Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2022.024715
Article

Crypto Hash Based Malware Detection in IoMT Framework

R Punithavathi[1], K Venkatachalam[2], Mehedi Masud[3], Mohammed A. AlZain[4] and Mohamed Abouhawwash[5,6,*]

[1]Department of Information Technology, M. Kumarasamy College of Engineering, Karur, 639113, India
[2]Department of Applied Cybernetics, Faculty of Science, University of Hradec Králové, Hradec Králové, 50003, Czech Republic
[3]Department of Computer Science, College of Computers and Information Technology, Taif University, Taif, 21944, Saudi Arabia
[4]Department of Information Technology, College of Computers and Information Technology, Taif University, Taif, 21944, Saudi Arabia
[5]Department of Mathematics, Faculty of Science, Mansoura University, Mansoura, 35516, Egypt
[6]Department of Computational Mathematics, Science, and Engineering (CMSE), Michigan State University, East Lansing, MI, 48824, USA
*Corresponding Author: Mohamed Abouhawwash. Email:abouhaww@msu.edu
Received: 28 October 2021; Accepted: 10 January 2022

Abstract: The challenges in providing e-health services with the help of Internet of Medical Things (IoMT) is done by connecting to the smart medical devices. Through IoMT sensor devices/smart devices, physicians share the sensitive information of the patient. However, protecting the patient health care details from malware attack is necessary in this advanced digital scenario. Therefore, it is needed to implement cryptographic algorithm to enhance security, safety, reliability, preventing details from malware attacks and privacy of medical data. Nowadays blockchain has become a prominent technology for storing medical data securely and transmit through IoMT concept. The issues in the existing research works are in terms of insecurity, non-reliability, remote hijacking, hacking of password and Denial of Service (DoS) attacks. In order to overcome these issues, this work is focused on the double layer encryption model using PoW consensus with Crypto Hash algorithm (PoW-CHA). This proposed work concentrates on secured storage of medical data via IoMT transmission. It ensures transparency, decentralization, security, immutability and preserving privacy, and precisely detecting the malware attack. The accuracy of PoW-CHA is 98% compared to PoW and Crypto Hash algorithm. Moreover, it takes minimum computation time for PoW-CHA.

Keywords: IOMT; malware detection; crypto hash algorithm; health care data; PoW

1 Introduction

The advancement of technology in the digital communication has changed the world faster and easier one. The digital communication through smart health care management data using smart wearable devices is referred as Internet of Medical Things (IoMT). It consists of smart medical related wearable devices

such as oximeter, pacemaker, blood glucose meter, blood pressure devices etc and these devices are associated to IoMT via internet. The transmission of information from smart medical devices using wireless communication like Wi-Fi, Bluetooth allows device to device communication in IoMT environment. In addition to that, the smart wearable devices monitor the health-related data of the patients and send it to servers like fog server, cloud server, etc [1–3].

Due to the rapid development of IoMT, a lot of issues are increasing day by day in terms of preserving sensitive information and providing security. As a result, there are different types of attacks in the IoMT environment through internet. Therefore, it results in various severe problems in monitoring and controlling the smart wearable medical devices. The attacker overtakes the control of smart wearable devices easily and automatically, it affects the communication between machine-to-machine communication [4]. The existing research works are not sufficient for the detection of malware in IoMT. Currently, the type of attacks performed by Bricker Bot botnets, Mirai has created weakness in security, protection in distributed denial-of-service (DDoS) in the field of IoMT environment. Also, it is very essential in providing strong protection and security in the detection and protection of sensitive information from the threatening attacks in IoMT environment [5–7].

In order to overcome these issues and to protect the information from malware attack, this paper has proposed PoW-CHA algorithm. This algorithm is used to protect the sensitive information of the patient and the prescription provided by the doctor in a secured way and to detect the malware attacks as well. In this proposed work, a secret key is generated, and the key is attached with the input data collected from smart wearable devices and stored in fog-based blockchain technology in IoMT environment. The main contributions of this work are:

1. Designed architecture for health care data against malware attack and protect the sensitive information of the patient.
2. Effective evaluation of PoW-CHA is done using performance metric measures in terms of precision, recall, sensitivity, effectiveness and accuracy and statistical measures such as correlation coefficient, mean squared error.
3. The paper has been organized as follows: Section 2 describes the review of literature, Section 3 implements the health care data management against malware detection and prevention, Section 4 discusses the experimental results and Section 5 concludes the paper with future directions.

2 Review of Literature

The Internet of Medical Things (IoMT) represent a system which interconnects more than one node, and each node is interlinked with IoMT wearable devices. Moreover, it produces both response times from the physician and patient by transmitting the prescription and treatment details [8]. As far as IoMT is concerned, the e-health information is transmitted from device-to-device communication through wireless network. The digital transformation monitors the status of patient carefully in e-healthcare management and stores in a protected way [9].

While transmitting the medical data, preserving the security and privacy remains crucial and so many research works have been explored. The primary drawback of existing algorithms depends purely on the deficiency in terms of detection and prevention of malware attack, less secure of data, unreliability, and high computation cost. In order to overcome these issues, the proposed work is scientifically based on PoW consensus algorithm with Crypto Hash algorithm for providing more security and prevents a malicious node in the network. The key advantage of the proposed work is providing double layer protection for the health care data management and monitoring malicious node and prevents it into the proposed system using malicious detection pattern.

In paper [10] the author surveyed carefully on the unique characteristics of block chain such as stability, non-modifiability, decentralization, security etc. Similarly, it uses the consensus algorithm and reviews its performance, characteristics and principles with various consensus algorithms. Hybrid security scheme is applied in the cryptographic techniques like symmetric and used in heterogeneous cryptosystems [11]. In the IoMT environment, the input data are accurately captured from the smart medical devices and instantly work in detecting the organized activities of the malicious node in the block. If it is noticed as malicious node, the IP address of malicious node is sent to the administrator for preventing it [12]. Blockchain based machine learning concepts are typically used for detecting the malware in the wearable IoT devices. This machine learning concepts are used automatically in the identification of malware information and extract it using clustering and classification algorithm. These extract information of malware is efficiently stored in the distributed malware database. Consequently, this will improve the performance of dynamic time detection of malware in an excessive speed [13].

