International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

An Intelligent Healthcare Framework for Data Security Based on Blockchain and Internet of Things

[1]Sharda Tiwari, [2]Dr. Namrata Dhanda and [3]Dr. Harsh Dev
[1,2]Department of Computer Science & Engineering, Amity University, Lucknow, Uttar Pradesh
[3]Department of Computer Science & Engineering, Pranveer Singh Institute of Technology, Kanpur
[1]sharda26tiwari@yahoo.com, [2]ndhanda@lko.amity.edu, [3]drharshdev@gmail.com

Submitted: 22/07/2022 **Accepted**: 25/09/2022

Abstract: A blockchain network offers flexible and trustworthy solutions for the storage of sensitive data like patient's medical records. Nowadays IoT devices are used to connect and transmit sensed information between object and human using internet. IoT has major applications in almost all the sectors like smart transportation, cities, and healthcare etc. In healthcare sector a doctor can monitor the patient parameters remotely in case of any emergency. The wearable IoT device is continuously sense the patient parameters and export the data over cloud or any storage unit. The accurate previous data and real time sensed data must be shared with doctor immediately during an emergency. In this paper the aim is to improves the functionality of healthcare system by integrating IoT system with blockchain network which is used to store all the sensed data by IoT devices.

Keywords: *Blockchain, Encryption, IoT, Health, Security,*

1. Introduction

The Internet of Things (IoT) is comprised of resource-constrained devices connected to the internet and interacting with other networks with or without direct human intervention. The IoT's primary objective is to maintain operations regardless of location to provide seamless interaction between users and "things" to transfer and/or retrieve data and respond with intelligent actions. The last few years, the performance, and capabilities of IoT devices have improved, nevertheless, the security of IoT devices has not kept the pace and it remains as the main challenge to address [1]. In October 2016, the major internet service provider Dyn suffered a major Denial-of-Service (DoS) attack by an army of compromised IoT machines, which has increased the urgency to deal with ill-protected IoT devices [2]. Forbes (2016) believed that by 2020, the Internet of Things would exchange over 40 Zettabytes of data as over 20 billion devices interact over the internet [3], increasing the risk spectrum significantly for the IoT. A main property for IoT devices is to be ubiquitous, which entails requirements for power efficiency as well as limited computing capabilities that do not drain the power of the device. Such intrinsic properties are found to contradict cryptography-based applications and other securing algorithms, making the IoT security environment even more challenging [4]. Nevertheless, security researchers have paid attention to new technologies that could help to cope with the current computing, energy, and security necessities of the IoT. The blockchain and its cryptocurrency applications have disrupted the Internet environment over the last few years, providing a new way to securely transact digital assets by combining reliable cryptographic principles and secure protocols. The IoT security community has been trying to use the
blockchain's strengths to make embedded devices less prone to cyberattacks. In a blockchain network each block store hash of previous block making it more secure.

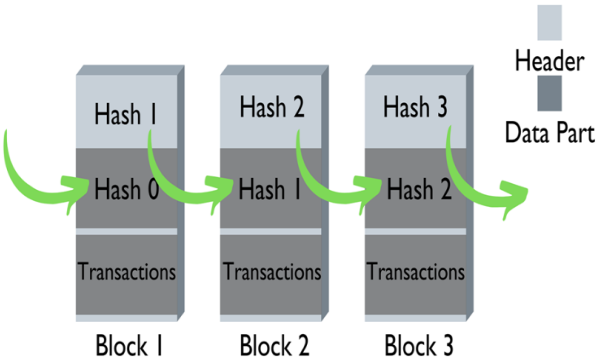

Figure 1: Blockchain Hash Structure

The purpose of this work was to present an application of the blockchain protocol to protect networks at different levels and, therefore, the IoT devices in it [5]. Also, this document introduced a security framework that uses the blockchain to share security intelligence, gathered directly from cyber targets, that within all network stakeholders.

