Journal of ISMAC (2021)
Vol.03/ No.02
Pages: 121-131
http://irojournals.com/iroismac/
DOI: https://doi.org/10.36548/jismac.2021.2.005

Security Enhanced Blockchain based Unmanned Aerial Vehicle Health Monitoring System

Jennifer S. Raj,
Professor,
Department of ECE,
Gnanamani College of Technology,
Namakkal, India.
Email: jennifer.raj@gmail.com

Abstract: In this research work and unmanned aerial vehicle (UAV) that uses blockchain methodology to collect health data from the users and saves it on a server nearby is introduced. In this paper the UAV communicates with the body sensor hives (BSH) through a low-power secure manner. This process is established using a token with which the UAV establishes relationship with the BSH. The UAV decrypts the retrieved HD with the help of of the shared key, creating a two-phase authentication mechanism. When verified, the HT is transmitted to a server nearby in a safe manner using blockchain. The proposed healthcare methodology is analysed to determine its feasibility. Simulation and implementation is executed and a performance of the work is observed. Analysis indicates that the proposed work provides good assistance in a secure environment.

Keywords: UAV, Blockchain, Healthcare, IoT, Security, Body Sensor Hives

1. Introduction

A network of actuators, sensors, etc., connected by means of internet to share data with each other is known as the internet of things. IoT is expected to grow in an exponential manner by 2030. Agriculture, smart grid and smart home are some of the various fields in which IoT has contributed a significant part and its role in healthcare is worth noting. The sensors and actuators provided in IoT are used to determine health information about a person such as electrocardiogram and blood pressure when it is placed near the body of the person.

ISSN: 2582-1369 (online)
Submitted: 29.04.2021
Revised: 25.05.2021
Accepted: 6.06.2021
Published: 14.06.2021

In rural environment and remote locations where access to the patient is difficult, collection of health information using IoT plays a prominent role in enabling a safe environment for the patients as well as the health care professionals. However activators and IoT sensors that are used to collect the health data face serious issues in terms of connectivity. Hence an unmanned aerial vehicle (UAV) [1] provides the apt solution for enabling access to the remote location. The promising characteristics of UAV such ubiquity, low maintenance cost and ease of deployment has drawn the attention of researchers resulting in application of UAV in several technological ventures such as product delivery, public safety and border surveillance. Because of its versatile characteristics, UAV is capable of supporting the IoT devices. To be specific UAV has the ability to provide solutions for severe issues such as remote data acquisition, network availability, low power communication etc., with respect to body sensors. However when the servers and IoT sensors communicate, they face a number of threats such as spoofing, reply attack and man-in-the-middle. Moreover it is crucial to preserve the integrity of the collected data. Authors in [x] have introduced UAV with healthcare architecture such that it performs data collection from the body sensor networks and further sends the collected data to a server [2].

However the authors have not considered security mechanism while transmitting as well as storing the collected data. Similarly in [3] the authors have developed a smart health monitoring system which collects data from the body sensors and sent to a smartphone by means of a cloud server. On the other hand authors in [4]collected data using a cloud based health monitoring device. Fog assisted health monitoring equipments were proposed by authors in [5] such that the data is gathered from the user and send to the cloud via fog nodes. Authors in [6] use smart gateways close to sensor nodes and fog computing to build an IoT based healthcare scheme. A cloud based system that monitors the health of a patient in real time with privacy preservation is proposed in [7]. However methods to secure the transmission of data as well as its storage are not examined my authors in [8]-[11]. Authors in [12] conducted research taking into account security issues but you saved to consider Data integrity on the server. Moreover the scarcity of network availability in remote locations was not considered in many of the researches [13]. When blockchain is used it copies data and stores it in every year similar to a distributed ledger. Using the logic protected from the

ISSN: 2582-1369 (online)
Submitted: 29.04.2021
Revised: 25.05.2021
Accepted: 6.06.2021
Published: 14.06.2021

contract a computer program is developed known as a smart contract which automates in blockchain through information management. Distributed computing [14], Data integrity [15] and secure communication are some of the advantages of using blockchain and proved to be effective in upholding data integrity and fending security attacks. In this work a blockchain based healthcare methodology is implemented by data collection through UAV [16].

