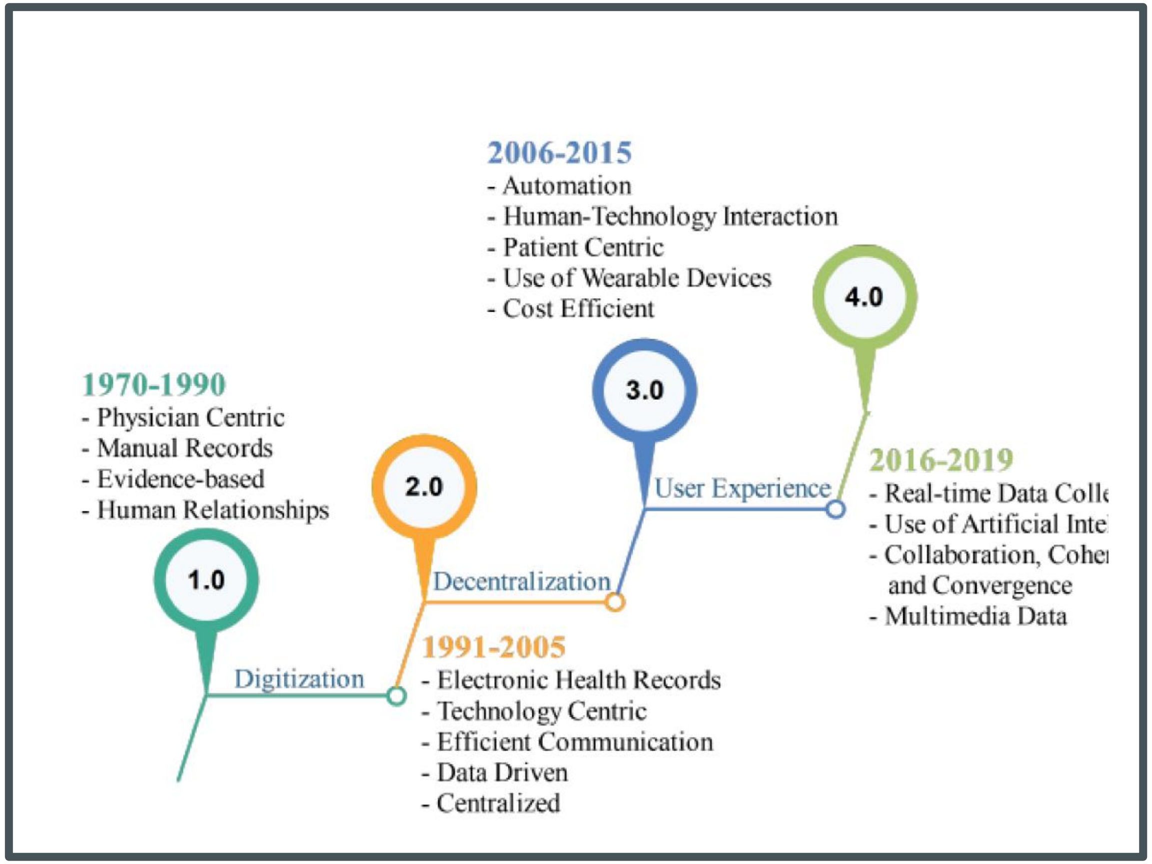
USE CASE ON VAHAK: A BLOCKCHAIN-BASED OUTDOOR DELIVERY SCHEME USING UAV FOR HEALTHCARE 4.0 SERVICES

SUDEEP TANWAR

PRESENTATION OUTLINE

- Introduction
- Research Contributions
- System Model
- *VAHAK:* The Proposed Approach
- Formal Security Verification of *VAHAK*
- Results and Discussion
- Conclusion
- References

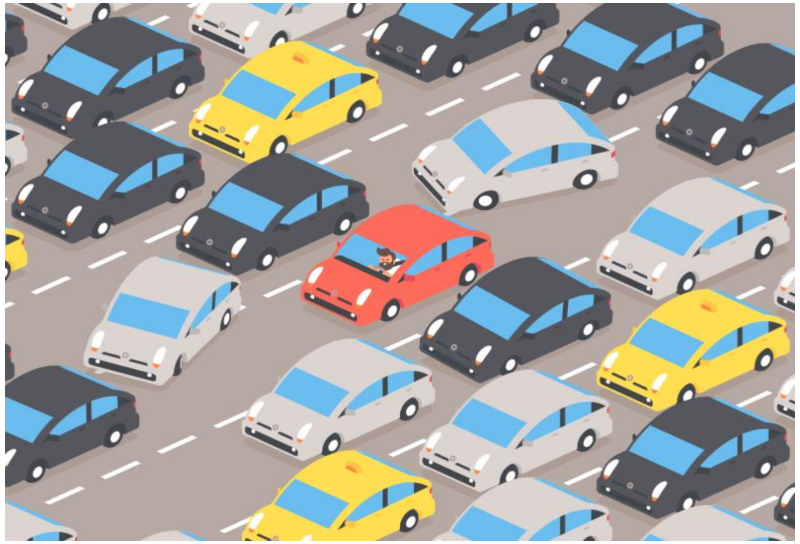
INTRODUCTION



Technological Revolution in Healthcare Industry

- Healthcare is the prime concern for the overall growth of any nation.
- It delivers medical care services to the people around the world with a vision to achieve a healthy and wealthy life.
- The healthcare industry has revolutionized from 1.0 to 4.0.