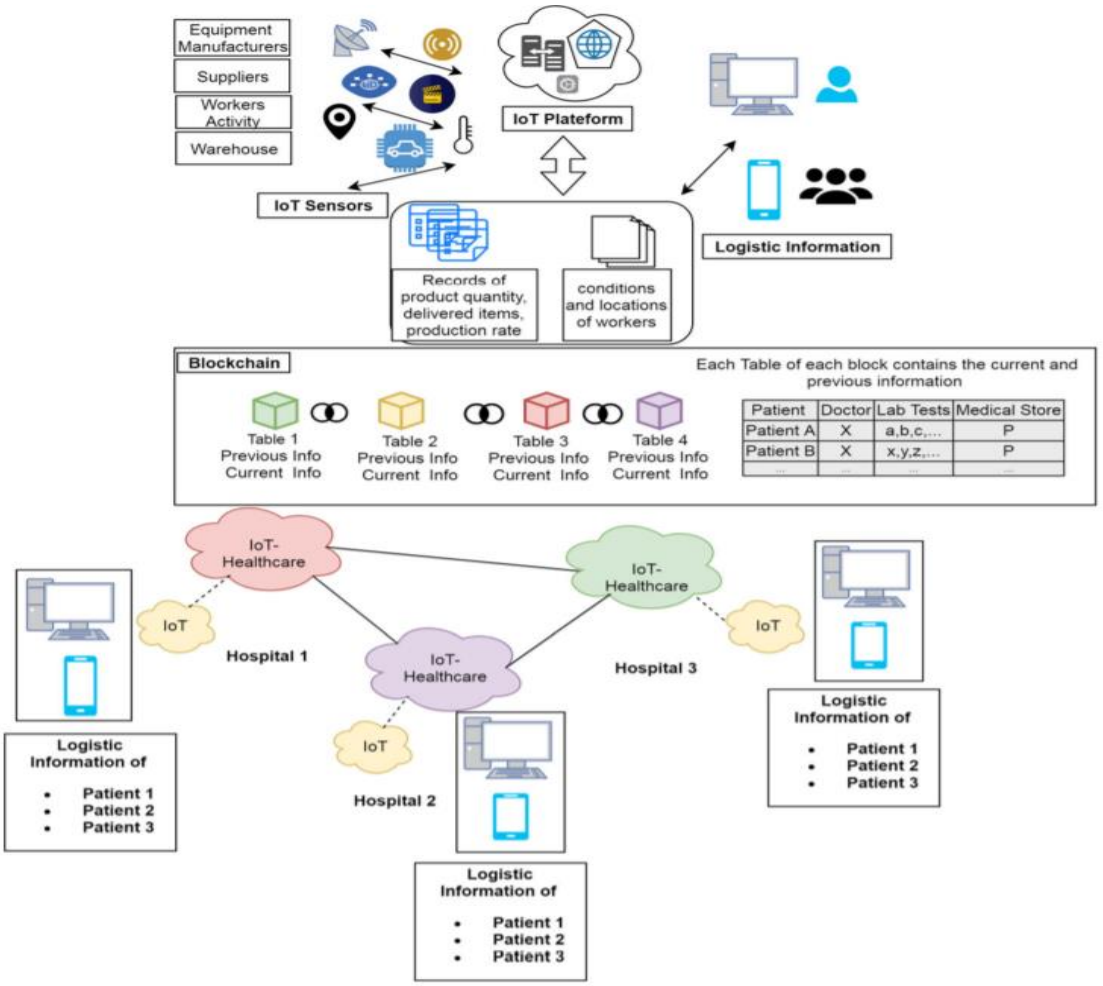

Figure 2: Blockchain Based Framework [6]

2. Literature Review

[7] had proposed an encrypted framework for healthcare using IoT and blockchain network. The framework helps in providing a secured control access policy to the end user to maintain the security and privacy of the patient health data. The proposed framework also supports the keyword-based data search to access and find the records easily with lesser time complexity. The proposed method had shown better accuracy, dead node, and search operations than existing models such as Medrec, Medchain.

[8] proposed a custom blockchain security model for the IoT that utilizes an Inter-Planetary File System (IPFS) that queried transactions. The IoT devices interacted as nodes of the blockchain, that isolates their interface with external networks, as only validated and signed transactions are processed. The authors simulated a deployment that indicated excessive latency and low throughput as the number of nodes and transactions augmented, which might indicate performance problems if the solution is taken under more challenging situations. Additionally, the paper does not offer data nor analysis on device performance as IoT equipment actively interacts with the blockchain and the file system.