To detect the anomaly detection in an accurate way, the misused detection is identified using Network-based Intrusion Detection System (NIDS). Moreover, the system precisely detects the unwarrantable intrusion through the complex network. Another detection mode based on Host-based Intrusion Detection System (HIDS) is implemented to monitor and detects the intrusion which is occurred inside an operating system [14,15]. Tab. 1. shows the survey of the existing research work.

Table 1: Survey on existing research work

Paper	Method used
[16]	Blockchain using ledger
[17]	Fog-based Blockchain
[18]	Light-weight authentication in IoMT
[19]	Malware analysis and detection using IoT
[20]	Fog based authenticated key management protocol
[21]	Cognitive edge framework of blockchain based IoT.
[22]	Four-layer iot frame perception for remote monitoring and diagnosis.
[23]	Malware detection mechanism for IoT devices
[24]	Malware detection using deep learning
[25]	Malware detection using multimodal deep learning method for android using various features
[26]	Biometrics-based privacy-preserving user authentication scheme for cloud-based environment.
[27]	Internet of medical things dealing with cyber-physical systems in medicine
[28]	Privacy-aware efficient fine-grained data access control in internet of medical things based fog computing
[29]	Cyber security problems are discussed using machine learning algorithms.

3 PoW-CHA Methodology in the Malware Protection

This paper proposes a proper protection of health care data from malware attacks in blockchain [30,31]. Typically, it consists of intelligent healthcare and monitoring tools such as smart watch, smart blood glucose meter, smart pacemaker, smart oximeter, etc. is shown in Tab. 2. The signals collected from these sensitive devices are stored securely in the fog server using PoW consensus and Crypto Hash algorithms. The smart

medical devices are properly equipped with wireless network communications namely, Bluetooth and Wi-Fi. Fig. 1. shows the model of the proposed algorithm (PoW-CHA).

Table 2: Simulation parameters

Parameter	Value
No. of. cloud service providers	32
No. of patients	155
Transactions of the data	1005 per round
Area of the simulation	500 m × 500 m
No. of IoMT devices	107050540
Response time	2–5 s
Simulation time	100 s

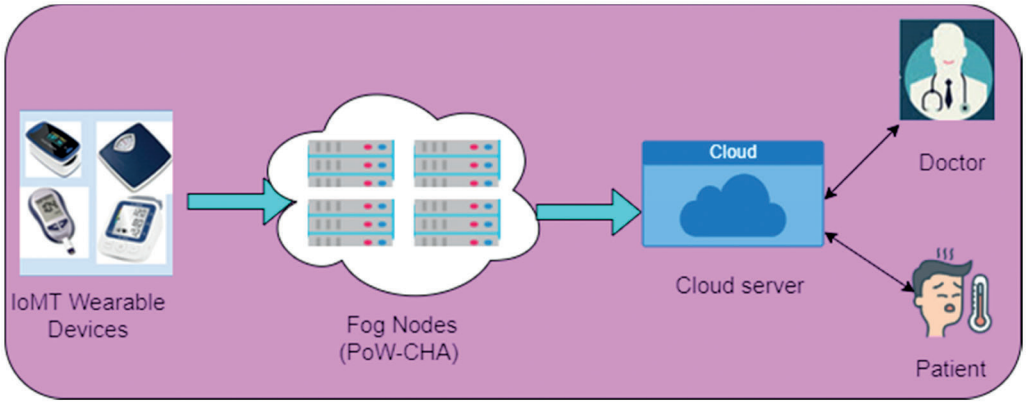

Figure 1: Model of PoW-CHA

3.1 Wearable Devices in IoMT Layer

To adequately monitor the health status of the patient, smart wearable devices are used in the IoMT layer. Smart wearable devices generate signals, and it is transmitted to centralized fog server in the blockchain network through radio frequency with the help of IoMT. In the centralized fog server, it is securely stored.

3.2 Categories of Malware

Malware is software that transmits over a complex network. Normally, it performs some malicious operation, and gently steals the sensitive stored information which is undoubtedly required by the potential attacker. Types of malwares are given below.

Spyware: This specific type of malware will perform spying activities of the user without their extensive knowledge. The activities of spyware such as, monitoring keystrokes, modify the settings of the software and it acts as a traditional program.

Key logger: To track the keystrokes of the user, the key logger is used by the hacker. It is, moreover, a small segment of code. It is really an energetic attacker which tries to enter the system of the user through the link in the email and the system is trickily hacked. By allocating a strong password, the system can be secured. In such case, a multifactor authentication is critically needed.

Virus: The malicious program is attached with numerous programs and spread into other systems. While executing the program, it will automatically infect the programs. In addition to that, it can be used to steal sensitive information that harms the system.

Trojan Horse: This malware supports the hacker to obtain authorization for accessing the infected system, and it can steal the sensitive information from the infected system.

Worm: To identify the weaknesses in the OS, it tries to spread through a network and harms the host through consumption of bandwidth and webservers. This malware spreads through e-mail which contains infected attachments and steal the sensitive information to get rid of the files.

Rootkit: As it is remotely an accessible malicious file, this kit can hack the system remotely without the consent of the user and steal the sensitive information and modify the configuration of the system. Detection and prevention of this malware are difficult because it always conceals itself.

Ransomware: This type of malware restricts the user to access the machine by requesting money. Additionally, it encrypts the file and blocks the system. At that time, the message will be displayed and invite the user to pay the money forcefully. Once the money is received, the key is provided to decrypt the file. the process spreads through the downloaded file to the system.

3.3 Proposed Prevention of Malware Attack in Fog Nodes Using PoW-CHA

To prevent the malware attack in the IoMT environment, the data collected from the sensor devices are securely stored in the fog-based cloud server network. This paper proposes double layer encryption model using PoW consensus with efficient Crypto Hash algorithm (PoW-CHA). Similarly, it detects and prevents the malware in the blockchain network.

3.3.1 Generation and Exchange of Key

For transmitting the information from IoMT device to Fog-based cloud server network, it is required to have a secret key. This secret key contains the input signals received from various IoMT wearable devices along with Hash function of 256 bits. When IoMT device starts transmitting the data, a secret key is assigned. After exchanging of the key process is over, it starts the transmission in a secured way.

3.3.2 Authentication of User and IoMT Device

It is a process of identifying and verifying the specific details of the user and IoMT wearable devices are attached in the proposed system. There are five phases; They are registration phase, login phase, password phase, authentication, and generation of key phases, adding of IoMT wearable device phase.