INTRODUCTION

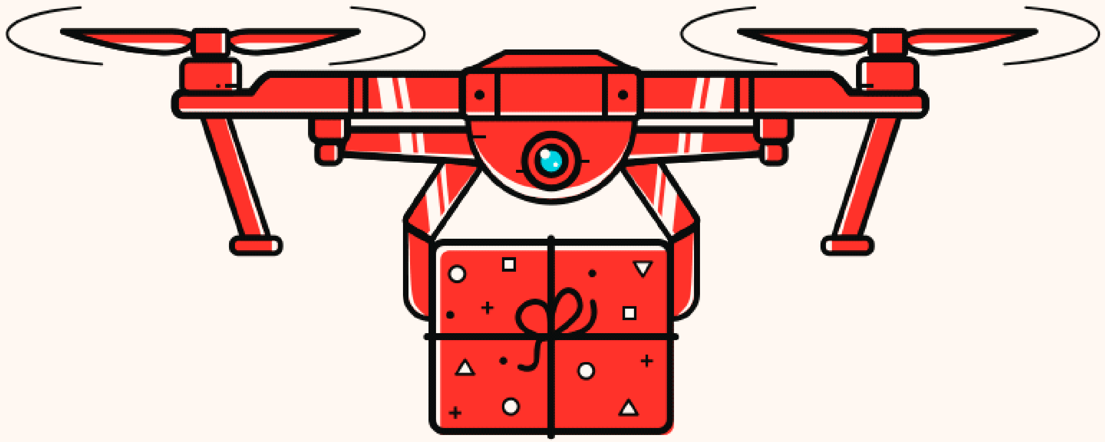


Traditional healthcare supply chain systems delivered medicines through road transport infrastructure, which has many limitations, such as road traffic, congested roads, and long-distance to cover.

Statistics given in show that 20% of emergency patients' deaths were caused by traffic jams.

One plausible solution to the above-illustrated issues is to change the mode of transportation

INTRODUCTION



- 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.

INTRODUCTION

- 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.
- This has raised various concerns about the security and reliability of **adopting drones** for healthcare-related deliveries.

Image Source: https://medium.com/@rchen8/cyber-security-and-physical-security-are-very-different-22e31a933907

INTRODUCTION (LITERATURE)

[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 (IEEE 802.15.4 (ZigBee) protocol).
- But the authors have not given much importance to the communication network properties, such as bandwidth, latency, and security.

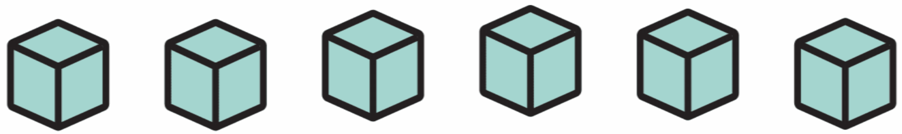
[14]

- The authors have developed a quad-copter prototype, i.e., aero ambulance. 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.

[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.
[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.

INTRODUCTION (BLOCKCHAIN)