[9] had proposed a model to secure the healthcare data using blockchain and internet of things. The IoT network sense and collect the environment data in real time and store data over blockchain network. The network is immutable and can detect and block all the malicious activities. But still the model had not addressed several issues like the power consumption of IoT devices and latency.

[10] offered a new security model custom blockchain inspired after Bitcoin, that trades tokens instead of coins that are used to distribute voting power and limit transactions rate to prevent DoS attacks. The new protocol exchange additional messages that exchange authentication information as well as public keys to enable confidential exchange of data. Nevertheless, the publication lacks cryptoanalysis of the different exchanges as well as experimental data that confirms the operability of the protocols. Custom offerings for blockchain protocols need to present empirical evidence of their feasibility and reliability.

Blockchain technologies can also be organized by their operation type: (1) Public, (2) Consortium, and (3) Private [11]. Public blockchains are accessible by anyone over the Internet, users can

interact freely with it and secured by monetary compensation. Consortium blockchains are maintained by a "pre-selected set of nodes" [12] where read rights may be public or not, and private blockchains are fully restricted systems with constrained rights to read, generally belonging to a specific organization. Table I compares the three types as the consensus method, the efficiency, and the security differ within each other.

Table I Blockchain Operational Categorization [13]

Parameter	Public Blockchain	Consortium Blockchain	Private Blockchain
Access	Unrestricted Public	Selected set of nodes can access the network	Restricted, only authorized private node can access.
Read and Write Permission	Public	Public or Restricted	Public or Restricted
Security	Cannot be tampered	Might be tampered	Might be tampered
Consensus Mechanism	Permission Less	Permissioned	Permissioned
Efficiency	Low	High	Highest

[14] introduced an access control management solution for IoT devices that uses blockchain technology to provide secure data sharing protocol. The Bitcoin blockchain stores access permissions that are granted on a data-stream basis, which could be revoked at any time by the data owner. The IoT devices interact with the blockchain through the IoT gateway that also serves as a intermediary storage unit, that also caches recently used data. The paper includes thorough description of the blockchain and data storage process that include formal message definitions. The primary evaluation presented by the authors shows a slowdown compared to Amazon's S3 storage service that increased with the inclusion of more nodes. Further testing and supporting data is needed for blockchain mining efficiency suitability from a proof-of-concept implementation.

[15] came up with a one-time authentication scheme built on top of a public Ethereum smart contract that determines resource accessibility. Once the user is authenticated, and granted an access token, she/he can interact with the IoT device (running an Ethereum lightweight client) by any communication method during the authorized time or until revoked. Initial testing showed resiliency against replay, man-in-the-middle (MITM) attacks, and malicious packet injections, although cryptanalysis is missing. It also shows ease of use, as the end user needs to make a single request to maintain data accessibility. In terms of blockchain efficiency, even though the study did not present data, seems reliable as mining is not needed as a Proof-of-Authority (PoA) protocol is used. Nevertheless, the solution needs actual currency (gas) to run instructions determined in the contract, which can mean an important financial stress over the system owners when more devices are attached. Also, the proposed platform requires blockchain-enabled devices to complete the authorization process, that might be difficult to achieve as IoT manufacturers need to be involved.

[12] proposed a multilayer network distributed architecture for enterprise environments. The solution uses the blockchain for network controllers to allocate network topology and traffic data to dictate policy rules for the software defined networking (SDN) management platform. The system learns common traffic patterns and reacts to abnormalities that interact with SDN and access control rules to block possible threats. The proposal strengths reside on its ability to adapt current technologies with fault tolerance distributed protocols without altering IoT composition and functioning that interact with a high-availability architecture. However, the solution works on top of a custom blockchain private network that might not offer the same robustness as major blockchain offerings. Also, additional real-world testing and comparison studies are needed as the published simulation might not encompass all variables. Finally, due to its complexity and scope it is limited to organizations with the financial means to deploy.