3.3.3 Registration Phase

In the registration phase, a user (patient) can provide their valuable information such as name, patient details, IoMT wearable device details, password and store it in a protected way and submit it to the Certificate Authority (CA). After completing this standard procedure successfully, CA will provide a smart card to the user and register in a secured manner.

3.3.4 Login Phase

The registered user information for a specific IoMT device check whether the user data is valid or not by sending login request. If it is successfully logged in, only then it allows the user to access the data in the blockchain.

3.3.5 Password Updating Phase

For enhancing the high dimensionality of security, it is necessary to provide strong password. Therefore, for the purpose of authentication instantly updating the secure password is done very often. It typically prevents the system from malware attacks.

3.3.6 Authentication and Generation of Key Phase

After verifying the login credentials with password user (sender), the information is transmitted to the authorized receiver. While transmitting the information, a secret key is generated using crypto hash algorithm. This secret key is attached with the input data that forms a message. This message transmits in a secured way. That is from IoMT wearable devices to Fog-based cloud server. When a new IoMT device is installed for a new patient in the environment, it must be authenticated. Then it gives assurance and starts accessing the data or transmit the same. Exchanging information between doctor and patient and vice versa in a safer way. For exchanging the information, they shared the secret key.

3.4 Detection of Malware

The Malware Detection System (MDS) is used for monitoring and analyses of malicious activities inside the proposed system. It detects and prevents the malware attacks to the system. In case of any malicious activities, it sends the message to Certificate Authority (CA) to block that particular IP address or raise an alarm signal. Therefore, a secured way is needed for preventing the malware activities. This work has proposed PoW consensus with Crypto Hash algorithm (PoW-CHA). The architecture of PoW-CHA is given in Fig. 2.

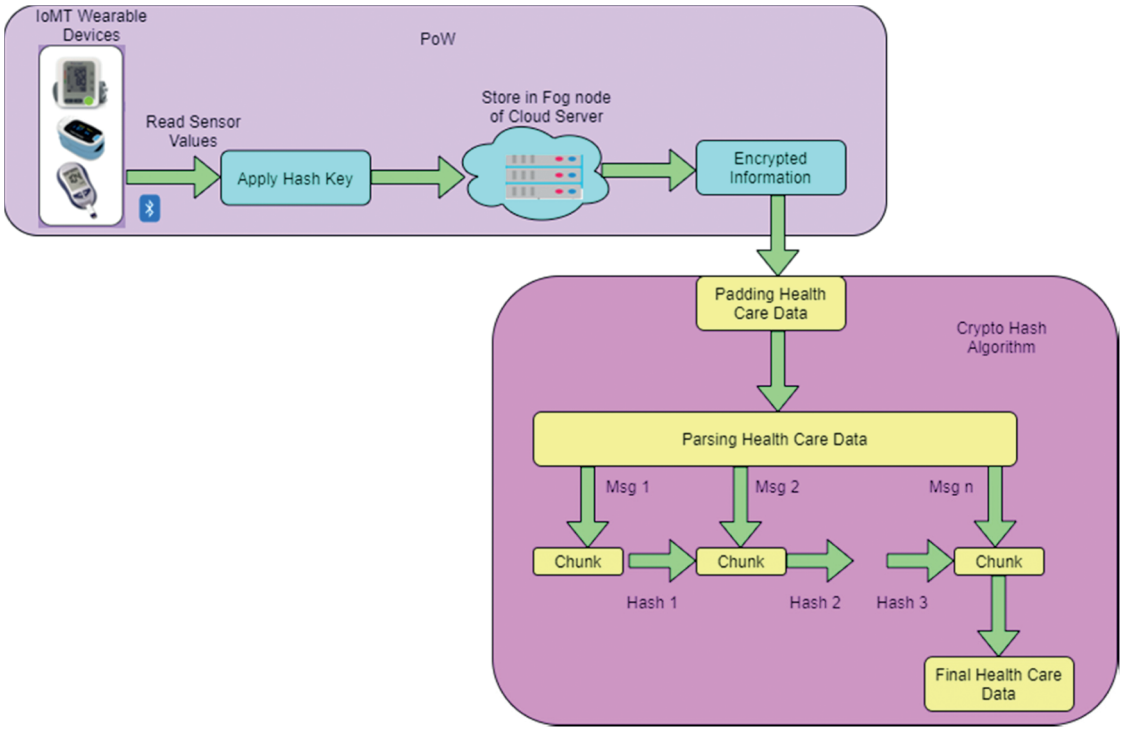

Figure 2: Architecture of PoW-CHA

These protocols provide security in IoMT in Fig. 2. It provides more security to the health care data in the blockchain network and prevents the attack from malwares. This paper describes the CHA as permission blockchain for providing security and preventing malware attacks.

Algorithm 1: PoW-CHA in Health Care Data Management Fog Based Cloud Server

Step 1: While $p_i$in $FBC(patient)$**do** // p_i **-** Patient

Step 2: Select p_i

Step 3: IF $p_i \in FBC(p_{list})$

Step 4: For each$FBC(Health-data_i)$ in *IoMT* **do**

Step 5: If$device_i$ select $FBC(Health-data_i)$ then

Step 6: Retrieve $FBC\ (p_i\ , FBC(Health-data_i))$

Step 7: Store in FBC − PoW(fog_FBC)

Step 8: global public key values (p, q, m) **//Generate hash Key**

Step 9: Choose largest prime number (p) in 160-bit number

Step 10: Evaluate $m = p * q$

Step 11: Evaluate $\varnothing(m) = (p-1) * (q-1)$

Step 12: Choose public key as e

Step 13: $gcd(\varnothing(m),\ e) = 1;\ 1 < e < \varnothing(m)$

Step 14: $d = e^{-1} mod\ \varnothing(m)$ // d is a private key; public key is e, n

Step 15: $array[char] \leftarrow$ FBC − PoW$(fog_FBC,\ d,\ e)$ // Select the Stored data split into array form as ASCII format.

Step 16: $bin \leftarrow array[char]$ //Converts array of codes to binary.

Step 17: convert b *in* value in 8-bits long by adding zeros in front of each bit //Padding

Step 18: $Pad\ (bin) \leftarrow$bin //

Step 19: $health-data_{patient} \leftarrow Pad(bin) + Message(M)$

Step 20: Break the message $health-data_{patient}$ into chunks with 512 characters.