The major contributions of this research work are as follow:

- A system model of an Unmanned Ariel Vehicle is used to collect health data from the patient using blockchain. This data is received by means of two-phase authentication.
- In this work, we have used a threat model to analyze the security aspects of in health data acquisition methodology.
- Based on false detection rate, dataset size, energy consumption and validation time, the proposed work is simulated and analyzed.
- The performance of the proposed work is analysed in terms of energy consumption, individual processing time and data transmission.

The healthcare UAV is incorporated with blockchain using Ethereum platform and the output of the work is analyzed in terms of block size, latency and throughput. The rest of the paper is organiszed such that section 2 outlines the UAV-assisted healthcare scheme, followed by methodology involved in communication in section 3. The simulation results are analyzed in section 4 and based on the results, a conclusion is arrived at in section 5.

2. Proposed UAV based Health Scheme

Figure 1 represents outline of the proposed health scheme. The following components contribute towards health care

- Health data is collected using the body sensor hive and then transmitted to the server nearby with the help of UAV.

ISSN: 2582-1369 (online)
Submitted: 29.04.2021
Revised: 25.05.2021
Accepted: 6.06.2021
Published: 14.06.2021

- This data is collected by the server and then saved using blockchain with proper permissions from the validator.

Depending on the communication channel available, different type of services are considered. When mobile network is available, Mobile edge computing (MEC) is used such that the private cloud, ground control station and MEC server perform the function of a validator to add data to the blockchain. Any non-government organisation or hospital will be able to access this data on prior permission from the users [17]. Every validator is connected to a satellite or for mobile networks depending on channel availability. The data is collected from the user by means of UAV and are safeguarded by means of blockchain. To access the data, users must initially register using their personal details which is also saved and maintained securely using a smart contract in blockchain [18].

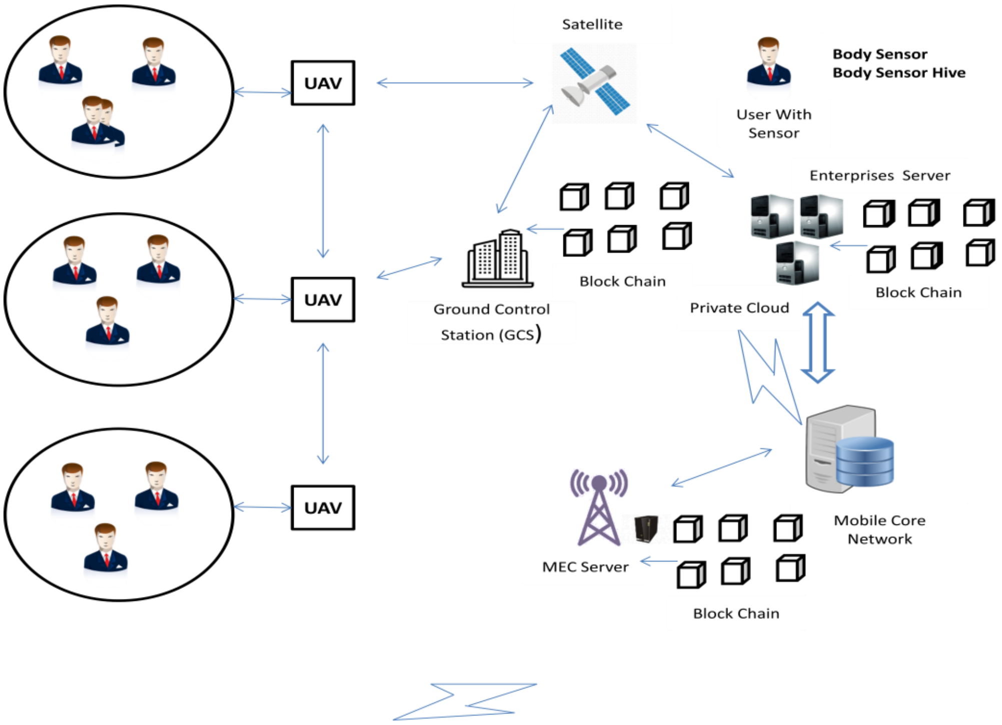

Fig.1. Proposed Blockchain Based HealthCare System

ISSN: 2582-1369 (online)
Submitted: 29.04.2021
Revised: 25.05.2021
Accepted: 6.06.2021
Published: 14.06.2021