Table II IoT security challenges and requirements [[18]–[20]]

IoT Layer	Security Challenges	Security Requirements
Perception	• Poor Physical Security of IoT devices • Jamming • Integrity and Confidentiality can be compromised	• Tamper Resistance
Network	• Weak Authentication • Insecure Network • DoS • Eavesdropping • Network Heterogeneity • Multiple entry points	• Strong Authentication and Access Control • Availability • Integrity • Strong attack defense mechanism

Application	• Insecure Web Interfaces • Poor privacy and security control • Weak passwords • Malware penetration • Faulty Software development methods • Poor client security • Fishing Pages • Application crashes	• Secured Environment • Secure data migration over cloud for recovery • Control access for privacy

3. Proposed Framework

In this work the focus is to propose a remote healthcare model to monitor the patients outside the hospital. The proposed model is based on two major technologies internet of things to sense the data using wearable devices and to transmit the data to a blockchain network [19]. The blockchain network store the data of the patient maintain the ledgers. The patient data is continuously monitored using IoT or wireless devices that will be uploaded over local database where the possible anomalies are monitored. In case of any emergency event the doctor can immediately take a suitable action. All the data is stored and analyzed from time to time to check the occurrence of various alarming events and o check their pattern of occurrence. The data in the complete scenario is confidential and must be only available for access by patient or any authorized party. In this work a blockchain based architecture is used to store data and monitor the patient.

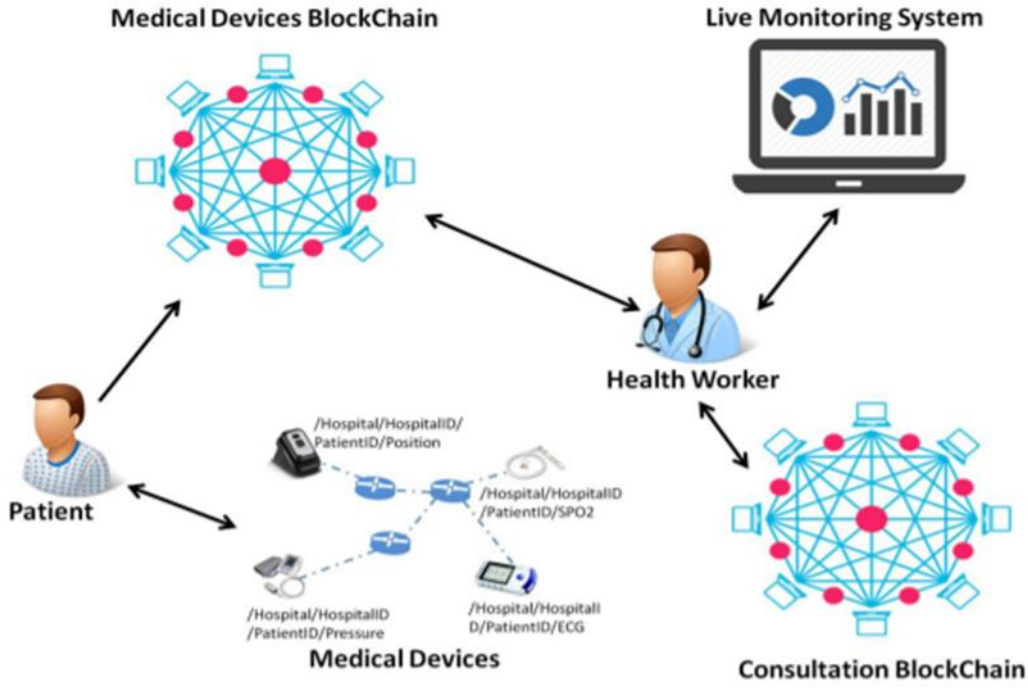

Figure 3: Blockchain Based Healthcare Framework

a. Patient: Patient act as a node for medical device blockchain network. Patient node receives data from various deployed medical devices and shared with patient. The data from node then transmitted to medical device blockchain where data is stored in ledger after data encryption.

b. Medical Devices: These are small wireless devices that can sense the patient parameter continuously. These devices are portable

c. Wireless or IoT based Medical Devices: The wireless medical devices are deployed at patient location or devices are wearable by the patient. These devices are deployed to record and collect the patient data to store over blockchain network. The smarts contract will be executed by minion nodes to commit the transaction. A learning network can also be used here that is trained to monitor the patient medical records and in case of any expecting emergency the report can be sent prior to a medical staff.