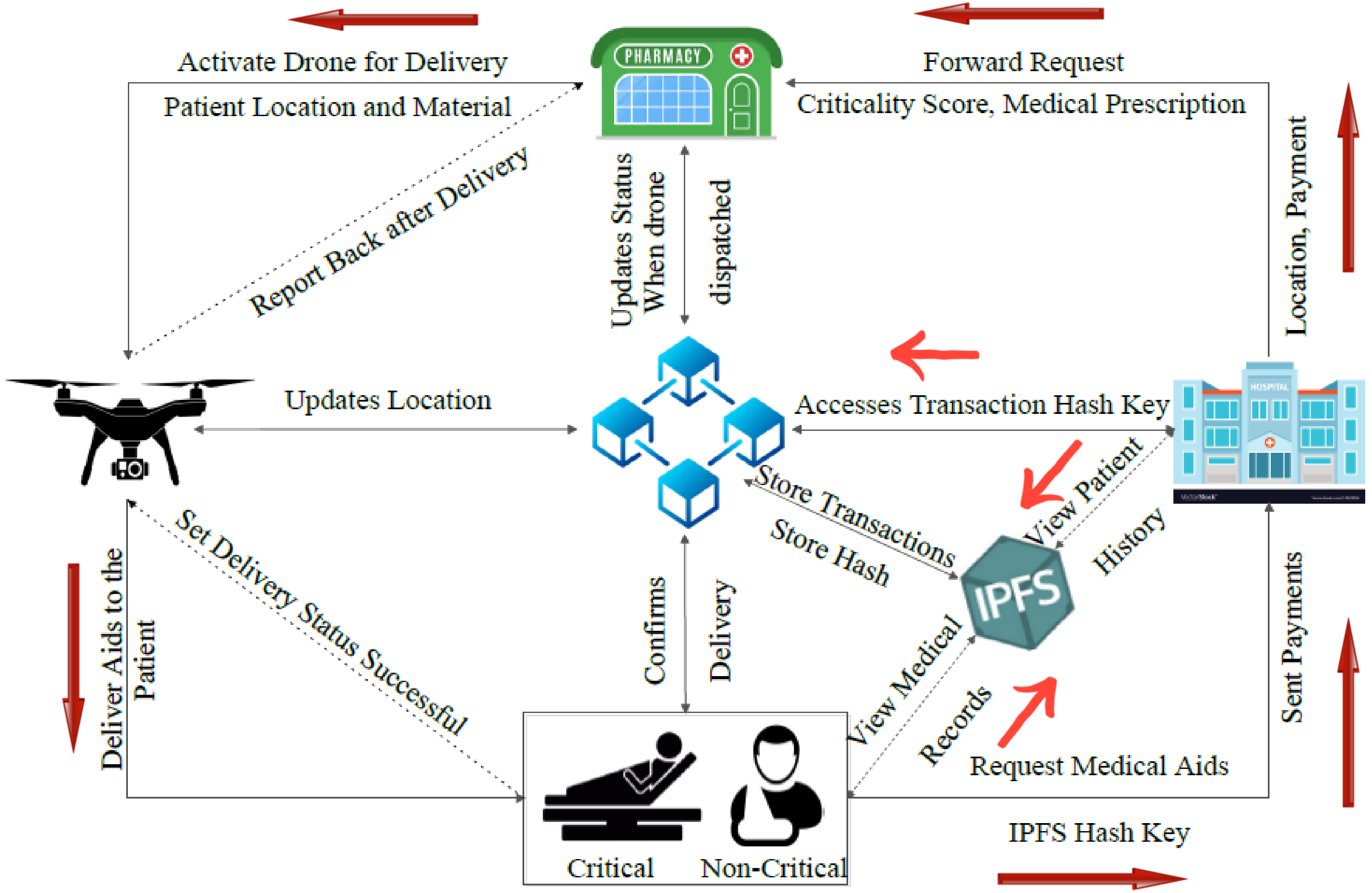
- BC and smart contract (SC) seem to be the technological solutions to overcome the security issues.
- This paper proposes an _Ethereum BC-based SCs for healthcare supply_ using UAVs called ***VAHAK*** that ensures the transaction reliably and security.
- VAHAK also ensures the **trust between all stakeholders** via the immutability and transparency of records.
- SCs are self-executable, self-verifiable, self-enforceable, and self-validated the transactions between system entities.