Step 21: Break the message $health-data_{patient}$ into chunks with subarray of sixteen 32-bit words.

Step 22: $PoW-Cha \leftarrow health-data_{patient} + (d,\ e)$//

Step 23: Else

Step 24: Display "Unauthorized User"

Step 25: End If; End If; End For; End

The working flow of Algorithm 1 is given in Fig. 3.

4 Result and Discussions

This section performs an analysis of protection in the health care data from the malware attack in Fog-based cloud server network in IoMT and the performance metric measures of PoW-CHA are given below:

If ordinary program is treated as ordinary program by Malware Detection System (MDS), it is termed as "True Negative" (TN). Similarly, if ordinary program is treated as malicious program by MDS, it is called as False Positive (FP). If a malicious program is treated as a malicious program by MDS, it is termed as "True Positive (TP)". If a malicious program is treated as an ordinary program by MDS, it is called as "False Negative (FN)". The simulation parameters used in the proposed systems are provided below.

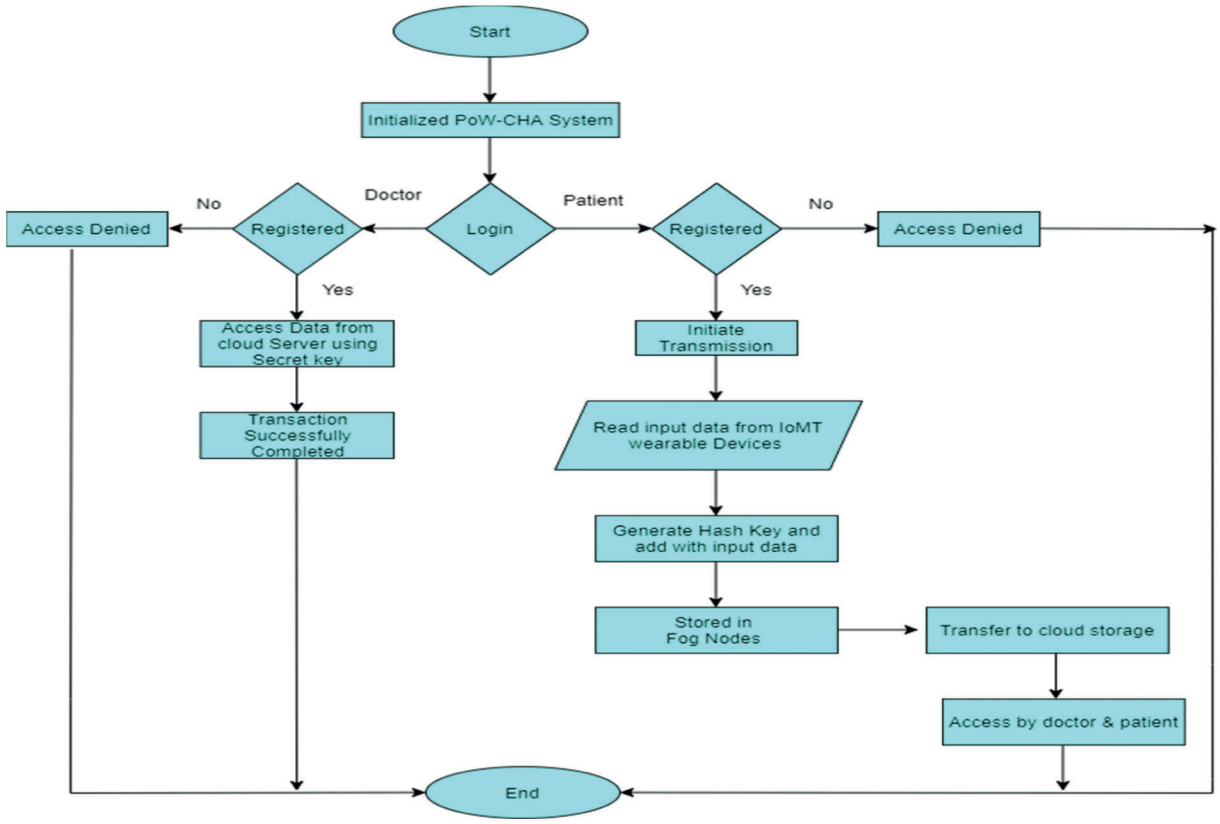

Figure 3: Workflow of PoW-CHA

4.1 Accuracy

It is used to measure all correctly identified cases.

$$accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{1}$$

4.2 Precision (PPV)

It is also called as positive predicted value. It is identified as intrusion cases correctly for all intrusion cases of predicted positive cases.

$$precision = \frac{TP}{TP + FP} \tag{2}$$

4.3 Recall

It is also called as detection rate or true positive rate. It is identified as intrusion cases correctly for all intrusion cases of real positive cases.

$$recall = \frac{TP}{TP + FN} \tag{3}$$

4.4 F1-score

This F1-measure can be used to compute the harmonic mean of "precision" and "recall.

$$F1 - Score = \frac{2 * precision * recall}{precision + recall} \tag{4}$$

From Tab. 3, it is clear that the precision rate PoW-CHA algorithm (96.2%) is better than PoW (75.6%) and Crypto Hash (89.4%). PoW-CHA outperforms the other algorithms with precision of 96.2%. For the recall value of the proposed work, PoW-CHA has better percentage of 80.3% in PoW and 85.2% in Crypto Hash. The PoW-CHA algorithm outperforms the other algorithms with an F-score of 99.10%. Fig. 4. shows the accuracy of PoW-CHA.

