%*) and ultra-low latency (i.e., $<$ 1ms). In *VAHAK*, any i^{th} patients MP_i is stored in IPFS, and only hash key H_K^i is sent to BC. Hash-key sizes are stored as 160 bits, which is less than original MP_i, whose size is in bytes. This allows more transactions to be appended to the BC. Thus, *VAHAK* offers more transactions to be added to the chain at the same quantum of time, which provides services the more number of users, hence improving the overall scalability.

C. Latency

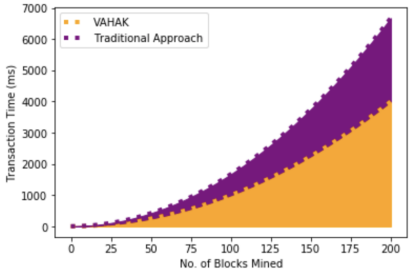
The latency comparison between the traditional approach and the proposed approach *VAHAK* based on the number of transactions is shown in Fig. 4c. Here, we consider the communication network of *VAHAK* is 5G-enabled TI, whereas LTE Advanced in the case of a traditional approach. Fig. 4c shows the linear regression of the calculated latency values of both methods. It illustrates that the latency in *VAHAK* is relatively low as compared to the LTE-based traditional approach. The reasoning behind this is the ultra-reliable low latency communications (URLLC) feature of TI [26], which It manages to attain round trip latency of $<$ 1ms, $(L_{5G-TI}) < 1ms)$ with 99.999% of reliability as compared to the round trip latency of LTE Advanced, which is below 10ms, $(LTE_{Advanced} < 10ms)$.

VI. Conclusion

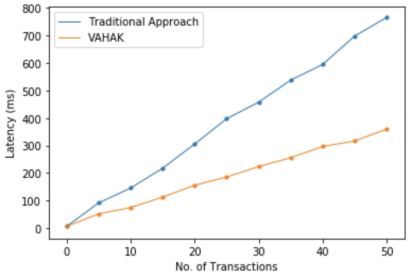
In this paper, a blockchain-based secure outdoor healthcare supply delivery scheme using UAVs called *VAHAK* is proposed. We have suggested deep insights into the traditional BC-based UAV system and highlight the latency, network bandwidth, and storage cost issues in detail. We presented how



(a) Bandwidth with Ethereum [25]



(b) Scalability with Traditional system.



(c) Latency with Traditional system.

Fig. 4: Performance Comparisons of *VAHAK*

ESC with IPFS and 5G-TI ensures security, privacy, ultra-low latency, ultra-high reliability, and cost-effective data storage by eliminating third-party organizations. We deployed the SCs over Remix IDE to view the block information. Finally, the performance of *VAHAK* is compared by considering the latency, scalability, and network bandwidth with the traditional BC-based systems over the LTE-Advanced communication network. In the future, we will improve the priority queue performance by eliminating the partial convoy effect with AI techniques.

ACKNOWLEDGMENT

This publication is an outcome of the R & D work undertaken project under the Visvesvaraya PhD Scheme of Ministry of Electronics & Information Technology, Government of India, being implemented by Digital India Corporation.

REFERENCES

[1] A. Kumari, S. Tanwar, S. Tyagi, and N. Kumar, "Fog computing for healthcare 4.0 environment: Opportunities and challenges," *Computers and Electrical Engineering*, vol. 72, pp. 1 – 13, 2018.

[2] J. Vora, P. Italiya, S. Tanwar, S. Tyagi, N. Kumar, M. S. Obaidat, and K. Hsiao, "Ensuring privacy and security in e- health records," in *2018 International Conference on Computer, Information and Telecommunication Systems (CITS)*, pp. 1–5, July 2018.

[3] J. J. Hathaliya, S. Tanwar, S. Tyagi, and N. Kumar, "Securing electronics healthcare records in healthcare 4.0 : A biometric-based approach," *Computers & Electrical Engineering*, vol. 76, pp. 398 – 410, 2019.

[4] S. Khan, "The health 4.0 revolution." https://health.economictimes.indiatimes.com/news/health-it/the-health-4-0-revolution/59187378. Accessed: 2020.

[5] R. Gupta, S. Tanwar, S. Tyagi, and N. Kumar, "Tactile-internet-based telesurgery system for healthcare 4.0: An architecture, research challenges, and future directions," *IEEE Network*, vol. 33, pp. 22–29, Nov 2019.

[6] M. Staff, "The biggest issues facing healthcare today." https://www.managedhealthcareexecutive.com/news/biggest-issues-facing-healthcare-today. Accessed: 2020.