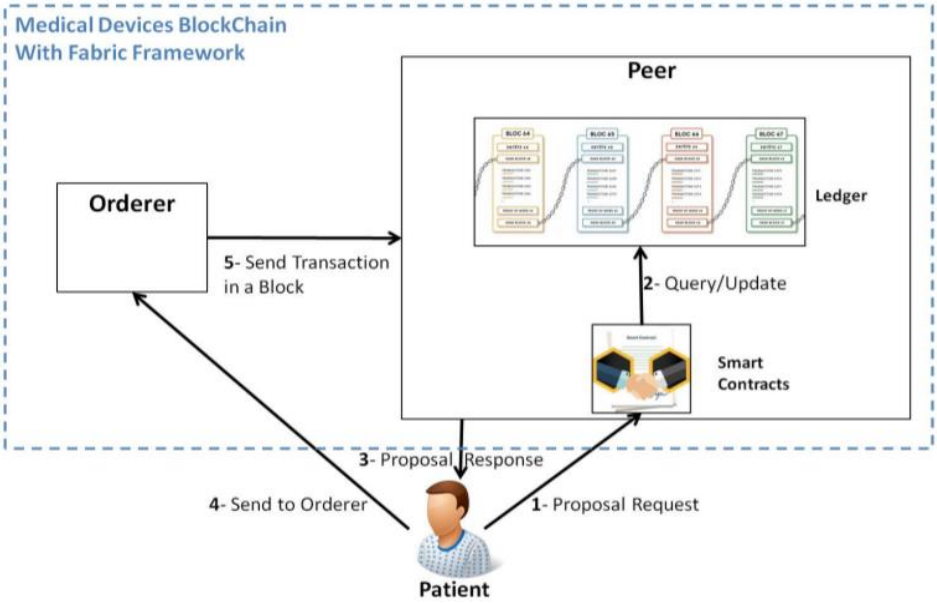

Figure 4: Patient and Medical Device Blockchain Interaction

d. Health Worker: A health worker can be any doctor or nurse. A health worker act as a node between both medical and consultation blockchain network. A health work physically visualizes and monitor the data of the patient using live monitoring system that displays the data stores over medical device blockchain network.

e. Encryption: Medical Blockchain provides an access control encrypted environment. Most of the existing model had just worked on providing the access control, but in this model the encryption is also used to provide the security. The keyword search is also providing to ease the data accessibility.

Algorithm 1: Encryption

Input: Public Key used for encryption and search
X ← 0 initial index value of keyword K;
Select key K_s for $K_{R\ (keyword)}$;
Choose key ∀ rounds + 1 (K_s, K_t …K_n);
for K [ ] do Z * p →parse DB (K_{id1}, id_{x+1});
t← DB (K_{id1}, id_{x+1});
for id ∈ DB(k) i_0 do
set Counter c ← 1;
Query: c x Q (cipher used to encrypt query Q), cQ←Encrypt(Q);
Function Encrypt (cQ) {
Initialize charnum = [0];
While(infile! →eof) do read
Text←infile.read(line) update charnum →eof;
cDB [charnum++] ← Encrypt(c); // Query encryption
end while;
return Q_e;
exit;

f. Blockchain Consultation Network: This network is used to store all the history of the patient information and records. It is distributed to medical centers that make it easy more secure to exchange the data between hospitals and doctors. This blockchain is to store the patient data permanently and make in immutable.

4. Overall Interaction Process (Health Worker, Medical Blockchain, User)

i. A patient visits the hospital where unique id given to patient. The patient interacts with doctor to generate the medical data.
ii. Once the information is generated a smart contract is initiated on blockchain by health worker. The generated hash value corresponding to signed medical data is stored in blockchain network.
iii. The medical records then are encrypted with a mutual access policy between doctor and patient and upload over LMS.
iv. LMS return the data location to the health worker where all the records are stored.
v. The health worker then encrypts the location of medical records and then embed cipher text (C) in transaction and broadcast on blockchain.
vi. For all the confirmed transactions, the address of those transaction was stored.
vii. The blockchain network encrypt the medical keywords and generates a keyword index. Then the generated keyword and transaction address are recorded in smart contract information format.
viii. The authorized user can request for patient medical data access, the identity of user is be verified by doctor. In case of an authorized user the information of user is added into smart contract.
ix. The attribute key of data is generated and shared with the user added in smart contract through a secured channel.