Before launching of the UAV a token is created by the server using a smart contract that uses a public key. On deployment, the UAV synchronises the data with the BSH of the user. Synchronisation data is collected by the UAV from the BSH. The data is properly encrypted and then transmitted to the UAV. On receiving the data the UAV will first verify the authenticity of the data and will also check the sender's validity. If data is verified properly it is forwarded to the nearest server where it is saved using blockchain on instructions given by the validators [19][20].

3. Proposed Work

3.1 Implementation of Methodology:

All UAV, servers as well as users must register with the system to obtain public key that they can use to sync with the BSH. Random seed r_s, current timestamp τ_c and MAC address α is used to generate private key. To create the private key, let Ω be the hash generated such that Ω=$\Phi(\alpha, \tau_c, r_s)$. Then the public key can be determined using the expression given in (1).

$$\partial_k = \Pi(\Omega)|\Pi: \{0,1\} * \rightarrow \{0,1\}^s, \rho_k = \partial_k \otimes (G_a, G_b) \quad (1)$$

where the coordinates of the identified curve is represented by G. Once the key is generated, the server or UAV or BSH will register the spatial information, basic information and key in the blockchain-generated smart contract. Hence a smart contract will be able to store all the information in a secure manner. A trust token is created by the server during the time of information storage to help the server communicate with the device and vice versa. This trust token can be expressed using equation (2).

$$T = \Phi\ (\mathrm{S}_{\Omega}, \tau_c, \delta, \gamma_{\{\mathrm{lt,ln}\}}|\Phi: \{0,1\} * \rightarrow \{0,1\}^l \quad (2)$$

where $\gamma_{\{\mathrm{lt,ln}\}}$ represents spatial information which is saved in the blockchain server.

3.2 Attacks:

In this methodology, the threats faced by the UAV during data transmission are as follows:

- Reply attack: The attack is found between the receiver and the sender in reply attacks. This attacker will store the information packets which he will use later on to communicate. The vulnerable places where attacks occur are identified to be between server and UAV, and between UAV and BSH. Reply attack is executed when the attacker uses the information that it has stored to gain access to the UAV. This attack occurs when the attacker sends an obsolete data between the server and UAV.
- Illegal Data tampering: Another serious threat faced is illegal tempering of data that shakes the integrity of the saved information. In this scenario, the attacker could be either an outsider or an insider. This is mainly because, data is vulnerable inside the server and inside the UAV. Hence if either the USB or the server is compromised by means of an attack the data saved can be tampered with.
- Unauthorized Access: Unauthorised Access is a severe threat that is faced by this methodology such that a malware is installed in a system which allows it to access sensitive information. In such cases the attacker will either silently steal information or directly harm the system. When the data is collected through UAV the attacker tries to intrude into the UAV by sending synchronising data, enabling access to tamper with the original data present.
- Man-In-The-Middle: The man-in-the-middle attack takes place between the server and UAV and between the UAV and BSH. In general the attacker is an outsider and on access will be able to obtain sensitive information and also alter it.

4. Results and Discussion

The effectiveness of the hash boom filter used in the proposed methodology is obtained through simulation results. The following figures represent the time taken to validate the BSH with the help of a classic algorithm, hash table and hash Bloom filter. Figure 2 indicates that

ISSN: 2582-1369 (online)
Submitted: 29.04.2021
Revised: 25.05.2021
Accepted: 6.06.2021
Published: 14.06.2021

to validate the BSH, classic algorithm takes more time when compared with other similar methodologies. This is mainly because of the linear search check that is executed by this algorithm to identify the data set. Figure 3 shows a graphical representation of the energy consumed to validate the BSH. Similar to figure 2, figure 3 also shows a higher consumption of energy by the classic algorithm.