[7] T. Nation, "20 per cent of emergency patient deaths blamed on traffic jam delays." https://www.nationthailand.com/national/30304268. Accessed: 2020.

[8] H. Innovations, "Top 8 challenges facing the healthcare supply chain." https://www.attainia.com/blog/challenges-facing-healthcare-supply-chain/. Accessed: 2020.

[9] M. Rucker, "The potential of drones providing health services." https://www.verywellhealth.com/potential-of-drones-providing-health-services-4018989. Accessed: 2020.

[10] "Security team exposes vulnerabilities in drones." https://www.trendmicro.com/vinfo/nl/security/news/internet-of-things/security-team-exposes-vulnerabilities-in-drones. Accessed: 2020.

[11] A. J. A. Dhivya and J. Premkumar, "Quadcopter based technology for an emergency healthcare," in *2017 Third International Conference on Biosignals, Images and Instrumentation (ICBSII)*, pp. 1–3, March 2017.

[12] V. V. Krishna, S. Shastri, and S. Kulshrestha, "Design of rpv for medical assistance," in *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1–7, July 2018.

[13] J. Vora, S. Tanwar, S. Tyagi, N. Kumar, and J. J. P. C. Rodrigues, "Home-based exercise system for patients using iot enabled smart speaker," in *2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom)*, pp. 1–6, Oct 2017.

[14] K. R. Ashok, P. Arulselvan, A. Ashif, S. Gokul, and R. Kuppusamy, "Aero ambulance quad copter based technology for an emergency healthcare," in *2019 5th International Conference on Advanced Computing Communication Systems (ICACCS)*, pp. 1197–1200, March 2019.

[15] R. Gupta, S. Tanwar, S. Tyagi, N. Kumar, M. S. Obaidat, and B. Sadoun, "Habits: Blockchain-based telesurgery framework for healthcare 4.0," in *2019 International Conference on Computer, Information and Telecommunication Systems (CITS)*, pp. 1–5, Aug 2019.

[16] G. G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, pp. 1–32, 2014.

[17] R. Gupta, S. Tanwar, F. Al-Turjman, P. Italiya, A. Nauman, and S. W. Kim, "Smart contract privacy protection using ai in cyber-physical systems: Tools, techniques and challenges," *IEEE Access*, pp. 1–1, 2020.

[18] A. Islam and S. Y. Shin, "Bhmus: Blockchain based secure outdoor health monitoring scheme using uav in smart city," in *2019 7th International Conference on Information and Communication Technology (ICoICT)*, pp. 1–6, July 2019.

[19] S. Tanwar, K. Parekh, and R. Evans, "Blockchain-based electronic healthcare record system for healthcare 4.0 applications," *Journal of Information Security and Applications*, vol. 50, p. 102407, 2020.

[20] R. Gupta, S. Tanwar, S. Tyagi, and N. Kumar, "Tactile internet and its applications in 5g era: A comprehensive review," *International Journal of Communication Systems*, vol. 32, no. 14, p. e3981, 2019. e3981 dac.3981.

[21] A. Rajalakshmi, K. Lakshmy, M. Sindhu, and P. Amritha, "A blockchain and ipfs based framework for secure research record keeping," *International Journal of Pure and Applied Mathematics*, vol. 119, pp. 1437–1442, 01 2018.

[22] P. Mehta, R. Gupta, and S. Tanwar, "Blockchain envisioned uav networks: Challenges, solutions, and comparisons," *Computer Communications*, vol. 151, pp. 518 – 538, 2020.

[23] ConsenSys, "Mythril security analysis tool." https://github.com/ConsenSys/mythril. Online; Accessed: 2019.

[24] R. M. Parizi, A. Dehghantanha, K.-K. R. Choo, and A. Singh, "Empirical vulnerability analysis of automated smart contracts security testing on blockchains," in *Proceedings of the 28th Annual International Conference on Computer Science and Software Engineering*, CASCON '18, (USA), p. 103–113, IBM Corp., 2018.

[25] StackExchange, "How fast should be an internet connection to mine eth?." https://ethereum.stackexchange.com/questions/3138/how-fast-should-be-an-internet-connection-to-mine-eth. Accessed: 2018.

[26] I. Budhiraja, S. Tyagi, S. Tanwar, N. Kumar, and J. J. Rodrigues, "Tactile internet for smart communities in 5g: An insight for noma-based solutions," *IEEE Transactions on Industrial Informatics*, pp. 1–1, 2019.