Table 3: PoW-CHA algorithm's performance metric measures

Algorithm	Precision	Recall	F1-score
PoW [20]	75.6%	80.3%	73.1%
Crypto hash [28]	89.4%	85.2%	83.2%
PoW-CHA (proposed)	96.2%	98.6%	99.10%

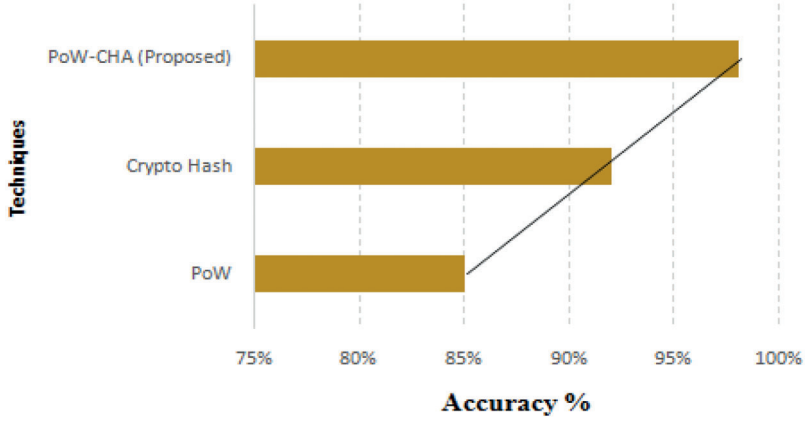

Figure 4: Accuracy

4.5 Throughput

In this performance parameter, it is the rate at which valid transactions of IoMT medical data are committed by the blockchain.

$$transaction\ per\ Node = (node\ size)/(average\ transaction\ size) \tag{5}$$

$$fraction\ of\ \ node\ per\ second = 1/(node\ time\ in\ seconds) \tag{6}$$

$$transaction\ per\ node = transcation\ per\ node * fraction\ of\ \ node\ per\ second \tag{7}$$

This throughput parameter is compared with fog-based in IoMT, and PoW-CHA. Fig. 5. shows the throughput.

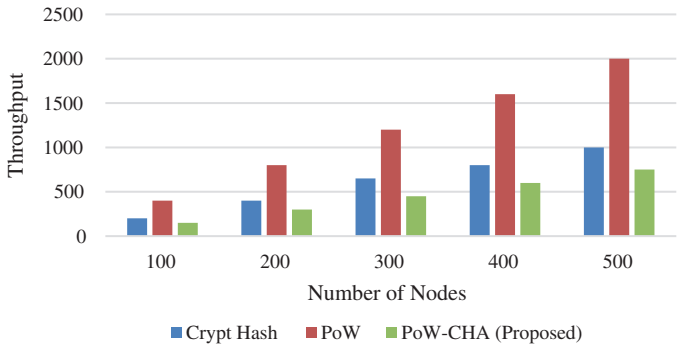

Figure 5: Throughput

Fig. 5. shows the number of nodes that increases the proposed work to execute more nodes in minimum time requirement. Tab. 4. shows the comparison of the proposed work with the existing techniques in malware detection.

Table 4: Comparison of existing algorithm

Author name	Method	Accuracy	F1-score
T. Lei et al. [32]	EveDroid	Not applicable	99.00%
S. M. PudukotaiDinakarrao et al. [33]	Malware detector of HaRM	92.21%	Not Applicable
H. Nguyen et al. [34]	CNN (Graph based)	92.00%	94.00%
J. Su et al [35]	CNN	94.00%	Not Applicable
Our proposed work	PoW-Crypto hash algorithm	98.00%	99.10%

Tab. 4. shows that the proposed work has provided better performance in the aspects of accuracy and F1-score values when it is compared with the existing algorithm for malware detection of fog-based network [36–51]. Tab. 5. shows the consumption of energy in terms of different architectures.

Table 5: Different nodes in the cloud server and its consumption of energy

	Consumption of energy (W)		
Number of nodes in the fog-based network	PoW	Crypto hash (CHA)	PoW-CHA
1 Node	5.1	4.5	2.3
2 Nodes	6.5	5.75	4.6
4 Nodes	10	8.5	6.5
More than 10 nodes	15	12	9.75

From Tab. 5, it is observed that the proposed work PW-CHA is implemented in Raspberry Pi 3-based platform. If number of nodes increases in the Raspberry Pi 3 platform, it needs more time and high energy consumption. The proposed work produces minimum consumption of energy when nodes get increased. Consequently, it gives the prominent result. Tab. 6. shows the number of malicious nodes in the fog-based network.

Table 6: Detecting malicious nodes using PoW-CHA

Nodes in fog based network	Malicious nodes in fog	Malicious miners (Storage) in cloud
200	20	50
400	40	100
600	80	150

From the Tab. 6, it is understood that in the detection of malicious operations network, PoW-CHA is used in the Fog-based cloud server technology. While adding nodes in the network, the proposed PoW-CHA analysis identifies the malicious activities using Algorithm 1 and segregates the malicious nodes (20, 40, 80) as well as malicious miners. In the health care management system, whenever a physician gives a treatment detail to a patient and at the same time, it is sent to each miner in the network. In the network data generated from the wearable devices along with prescription and treatment details of the patient are authenticated and then only included in the network. Fig. 6. shows the average latency of the proposed algorithm with the existing algorithm.

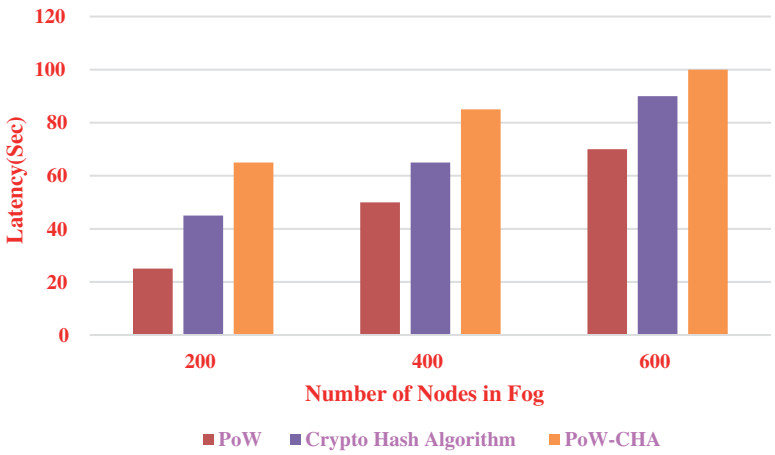

Figure 6: Average latency

The transmission of data with malicious node in the fog and miners in the cloud server has been implemented using PoW-CHA. Fig. 6. shows the proposed algorithm PoW-CHA that produces high average latency. When malicious operation occurs in the network, PoW-CHA algorithm detect and prevent the malicious node and retransmit the authenticated data to the next fog node. The proposed work PoW-CHA is accessed by statistical index values of:

Mean Square Error (MSE)

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(m-p)^2 \tag{8}$$

Correlation of Coefficient (CC)

$$CC = \frac{\sum_{i=1}^{n}(m-\bar{m})(p-p)}{\sqrt{\sum_{i=1}^{n}(m-\bar{m})^2 \sum_{i=1}^{n}(m-p)^2}} \tag{9}$$

Figs. 7 and 8 show the comparison of Mean Squared Error value and Correlation coefficient value and with our proposed work PoW-CHA.