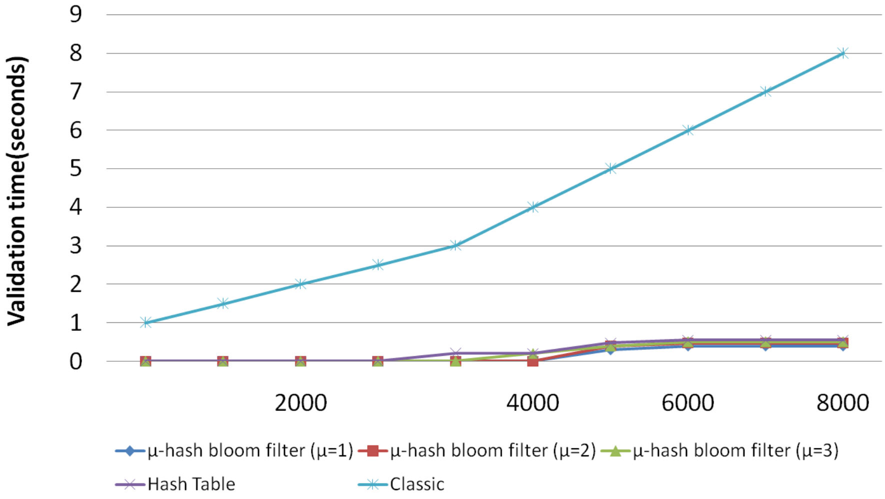

Fig.2. Time Taken for Validation

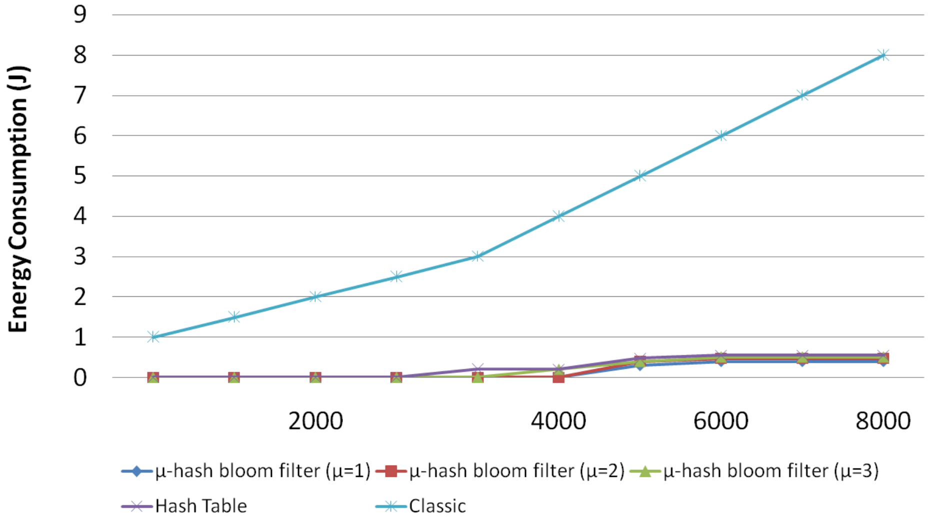

Fig.3. Energy Consumption for Validation

ISSN: 2582-1369 (online)
Submitted: 29.04.2021
Revised: 25.05.2021
Accepted: 6.06.2021
Published: 14.06.2021

Similarly Fig.4 and Fig.4 show a comparison in terms of size of datasets and false detection rate, respectively.