x. The authorized user creates a search token and execute the smart contract passing search token as parameter.

xi. The identity of authorized user then verified before smart contract execution, if identify is verified the smart contract share the search results with user.

xii. The request user read the transaction data from block chain network and compute the address of file location.

xiii. The request user once obtains the file location then can download the encrypted medical records.

xiv. The request user identifies the cipher file structure and obtain the decrypted copy of medical data.

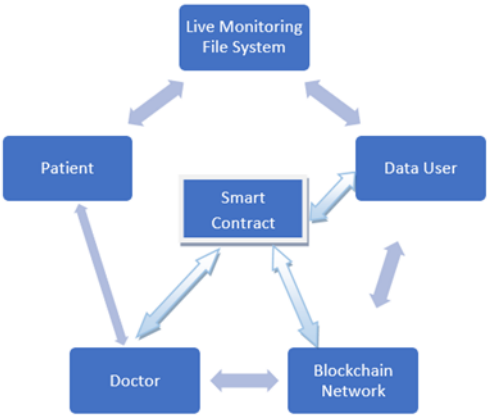

Figure 5: Interaction Process Flow

5. Security and Performance Analysis of Proposed Algorithm

The proposed framework introduces the control access with data encryption for better security and a learning algorithm model of reinforcement or back propagation learning can be used to analysis the information from patient data and helps in prediction future health issues. Also, the network can help the patient by suggesting the suitable course of action in emergency when doctor is not available. The proposed model ensures the secured storage, provides the privacy, tamper proof.

a) Secure Storage: The data storage security is one of the most important aspects of this work. The complete process of exchanging and generating information is secure. The medical records of the patients are stored over blockchain network, and the stored information cannot be tampered and not available for public view. The health worker is authorized to generate the hash value for the record to store on blockchain. The records are encrypted and store on blockchain recording its location. The distributed storage system ensures the data storage security.

b) Protection of Privacy: The request user demands the records in anonymous way with different values of public and private keys, this protects the user identity [20]. The address location of the data is stored on the blockchain any malicious user cannot access the information. Further if the contract execution policy not satisfied then it is impossible to obtain the data from blockchain.

c) Tamper Proof: The information stored on the blockchain public. The consensus mechanism of the blockchain network is not relied on any third party. Once the information is written on the blockchain network after the 50% polling from authentication nodes the information cannot be tampered as each block is saving the hash of previous. In case any malicious node tries to modify the information than 51% of the total computation power or 51% of the node's authentication required, which is impossible to obtain for a malicious node. This makes the proposed network non tempered.

d) Learning: The proposed model used a learning framework with designed consensus mechanism based on learning gradient verification. The data is downloaded from the latest blockchain block and the average gradient for all the qualified blocks is computed. The training rounds are continuous till the max round reached. In each round the reputation value of IoT device is increased or decreased according to the threshold. In case of value lesser then threshold the node is blacklisted. The model is trained based on the real time present and past information and helps the patient in case of an emergency.

Algorithm 2 Federated Learning

Input: Dataset D //recorded data from IoT devices
Output: Out_model O_{final}
Initialize O_{final} model parameters
for i→ end do repeat
Forward propagation- out→model = func f [p(D_i, O_i);
For i to n calculate loss: L = loss(func f p (D_i,), out);
if $L_i < \in$ then
break
else
back-propagation: $gradient_i$ = bp(D_i, O_i, L_i);
for each round forward →gradient value to server → out new gradient
update: gradient value as
$O_{i+1} = O_i - lr * gradient_{updated}$
end if;
end for;
return →Final Model = O_{final}

6. Conclusion

In this paper the focus is on developing a healthcare monitoring system where the data sensed and collected by

the various IoT devices is critical. This paper proposes a framework integrating the blockchain and IoT network together to ensure the privacy and data security. The module of learning is also introduced with blockchain to learn from the patient data and predict the future problems. This helps the doctor and patient to understand and take a required action against the predicted problem This network also helps the patent by suggesting the course of action in case of emergency based on the past experience in case of doctor not available. The proposed model looks promising in terms of security analysis too. In future, the proposed model can be implemented using suitable tools to analysis the performance of network in real time.