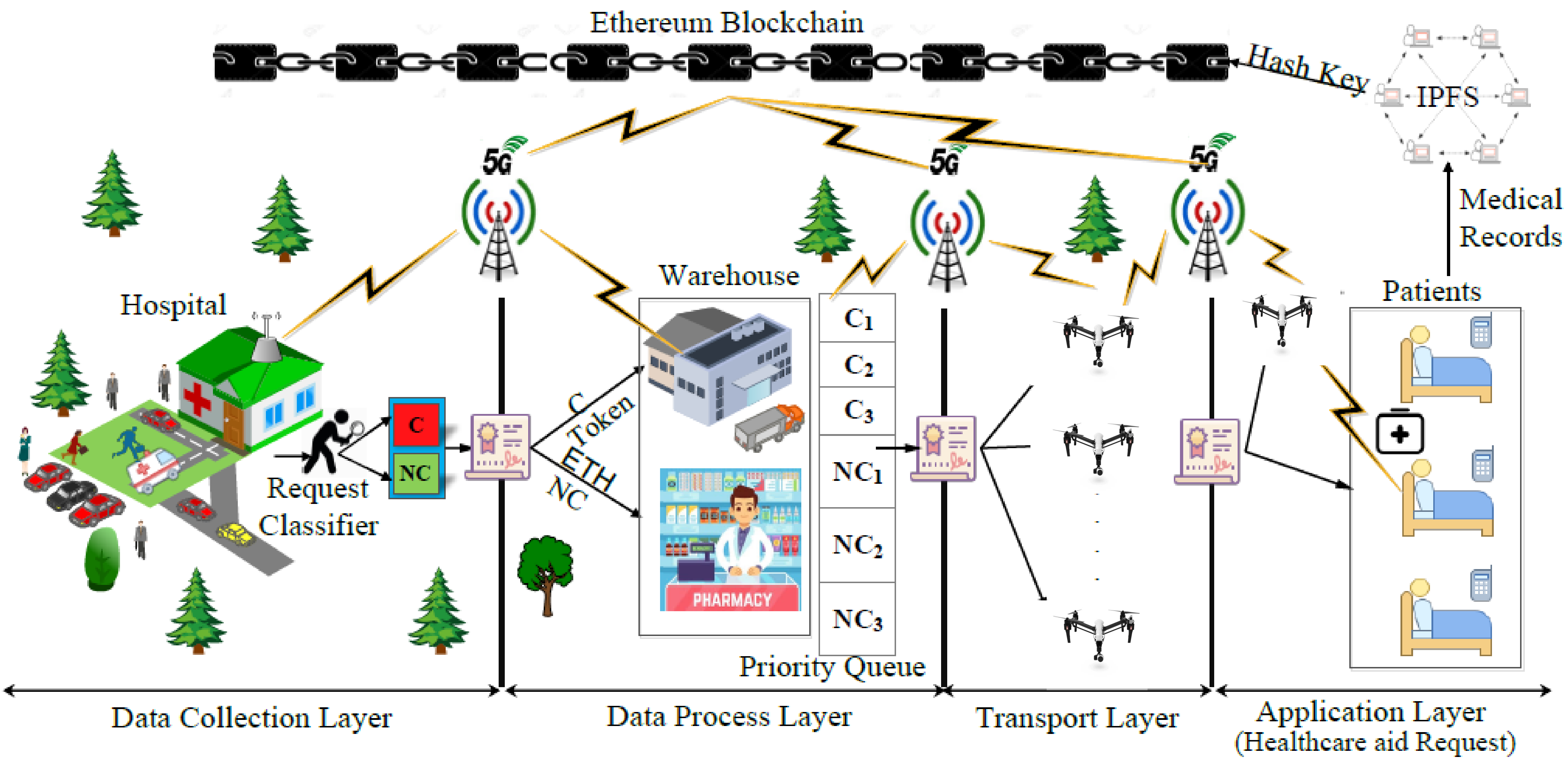
RESEARCH CONTRIBUTIONS

- Following are the research contributions of this case study.
- An Ethereum SC-based secure approach is proposed to track the delivery of healthcare supplies by UAVs.
- An 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.

SYSTEM MODEL

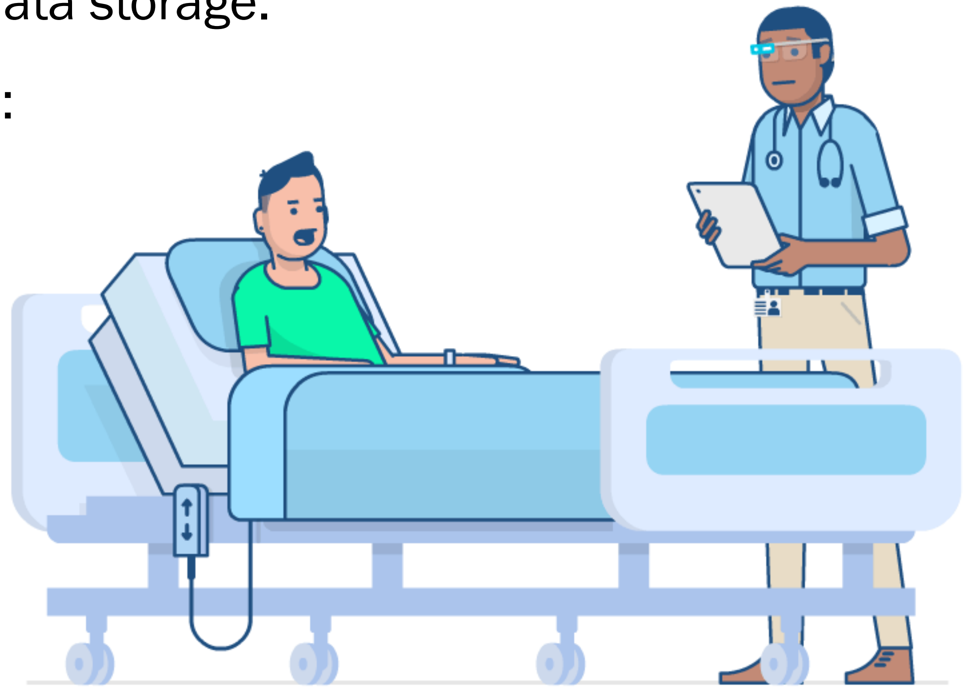


VAHAK: THE PROPOSED APPROACH



VAHAK: THE PROPOSED APPROACH

- *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.
- *VAHAK* is divided into four different working layers:
  - (i) Data collection Layer
  - (ii) Data process Layer
  - (iii) Transport Layer
  - (iv) Application Layer.