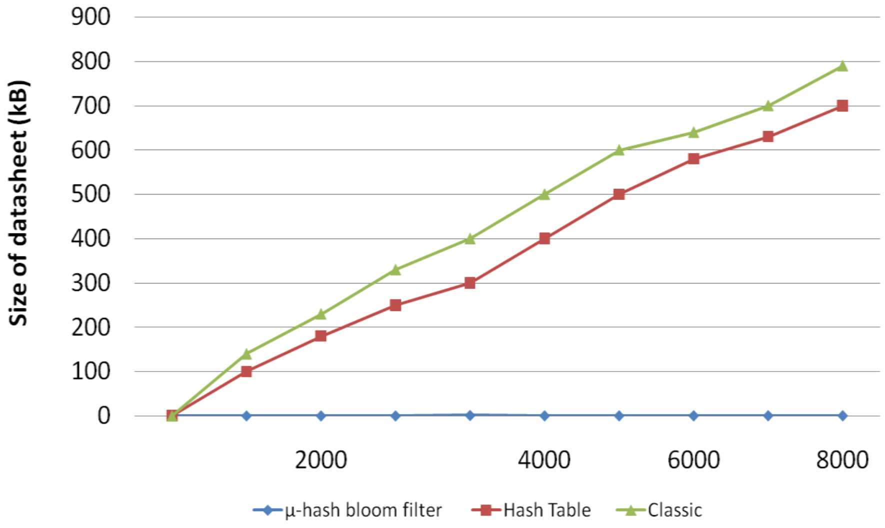

Fig.4. Size of Validation

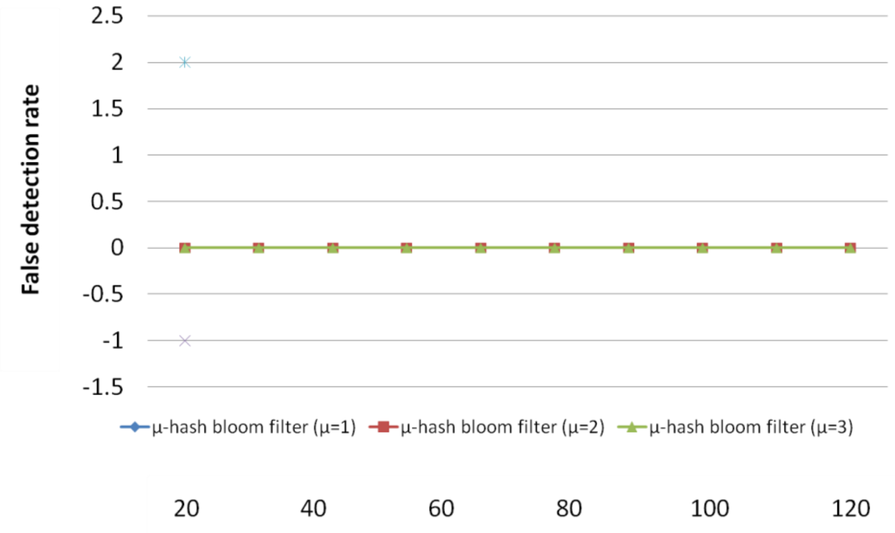

Fig.5. Block size in Blockchain

ISSN: 2582-1369 (online)
Submitted: 29.04.2021
Revised: 25.05.2021
Accepted: 6.06.2021
Published: 14.06.2021

5. Conclusion

In this proposed work a blockchain-based UAV- health monitoring system is proposed. Health data is collected from the BSH and transmitted to a server nearby with the help of UAV. To maintain security while transmitting data, a shared key methodology is incorporated such that this key is used to encrypt the data. At the receiving end this data is decrypted using the common key. To determine the feasibility of the proposed work a security analysis is carried out and it is found that there is a significant improvement in data transmission security as well as data integrity. As future scope one can analyse the implementation of a similar methodology using satellite communication in remote areas.

References

[1] Sankarasrinivasan, S., E. Balasubramanian, K. Karthik, U. Chandrasekar, and Rishi Gupta. "Health monitoring of civil structures with integrated UAV and image processing system." *Procedia Computer Science* 54 (2015): 508-515.

[2] Shakya, Subarna, and Lalitpur Nepal. "Computational Enhancements of Wearable Healthcare Devices on Pervasive Computing System." Journal of Ubiquitous Computing and Communication Technologies (UCCT) 2, no. 02 (2020): 98-108.

[3] Qiu, L., & Yuan, S. (2009). On development of a multi-channel PZT array scanning system and its evaluating application on UAV wing box. *Sensors and Actuators A: physical*, *151*(2), 220-230.

[4] Chen, J. I. Z., & Yeh, L. T. (2020). Data Forwarding in Wireless Body Area Networks. Journal of Electronics, 2(02), 80-87.