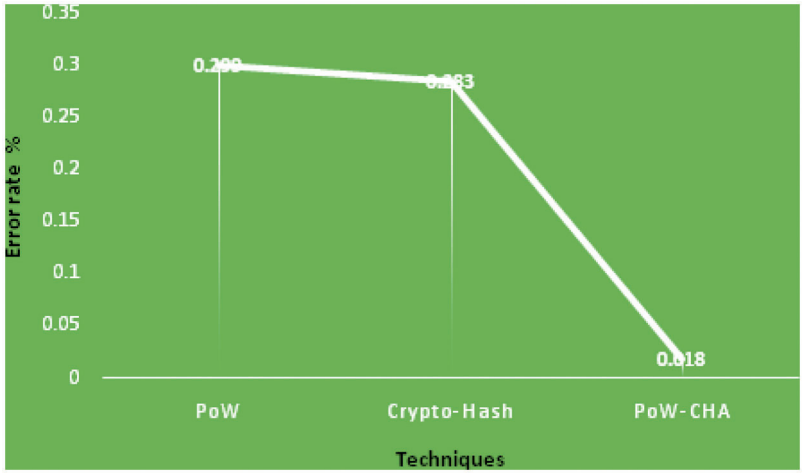

Figure 7: Mean squared error

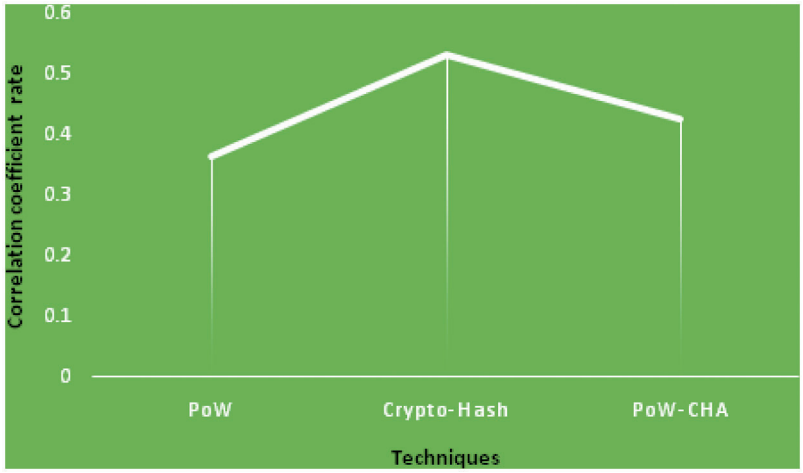

Figure 8: Correlation coefficient

Hence, from various performance metric measures, it is shown that our proposed KNN-MLSC has high classification accuracy, minimum error, and reduced computational complexity.

Fig. 8 calculates the correlation coefficient of the proposed work PoW-CHA that outperforms compared to the existing algorithm. Fig. 9. shows the computation time of the proposed work.

Fig. 9. shows the computation time of the proposed study which takes minimum time. Therefore, it produces minimum execution time and minimum error rate.

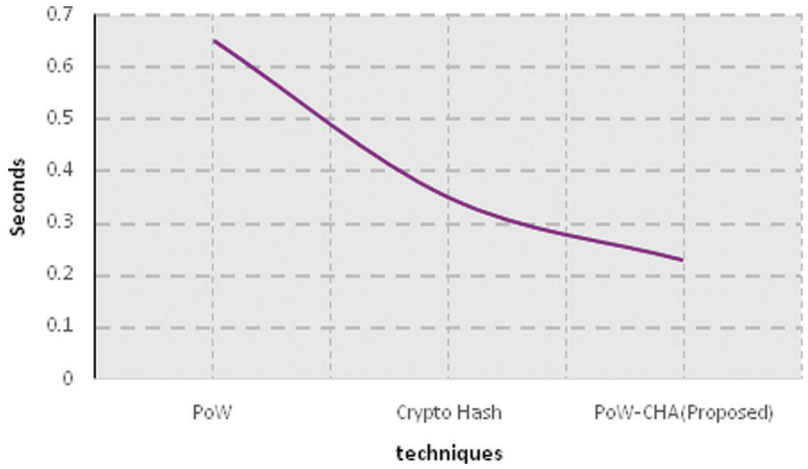

Figure 9: Computation time

5 Conclusion

IoMT based applications have become important in our routine life. Protection of health care data from malware attack in fog based IoMT remains a difficult task. However, in accessing the data in a secured way from malware attack remains a major issue. To overcome these issues and to implement an effective and efficient way in the detection and prevention of malware attack using the proposed work of PoW-CHA algorithm. In this work, the authenticated data are stored in the fog-based cloud server and subsequently, the dynamic attacks of malware are monitored in the IoMT environment. The accuracy of PoW-CHA is 98% compared to PoW and Crypto Hash algorithm. It takes minimum computation time for PoW-CHA. Future work can be extended to the detection of malware using various meta heuristics algorithms with the help of IoMT wearable devices in edge computing.

Acknowledgement: We would like to give special thanks to Taif University Research supporting Project Number (TURSP-2020/98), Taif University, Taif, Saudi Arabia.

Funding Statement: Taif University Researchers Supporting Project number (TURSP-2020/98), Taif University, Taif, Saudi Arabia.

Conflicts of Interest: The authors declare that there is no conflict of interests regarding the publication of the paper.

References

[1] A. M. Gatouillat, Y. Badr, B. Massot and E. Sejdic, "Internet of medical things: A review of recent contributions dealing with cyber-physical systems in medicine," *IEEE Internet of Things*, vol. 5, no. 5, pp. 3810–3822, 2018.

[2] X. Wang, L. Wang, Y. Li and K. Gai, "Privacy aware efficient fine grained data access control in internet of medical things based fog computing," *IEEE Access*, vol. 6, no. 4, pp. 657–665, 2018.