VAHAK: THE PROPOSED APPROACH

- 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.

Application Layer

- It consists of a patient who needs medical aid, and a caregiver or bystander can also be a part of this layer.
- They can put their request for healthcare aids from this layer.
- It also gives the location where the required supplies get delivered by UAVs and must be in the proximity

VAHAK: THE PROPOSED APPROACH

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
$R \in \{R_{Patient}, R_{Hospital}, R_{Warehouse}, R_{Authority}, R_{UAV}\}$.

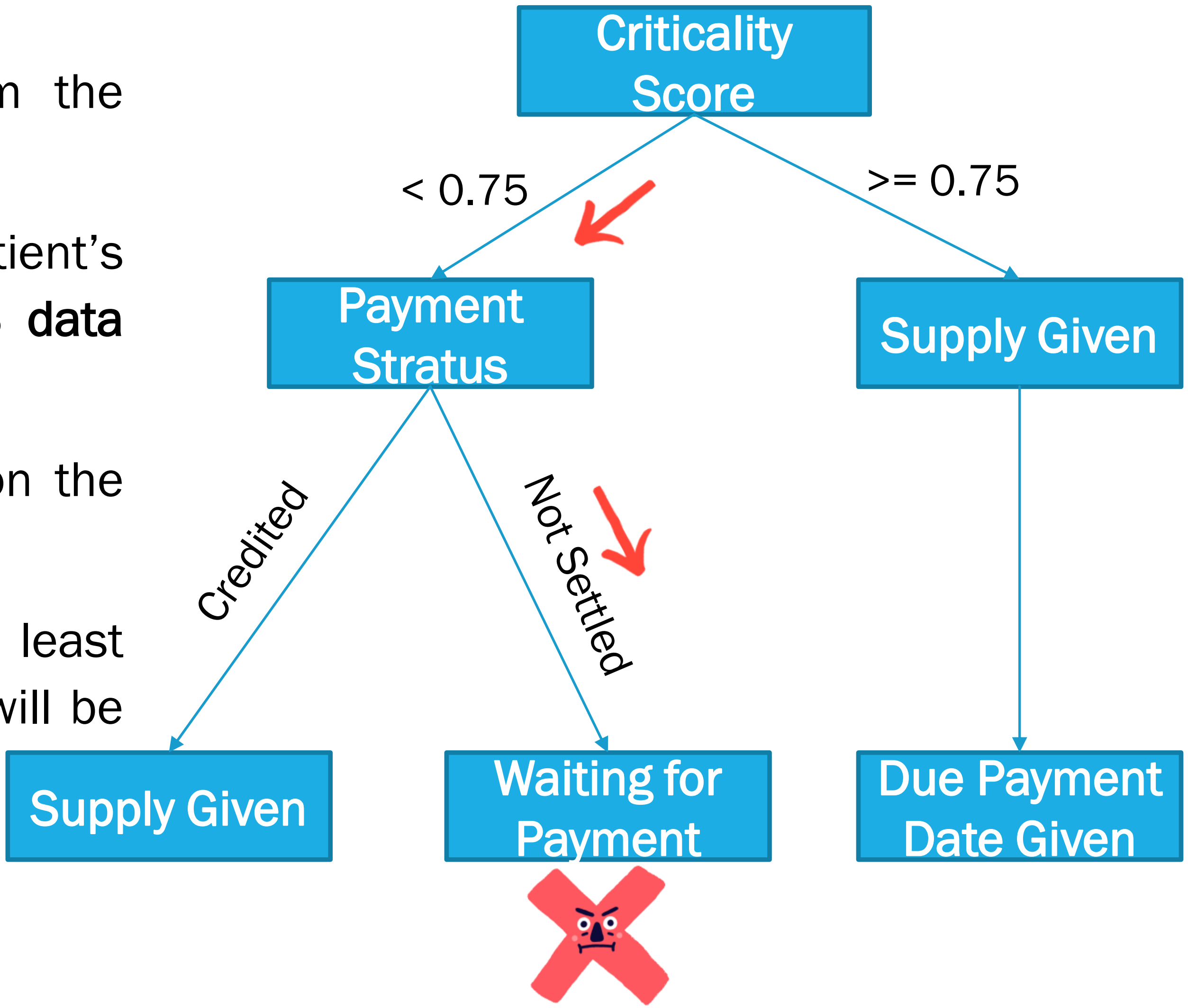
procedure PATIENT_REQUEST(R, MP_i)
  if ($R \in R_{Patient}$) **then**
    $H_k \leftarrow$ REQUEST_HEALTH_SUPPLY($ID(P_i), H^i_{Key}$)
    while (Items_Left $>$ 0) **do**
      $H_k \leftarrow$ ADD_PRESCRIPTION_ITEMS (MP_i)
    end while
  else
    $R_{Authority} \leftarrow$ REQUEST_REGISTRATION (R, P_n)
  end if
  while (TRUE) **do**
    if (No_Item_Left) **then**
      $R_{Patient} \leftarrow CS_{Aggregated}$
      $ETH_{Tx\_Fee} \leftarrow$ CALCULATE_BILL(P^i_D)
    else
      $CS(P^i_D) \leftarrow$ GENERATE_CS(P^i_D)
      $CS_{Aggregated} \leftarrow CS_{Aggregated} + CS(P^i_D)$
    end if
  end while
  $H_i \leftarrow$ REQUEST_CLASSIFY ($CS_{Aggregated}$)
  $R_{Patient \rightarrow Type} \rightarrow \{C, NC\}$
  $R_{Validate} \leftarrow$ VALIDATE_PRESCRIPTION (MP_i, H^i_{Key})
  $R_{Patient \rightarrow Valid} \rightarrow$ VALID(*0:FALSE, 1:TRUE*)
  if ($R_{Patient \rightarrow Type} == NC$) **then**
    $R_{Hospital} \leftarrow$ TRANSFER($R_{Patient}, ETH_{Tx\_Fee}$)
  end if
end procedure