References

[1]. P. Malhotra, Y. Singh, P. Anand, D. K. Bangotra, P. K. Singh, and W. C. Hong, "Internet of things: Evolution, concerns and security challenges," Sensors, vol. 21, no. 5, pp. 1–35, 2021, doi: 10.3390/s21051809.

[2]. X. Yao, F. Farha, R. Li, I. Psychoula, L. Chen, and H. Ning, "Security and privacy issues of physical objects in the IoT: Challenges and opportunities," Digit. Commun. Networks, vol. 7, no. 3, pp. 373–384, 2020, doi: 10.1016/j.dcan.2020.09.001.

[3]. J. Neeli and S. Patil, "Insight to security paradigm , research trend & statistics in internet of things(IoT)," Glob. Transitions Proc., vol. 2, no. 1, pp. 84–90, 2021, doi: 10.1016/j.gltp.2021.01.012.

[4]. M. S. Gross and R. C. Miller, "Ethical Implementation of the Learning Healthcare System with Blockchain Technology," Blockchain Healthc. Today, vol. 2, no. July, 2019, doi: 10.30953/bhty.v2.113.

[5]. J. Y. Lee and J. Lee, "Current Research Trends in IoT Security: A Systematic Mapping Study," Mob. Inf. Syst., 2021, doi: 10.1155/2021/8847099.

[6]. G. Rathee, A. Sharma, H. Saini, R. Kumar, and R. Iqbal, "A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology," Multimed. Tools Appl., vol. 79, no. 15–16, pp. 9711–9733, 2020, doi: 10.1007/s11042-019-07835-3.

[7]. A. Ali et al., "An Industrial IoT-Based Blockchain-Enabled Secure Searchable Neural Network," Sensors, vol. 22, no. January, 2022.

[8]. G. Huang and A. Al Foysal, "Blockchain in Healthcare," Technol. Invest., vol. 12, no. 03, pp. 168–181, 2021, doi: 10.4236/ti.2021.123010.

[9]. A. Banotra, J. S. Sharma, S. Gupta, S. K. Gupta, and M. Rashid, "Use of Blockchain and Internet of Things for Securing Data in Healthcare Systems," Multimed. Secur. Algorithms Intell. Syst., vol. 31, no. January, pp. 255–267, 2021, doi: 10.1007/978-981-15-8711-5_13.

[10]. Vanitha, D. D. . (2022). Comparative Analysis of Power switches MOFET and IGBT Used in Power Applications. International Journal on Recent Technologies in Mechanical and Electrical Engineering, 9(5), 01–09. https://doi.org/10.17762/ijrmee.v9i5.368

[11]. Q. Qu, R. Xu, Y. Chen, E. Blasch, and A. Aved, "Enable Fair Proof-of-Work (PoW) Consensus for Blockchains in IoT by Miner Twins (MinT)," Futur. Internet, vol. 13, no. 11, p. 291, 2021, doi: 10.3390/fi13110291.

[12]. Kadhim, R. R., and M. Y. Kamil. "Evaluation of Machine Learning Models for Breast Cancer Diagnosis Via Histogram of Oriented Gradients Method and Histopathology Images". International Journal on Recent and Innovation Trends in Computing and Communication, vol. 10, no. 4, Apr. 2022, pp. 36-42, doi:10.17762/ijritcc.v10i4.5532.

[13]. S. Algarni et al., "Blockchain-based secured access control in an iot system," Appl. Sci., vol. 11, no. 4, pp. 1–16, 2021, doi: 10.3390/app11041772.

[14]. J. Warraich, C. Singh, and P. Thapa, "Blockchain-based Intelligent Monitored Security System for Detection of Replication Attack in the Wireless Healthcare Network," Eur. J. Eng. Technol. Res., vol. 6, no. 6, pp. 160–170, 2021, doi: 10.24018/ej-eng.2021.6.6.2599.