[3] V. P. Yanambaka, S. P. Mohanty, E. Kougianos and D. Puthal, "Pmsec: Physical unclonable function-based robust and lightweight authenticationin the internet of medical things," *IEEE Transactions on Consumer Electronics*, vol. 65, no. 3, pp. 388–397, 2019.

[4] M. Wazid, D. Ashok Kumar, J. P. Joel and S. Youngho, "IoMT malware detection approaches: Analysis and research challenges," *IEEE*," *Access*, vol. 7, no. 4, pp. 182459–182476, 2019.

[5] Z. Liu, L. Zhang, Q. Ni, J. Chen, R. Wang *et al.,* "An integrated architecture for IoT malware analysis and detection," in *Proc. Int. Conf. on Internet of Things as a Service*, Patna, India, pp. 127–137, 2019.

[6] J. Su, D. V. Vasconcellos, S. Prasad, D. Sgandurra, Y. Feng *et al.,* "Light weight classification of IoT malware based on image recognition," in *Proc. IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*, Tokyo, Japan, vol. 2, pp. 664–669, 2018.

[7] V. Clincy and H. Shahriar, "IoT malware analysis," in *Proc. IEEE 43rd Annual Computer Software and Applications Conf. (COMPSAC)*, Milwaukee, USA, vol. 1, pp. 920–921, 2019.

[8] O. Bonsu, A. Stein and M. Boswell, "The current ethical and regulatory status of the internet of medical things and the need of a new IoMT Law," *The Journal of Health Care Ethics & Administration*, vol. 4, no. 2, pp. 12–25, 2018.

[9] S. Smagulov and V. Smagulova, "Challenges of digital transformation in health care," *Intellectual Archive*, vol. 8, no. 1, pp. 12–32, 2019.

[10] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei and C. Qijun, "A review on consensus algorithm of blockchain," in *Proc. IEEE Int. Conf. on Systems, Man, and Cybernetics (SMC)*, Melbourne, Australia, pp. 2567–2572, 2017.

[11] C. S. Jang, D. G. Lee, J. W. Han and J. H. Park, "Hybrid security protocol for wireless body area networks," *Wireless Communication. Mobile Computation*, vol. 11, no. 2, pp. 277–288, 2011.

[12] T. S. Messerges, E. A. Dabbish and R. H. Sloan, "Examining smart card security under the threat of power analysis attacks," *IEEE Transactions on Computers*, vol. 51, no. 5, pp. 541–552, 2002.

[13] R. Kumar, X. Zhang, W. Wang, R. U. Khan, J. Kumar *et al.,* "A multi modal malware detection technique for android IoT devices using various features," *IEEE Access*, vol. 7, no. 5, pp. 64411–64430, 2019.

[14] V. Bhuse and A. Gupta, "Anomaly intrusion detection in wireless sensor networks," *Journal of High-Speed Networks*, vol. 15, no. 1, pp. 33–51, 2006.

[15] I. Butun, S. D. Morgera and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks," *Journal of High Speed Networks*, vol. 16, no. 1, pp. 266–282, 2014.

[16] D. Pavithran, K. Shaalan, J. N. Alkaraki and A. Gawanmeh, "Towards building a blockchain framework for IoT," *Cluster Computing*, vol. 12, no. 2, pp. 1–15, 2020.

[17] P. Singh, A. Nayyar, A. Kaur and U. Ghosh, "Blockchain and fog based architecture for internet of everything in smart cities," *Future Internet*, vol. 12, no. 61, pp. 1–24, 2020.

[18] T. K. Mackey, T. T. Kuo, B. Gummadi, K. A. Clauson, G. Church *et al.,* "Fit-for-purpose? Challenges and opportunities for applications of blockchain technology in the future of healthcare," *BMC Medicine*, vol. 17, no. 1, pp. 1–17, 2019.

[19] Z. Liu, L. Zhang, Q. Ni, J. Chen, R. Wang *et al.,* "An integrated architecture for IoT malware analysis and detection," in *Proc. Int. Conf. on Internet of Things as a Service*, Xian, China, pp. 127–137, 2019.

[20] M. Wazid, P. Bagga, A. K. Das, S. Shetty, J. J. P. C. Rodrigues *et al.,* "AKM-IoV: Authenticated key management protocol in fog computing based internet of vehicles deployment," *IEEE Internet of Things*, vol. 6, no. 5, pp. 8804–8817, 2019.

[21] M. A. Rahman, M. M. Rashid, M. S. Hossain, E. Hassanain, M. F. Alhamid *et al.,* "Blockchain and IoT-based cognitive edge framework for sharing economy services in a smart city," *IEEE Access*, vol. 7, pp. 18611–18621, 2019.

[22] J. Li, Y. Liu, J. Xie, M. Li, M. Sun *et al.,* "A remote monitoring and diagnosis method based on four-layer IoT frame perception," *IEEE Access*, vol. 7, pp. 144324–144338, 2019.

[23] H. Takase, R. Kobayashi, M. Kato and R. Ohmura, "A prototype implementation and evaluation of the malware detection mechanism for IoT devices using the processor information," *International Journal of Information Security*, vol. 19, no. 1, pp. 71–81, 2019.

[24] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran and S. Venkatraman, "Robust intelligent malware detection using deep learning," *IEEE Access*, vol. 7, no. 2, pp. 46717–46738, 2019.

[25] T. Kim, B. Kang, M. Rho, S. Sezer and E. G. Im, "A multimodal deep learning method for android malware detection using various features," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 3, pp. 773–788, 2019.

[26] A. K. Das, M. Wazid, N. Kumar, A. V. Vasilakos and J. J. P. C. Rodrigues, "Bio metrics based privacy preserving user authentication scheme for cloud- based industrial internet of things deployment," *IEEE Internet of Things*, vol. 5, no. 6, pp. 4900–4913, 2018.

[27] A. Gatouillat, Y. Badr, B. Massot and E. Sejdic, "Internet of medical things: A review of recent contributions dealing with cyber-physical systems in medicine," *IEEE Internet of Things*, vol. 5, no. 5, pp. 3810–3822, 2018.

[28] X. Wang, L. Wang, Y. Li and K. Gai, "Privacy aware efficient fine-grained data access control in internet of medical things based fog computing," *IEEE Access*, vol. 6, pp. 47657–47665, 2018.