VAHAK: THE PROPOSED APPROACH

Data Collection Layer

- It receives the medical supply request from the patient.
- It uses the patient **Hash Key** to access the patient's medical records that are stored on the **IPFS data storage** system.
- Requests are classified into **C or NC** based on the level of criticality (**Criticality Score**).
- 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 patient is not critical and payment not settled, then the flow will be like:



VAHAK: THE PROPOSED APPROACH

Data Process Layer

- It consists of healthcare supplies like first aid kits, vaccines, medicines, or insulin.
- It also maintains a **multi-level priority queue** (PQ) based on the criticality score request received from the data collection layer.
- All NC the requests are being stored in the first-come-first-serve manner.

VAHAK: THE PROPOSED APPROACH

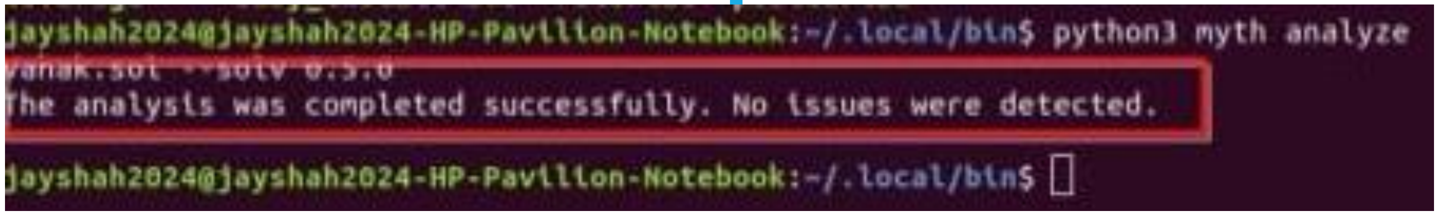
Algorithm 2 Hospital to warehouse communication

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 ($R \in R_{Hospital}$) **then**
        $R_{Warehouse} \leftarrow$ REQUEST_SUPPLIES($MP_i, R_{Patient}$)
        if ($R_{Patient \rightarrow Type} == C$) **then**
            $R_{Warehouse} \leftarrow$ GENERATE_TOKEN ($R_{Patient}, R_{Hospital}, MP_i$)
            $R_{Patient} \leftarrow$ GRANT_PERIOD(ETH_{Tx_Fee}, T)
        else
            $R_{Warehouse} \leftarrow$ TRANSFER($R_{Hospital}, ETH_{Tx\_Fee}$)
        end if
    else
        $R_{Authority} \leftarrow$ REQUEST_REGISTRATION ($R_{Hospital}$)
    end if
    $R_{Warehouse} \leftarrow$ ADD_TO_PQUEUE ($R_{Patient}$)
    while (TRUE) **do**
        if (UAV_AVAILABLE() = = TRUE) **then**
            $R_{UAV} \leftarrow$ INITIATE_DELIVERY(MP_i, UAV_h)
            BREAK()
        end if
    end while
end procedure