[15]. A. Sharma, S. Kaur, and M. Singh, "A comprehensive review on blockchain and Internet of Things in healthcare," Trans. Emerg. Telecommun. Technol., vol. 32, no. 10, pp. 1–53, 2021, doi: 10.1002/ett.4333.

[16]. P. Ratta, A. Kaur, S. Sharma, M. Shabaz, and G. Dhiman, "Application of Blockchain and Internet of Things in Healthcare and Medical Sector: Applications, Challenges, and Future Perspectives," J. Food Qual., vol. 8, no. 3, 2021, doi: 10.1155/2021/7608296.

[17]. E. Westphal and H. Seitz, "Digital and Decentralized Management of Patient Data in Healthcare Using Blockchain Implementations," Front. Blockchain, vol. 4, no. August, pp. 1–6, 2021, doi: 10.3389/fbloc.2021.732112.

[18]. I. Technology, "BLOCKCHAIN-BASED SECURITY FRAMEWORK FOR THE by," no. May, 2021.

[19]. Pepsi M, B. B. ., V. . S, and A. . A. "Tree Based Boosting Algorithm to Tackle the Overfitting in Healthcare Data". International Journal on Recent and Innovation Trends in Computing and Communication, vol. 10, no. 5, May 2022, pp. 41-47, doi:10.17762/ijritcc.v10i5.5552.

[20]. S. Jeong, J. H. Shen, and B. Ahn, "A Study on Smart Healthcare Monitoring Using IoT Based on Blockchain," Wirel. Commun. Mob. Comput., vol. 14, no. 7, 2021, doi: 10.1155/2021/9932091.

[21]. C. Nartey et al., "Blockchain-IoT peer device storage optimization using an advanced time-variant multi-objective particle swarm optimization algorithm," EURASIP J. Wirel. Commun. Netw., vol. 2022, no. 1, 2022, doi: 10.1186/s13638-021-02074-3.

[22]. R. Arul, R. Alroobaea, U. Tariq, A. H. Almulihi, F. S. Alharithi, and U. Shoaib, "IoT-enabled healthcare systems using block chain-dependent adaptable services," Pers. Ubiquitous Comput., 2021, doi: 10.1007/s00779-021-01584-7.

[23]. S. Khatri, F. A. Alzahrani, M. T. J. Ansari, A. Agrawal, R. Kumar, and R. A. Khan, "A Systematic Analysis on Blockchain Integration with Healthcare Domain: Scope and Challenges," IEEE Access, vol. 9, pp. 84666–84687, 2021, doi: 10.1109/ACCESS.2021.3087608.

[24]. Kuila, S., Dhanda, N., Joardar, S., & Neogy, S. (2019). Analytical survey on standards of Internet of Things framework and platforms. In Emerging Technologies in

Data Mining and Information Security (pp. 33-44). Springer, Singapore.

[25]. Kuila, S., Dhanda, N., Joardar, S., Neogy, S., & Kuila, J. (2019). A generic survey on medical big data analysis using internet of things. In First International Conference on Artificial Intelligence and Cognitive Computing (pp. 265-276). Springer, Singapore.

[26]. Joy, P., Thanka, R., & Edwin, B. (2022). Smart Self-Pollination for Future Agricultural-A Computational Structure for Micro Air Vehicles with Man-Made and Artificial Intelligence. International Journal of Intelligent Systems and Applications in Engineering, 10(2), 170–174. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/1743

[27]. Gill, D. R. . (2022). A Study of Framework of Behavioural Driven Development: Methodologies, Advantages, and Challenges. International Journal on Future Revolution in Computer Science &Amp; Communication Engineering, 8(2), 09–12. https://doi.org/10.17762/ijfrcsce.v8i2.2068

[28]. Verma, R., Dhanda, N., & Nagar, V. (2022). Security Concerns in IoT Systems and Its Blockchain Solutions. In Cyber Intelligence and Information Retrieval (pp. 485-495). Springer, Singapore.

[29]. Tiwari, S., Dhanda, N., & Dev, H. (2022). A Systematic Review of Adoption of Blockchain and Machine Learning Technology and Its Application. Soft Computing for Security Applications, 73-95.