[29] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, S. Chen *et al.,* "Performance comparison and current challenges of using machine learning techniques in cyber security," *Energies*, vol. 13, no. 10, pp. 2509, 2020.

[30] M. V. Kumar, K. Venkatachalam, P. Prabu, A. Almutairi and M. Abouhawwash, "Secure biometric authentication with de-duplication on distributed cloud storage," *PeerJ Computer Science*, vol. 7, no. 3, pp. e569, 2021.

[31] M. Abdel Basset, N. Moustafa, R. Mohamed, M. Osama and M. Abouhawwash, "Multi-objective task scheduling approach for fog computing," *IEEE Access*, vol. 9, pp. 126988–127009, 2021.

[32] T. Lei, Z. Qin, Z. Wang, Q. Li and D. Ye, "Eve droid: Event aware android malware detection against model degrading for IoT devices," *IEEE Internet of Things*, vol. 6, no. 4, pp. 6668–6680, 2019.

[33] S. M. Pudukotai, H. Sayadi, H. M. Makrani, C. Nowzari, S. Rafatirad *et al.,* "Lightweight node-level malware detection and network-level malware confinement in IoT networks," in *Proc. Design, Automation Test in Europe Conf. Exhibition (DATE)*, Antwerp, Belgium, pp. 776–781, 2019.

[34] H. Nguyen, Q. Ngo and V. Le, "IoT Bot-net detection approach based on PSI graph and DGCNN classifier," in *Proc. IEEE Int. Conf. on Information Communication and Signal Processing (ICICSP)*, Singapore, pp. 118–122, 2018.

[35] T. M. Alam, K. Shaukat, A. Ibrahim, H. S. Luo, M. Sarwar *et al.,* "An investigation of credit card default prediction in the imbalanced datasets," *IEEE Access*, vol. 8, pp. 201173–201198, 2020.

[36] M. Abouhawwash and A. Alessio, "Develop a multi-objective evolutionary algorithm for pet image reconstruction: Concept," *IEEE Transactions on Medical Imaging*, vol. 40, no. 8, pp. 2142–2151, 2021.

[37] M. Abouhawwash, "Hybrid evolutionary multi-objective optimization algorithm for helping multi-criterion decision makers," *International Journal of Management Science and Engineering Management*, vol. 16, no. 2, pp. 94–106, 2021.

[38] M. Abdel-Basset, R. Mohamed, M. Abouhawwash, R. K. Chakrabortty and M. J. Ryan, "EA-MSCA: An effective energy-aware multi-objective modified sine-cosine algorithm for real-time task scheduling in multiprocessor systems: Methods and analysis," *Expert Systems with Applications*, vol. 173, no. 4, pp. 114699, 2021.

[39] M. Masud, G. Gaba, K. Choudhary, M. Hossain, M. Alhamid *et al.,* "Lightweight and anonymity-preserving user authentication scheme for IoT-based healthcare," *IEEE Internet of Things Journal*, vol. 24, no. 2, pp. 1–12, 2021.

[40] A. Ali, H. A. Rahim, J. Ali, M. F. Pasha, M. Masud *et al.,* "A novel secure blockchain framework for accessing electronic health records using multiple certificate authority," *Applied Sciences*, vol. 11, no. 21, pp. 1–14, 2021.

[41] M. Abouhawwash, K. Deb and A. Alessio, "Exploration of multi-objective optimization with genetic algorithms for PET image reconstruction," *Journal of Nuclear Medicine*, vol. 61, no. 3, pp. 572–572, 2020.

[42] M. Masud, G. S. Gaba, K. Choudhary, R. Alroobaea and M. S. Hossain, "A robust and lightweight secure access scheme for cloud-based e-healthcare services," *Peer-to-peer Networking and Applications*, vol. 14, no. 3, pp. 3043–3057, 2021.

[43] M. Masud, G. Gaba, S. Alqahtani, G. Muhammad, B. Gupta *et al.,* "A lightweight and robust secure key establishment protocol for internet of medical things in COVID-19 patients care," *IEEE Internet of Things Journal*, vol. 8, no. 21, pp. 15694–15703, 2021.

[44] S. Ibrahim, H. Alhumyani, M. Masud, S. S. Alshamrani, O. Cheikhrouhou *et al.,* "Framework for efficient medical image encryption using dynamic S-boxes and chaotic maps," *IEEE Access*, vol. 8, no. 13, pp. 160433–160449, 2020.

[45] M. Rawashdeh, M. Zamil, S. M. Samarah, M. Obaidat and M. Masud, "IOT-Based service migration for connected communities," *Computers & Electrical Engineering*, vol. 96, no. 2, pp. 1–10, 2021.

[46] M. Abouhawwash and K. Deb, "Karush-kuhn-tucker proximity measure for multi-objective optimization based on numerical gradients," in *Proc. of the 2016 on Genetic and Evolutionary Computation Conf. Companion*, Denver, USA, pp. 525–532, 2016.

[47] Y. Wang, J. Ma, A. Sharma, P. K. Singh, G. Singh *et al.,* "An exhaustive research on the application of intrusion detection technology in computer network security in sensor networks," *Journal of Sensors*, vol. 2021, no. 3, pp. 1–11, 2021.

[48] M. Masud, M. Alazab, K. Choudhary and G. S. Gaba, "3P-SAKE: Privacy-preserving and physically secured authenticated key establishment protocol for wireless industrial networks," *Computer Communications*, vol. 175, no. 4, pp. 82–90, 2021.

[49] M. Abdel-Basset, R. Mohamed, M. Abouhawwash, R. K. Chakrabortty and M. J. Ryan, "A simple and effective approach for tackling the permutation flow shop scheduling problem," *Mathematics*, vol. 9, no. 3, pp. 270–282, 2021.

[50] P. Singh, M. Masud, M. S. Hossain and A. Kaur, "Cross-domain secure data sharing using blockchain for industrial IoT," *Journal of Parallel and Distributed Computing*, vol. 156, no. 3, pp. 176–184, 2021.

[51] S. M. M. Rahman, M. Masud, M. A. Hossain, A. Alelaiwi, M. M. Hassan *et al.,* "Privacy preserving secure data exchange in mobile P2P cloud healthcare environment," *Peer-to-Peer Networking and Applications*, vol. 9, no. 5, pp. 894–909, 2016.