[5] Dash, J. P., Watt, M. S., Pearse, G. D., Heaphy, M., & Dungey, H. S. (2017). Assessing very high resolution UAV imagery for monitoring forest health during a simulated disease outbreak. *ISPRS Journal of Photogrammetry and Remote Sensing*, *131*, 1-14.

[6] Adithya, M., P. G. Scholar, and B. Shanthini. "Security Analysis and Preserving Block-Level Data DE-duplication in Cloud Storage Services." Journal of trends in Computer Science and Smart technology (TCSST) 2, no. 02 (2020): 120-126.

ISSN: 2582-1369 (online)
Submitted: 29.04.2021
Revised: 25.05.2021
Accepted: 6.06.2021
Published: 14.06.2021

[7] Khadka, A., Fick, B., Afshar, A., Tavakoli, M., & Baqersad, J. (2020). Non-contact vibration monitoring of rotating wind turbines using a semi-autonomous UAV. *Mechanical Systems and Signal Processing*, *138*, 106446.

[8] Bhalaji, N. "Reliable Data Transmission with Heightened Confidentiality and Integrity in IOT Empowered Mobile Networks." *Journal of ISMAC* 2, no. 02 (2020): 106-117.

[9] Sreenath, S., Malik, H., Husnu, N., & Kalaichelavan, K. (2020). Assessment and use of unmanned aerial vehicle for civil structural health monitoring. *Procedia Computer Science*, *170*, 656-663.

[10] Shrestha, Sujan, and Subarna Shakya. "A Comparative Performance Analysis of Fog-Based Smart Surveillance System." Journal of trends in Compu ter Science and Smart technology (TCSST) 2 02 (2020): 78-88

[11] Seo, J., Han, S., Lee, S., & Kim, H. (2015). Computer vision techniques for construction safety and health monitoring. *Advanced Engineering Informatics*, *29*(2), 239-251.

[12] Hamdan, Yasir Babiker. "Smart Home Environment Future Challenges and Issues-A Survey." Journal of Electronics 3, no. 01 (2021): 239-246.

[13] Tziavou, O., Pytharouli, S., & Souter, J. (2018). Unmanned Aerial Vehicle (UAV) based mapping in engineering geological surveys: Considerations for optimum results. *Engineering Geology*, *232*, 12-21.

[14] Shakya, Subarna. "Analysis of Soil Nutrients based on Potential Productivity Tests with Balanced Minerals for Maize-Chickpea Crop." Journal of Electronics 3, no. 01 (2021): 23-35.

[15] Valavanis, K. P., & Vachtsevanos, G. J. (Eds.). (2015). *Handbook of unmanned aerial vehicles* (Vol. 1). Dordrecht: Springer Netherlands.

[16] Shakya, Subarna. "Collaboration of Smart City Services with Appropriate Resource Management and Privacy Protection." Journal of Ubiquitous Computing and Communication Technologies (UCCT) 3, no. 01 (2021): 43-51.

[17] Abdulridha, J., Ampatzidis, Y., Kakarla, S. C., & Roberts, P. (2020). Detection of target spot and bacterial spot diseases in tomato using UAV-based and

ISSN: 2582-1369 (online)
Submitted: 29.04.2021
Revised: 25.05.2021
Accepted: 6.06.2021
Published: 14.06.2021

benchtop-based hyperspectral imaging techniques. *Precision Agriculture*, *21*(5), 955-978.

[18] Chen, Joy Iong Zong, and P. Hengjinda. "Early Prediction of Coronary Artery Disease (CAD) by Machine Learning Method-A Comparative Study." Journal of Artificial Intelligence 3, no. 01 (2021): 17-33.

[19] Rajeswaran, N., Madhu, T., & Joy, B. (2015). Ultra low voltage and low power Static Random Access Memory design using average 6.5 T technique. *Leonardo Electronic Journal of Practices & Technologies*, *14*(27), 138-154.

[20] Suma, V., and Wang Haoxiang. "Optimal Key Handover Management for Enhancing Security in Mobile Network." Journal of trends in Computer Science and Smart technology (TCSST) 2, no. 04 (2020): 181-187.

ISSN: 2582-1369 (online)
Submitted: 29.04.2021
Revised: 25.05.2021
Accepted: 6.06.2021
Published: 14.06.2021