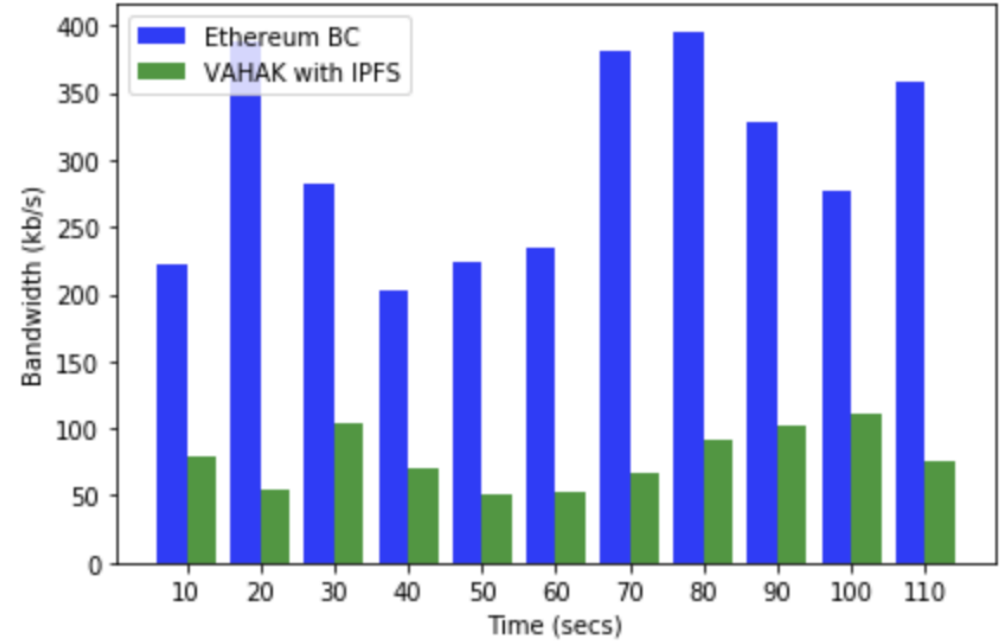
FORMAL SECURITY VERIFICATION OF *VAHAK*

- The proposed SC in VAHAK are analyzed for security vulnerabilities using **MyThril** tool.
- As output, it returned a message “**No issues were detected**”



Formal security verification of VAHAK

RESULTS AND DISCUSSION



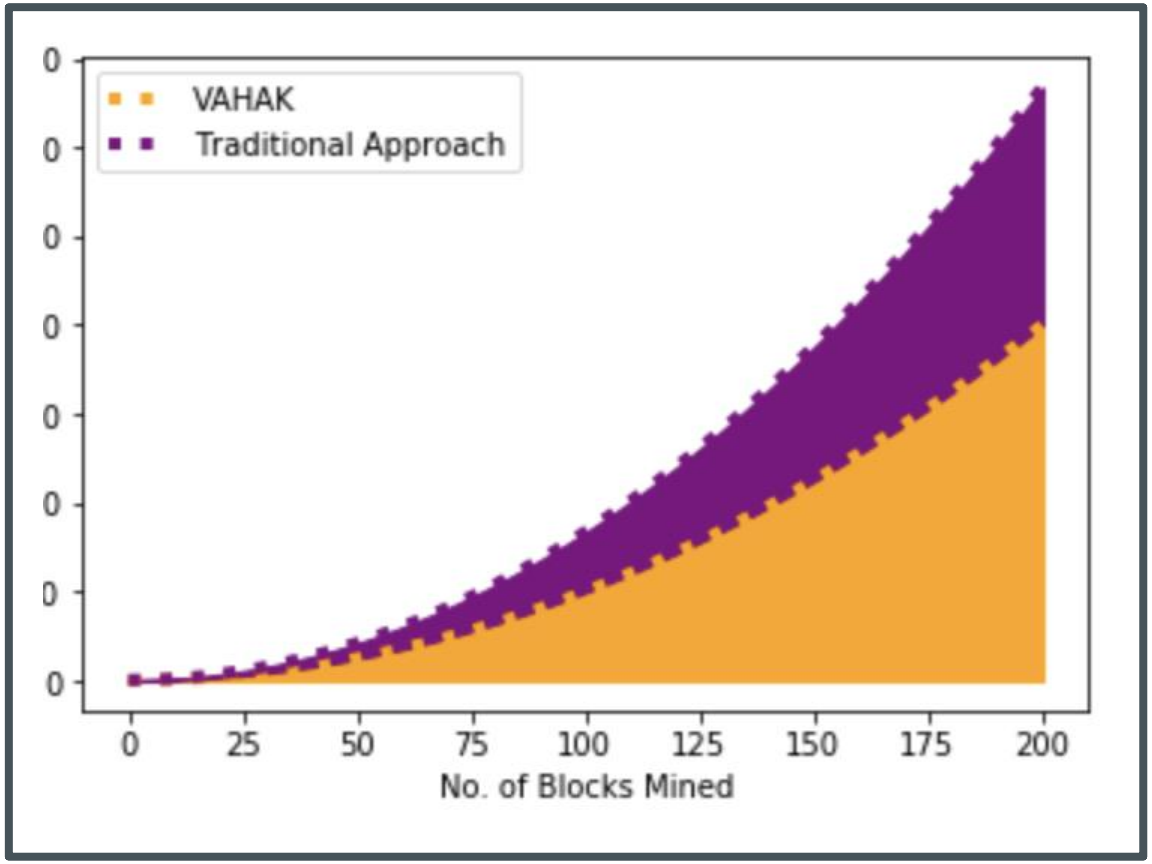
Comparison of *VAHAK* Bandwidth with Ethereum

- We evaluate the performance of VAHAK with respect to the scalability, bandwidth, latency, and data storage cost.

Bandwidth

- The bandwidth utilization of IPFS data storage protocol is compiled by simulating the IPFS node for one-hour duration in real-time.
- The network bandwidth of Ethereum is around **200Kbps to 300Kbps.**
- VAHAK outperforms in bandwidth utilization in range **51Kbps to 80 Kbps.**

RESULTS AND DISCUSSION

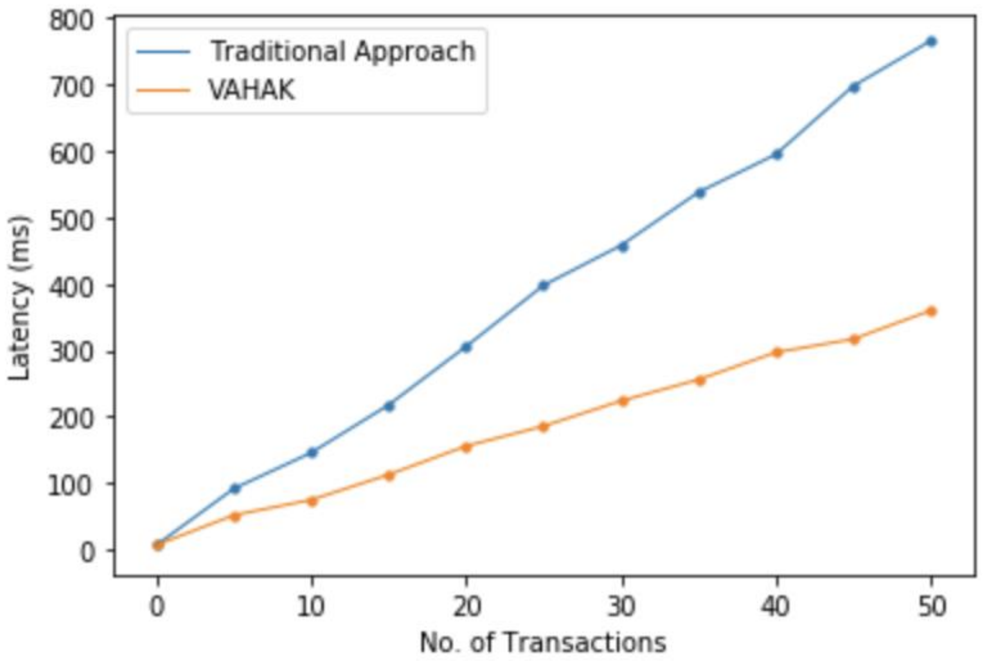


Comparison of *VAHAK* Scalabity with Ethereum

Scalability

- Thus, VAHAK offers more transactions to be added to the chain at the same quantum of time, which provides services the greater number of users, hence improving the overall scalability.

RESULTS AND DISCUSSION



Comparison of *VAHAK* Latency with Ethereum

Latency

- The latency comparison between the traditional approach and the proposed approach VAHAK based on the number of transactions

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 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.

REFERENCES

- 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.
- S. Khan, “The health 4.0 revolution.” https://health.economictimes. indiatimes.com/news/health-it/the-health-4-0-revolution/59187378. Accessed: 2020.
- M. Staff, “The biggest issues facing healthcare today.” https://www.managedhealthcareexecutive.com/news/biggest-issuesfacing-healthcare-today. Accessed: 2020.
- T. Nation, “20 per cent of emergency patient deaths blamed on traffic jam delays.” https://www.nationthailand.com/national/30304268. Accessed: 2020
- H. Innovations, “Top 8 challenges facing the healthcare supply chain.” https://www.attainia.com/blog/challenges-facing-healthcaresupply-chain/. Accessed: 2020.
- M. Rucker, “The potential of drones providing health services.” https://www.verywellhealth.com/potential-of-drones-providing-healthservices-4018989. Accessed: 2020.
- “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.
- G. G. Wood, “Ethereum: A secure decentralised generalised transaction ledger,” Ethereum project yellow paper, vol. 151, pp. 1–32, 2014.
- 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.
- ConsenSys, “Mythril security analysis tool.” https://github.com/ ConsenSys/mythril. Online; Accessed: 2019.