Applications of Ensuring Security and Privacy Using Block Chain with IoT for Health Record

Abdul Shareef Pallivalappil*
College of CSIS
Srinivas University
Mangalore, India
shareef.abdul777@gmail.com

Dr. Sayed Sayeed Ahmad
College of Engineering and Computing, Al Ghurair University
Dubai, UAE
saeed.ks@gmail.com

Dr. Yeligeti Raju
Dept. of CSE
Vignana Bharathi Institute of Technology, Hyderabad, India
raju.yeligeti@gmail.com

Ch. Kishore Kumar
Dept. of Computer Science
Vels University
Chennai, India
kishore.chennuri@gmail.com

Mr. Thamba Meshach W
Dept. of CSE
Prathyusha Engineering College, Tamilnadu, India
twmeshach@gmail.com

Dr. Nallam Krishnaiah,
Dept. of IT
St. Martin's Engineering College, Telangana, India
nkrishna520@gmail.com

2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) | 978-1-6654-3789-9/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICACITE53722.2022.9823735

Abstract— The healthcare system has key security and privacy requirements when considered like an enterprise, such as safeguarding patients' medical records from unwanted access, protected drug tracking, secure connection with transportation such as ambulances, and secure and smart e-health surveillance. With suitable security measures, block chain has brought novel concepts in security and safety of medical data, and it may reconcile the discrepancy among sharing data and confidentiality. We combine the strengths of both block chain and cloud computing in this research to provide a confidentiality method for block chain and IoT. This strategy incorporates IoT and delivers IoT services to block chain nodes; in the meantime, it gathers, examines, operates, and preserves in the identity validation for health information. Interaction and addresses the inadequate computing capabilities of some block chain nodes in order to confirm data validity and feasibility. The proposed approach is efficient, as demonstrated by the simulation experiment. It can preserve and verify the integrity of medical data while also addressing issues such as high computer complexity, data exchange, and privacy protection.

Keywords - ***Block chain, Healthcare system, IoT, security, privacy and storage***

I. INTRODUCTION

Clinical studies necessitate substantially de-identified patient data. The aggregation process for de-identification of patient data requires a long time and effort, resulting in a significant cost. The (i) accessibility and (ii) analyzable features of enormous PT sets that must be de-identified are major challenges in achieving precision in the results of real clinical trials. In the final stage of the activity, a meta-analysis is required to determine whether the majority of e-health customers are willing to contribute their EHR for research and clinical examination, as long as privacy and confidentiality are protected. Constructing the block chain, which has higher openness, can be used to visualize such a trust-leveraging operation. With the support of an embedded hybrid block chain facility, widespread e-health patients can leverage IoT architecture to openly change and discreetly store their own EHR data. To disseminate the DLT (Distributed Ledger Technology) for the facilitation of safe clinical information amongst community-driven clinical study and research, hybrid key cryptography can be used. Patients subject to IoT system can quickly access and control their own EHR, as well as allow or deny EHR-data accessibility to health care providers, hence assisting clinical organizations in accessing DLT via a vast EHR library of correct and complete clinical data [1].

As block chain and the Internet of Things mature, associated approaches in medical and health services, such as medical information, mobile health, e-commerce in health, wearable's, and online services in medical, have seen tremendous growth [2]. Block chain technology must encompass four features in general: point-to-point network design, encryption method, distributed algorithm execution, and data storing techniques. Other features include things like distributed storage, machine learning, virtual reality, the internet of things, big data, and so on. In its most basic form, block chain is limited to data storage technology, database or file operations, and so on [3]. Proxy re encryption and attribute-based encryption can be utilized in sharing of medical data with patient confidentiality in addition to existing encryption methods [4]. The user retrieves and decrypts privately encrypted text material using conventional encryption standards. The client then encrypts information by the designated client's public key, which can decrypt the data, although this adds to the client's costs by increasing network overhead and running costs, as well as occupying the client's limited memory [5].Proxy re-encryption is defined as a client's ability to decrypt the encrypted text of another related user without exposing the users' private key, that is typically [6]. In ABE, a data holder define an accessing policy only customers that meet the authorization in data encryption could decode the text, enabling for one-to-many information sharing and personal data security [7]. These will have a significant influence on the progress of healthcare industry's development.

The following are some of this paper's unique contributions:

A. *We investigate traditional approaches in depth with the goal of data exchange and patient personal privacy in intelligent hospitals, as well as others. We also look into how block chain and IoT technology can be used in smart healthcare scenarios.*

B. *To improve the processing capacity of the user side, we offer a strategy for protecting the privacy of medical data that is distributed, include IoT patterns, and develop a block chain-based distributed data management framework. Likewise, to protect the confidentiality of patient sensitive information, we use the private chain in block chain.*

C. *The efficiency of the strategy in this research was confirmed by a simulated exercise. Not only can healthcare data be successfully exchanged across medical institutions using block chain and IoT, but the patient data confidentiality may also be ensured.*

Figure 1 depicts an Internet of Things (IoT)-based Block Chain Technology (BCT) system for securing and protecting health-care data. The following are the steps in applying principles:

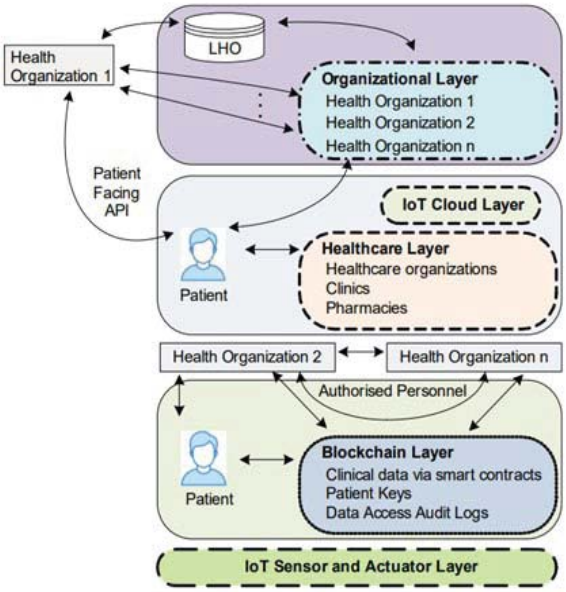

Fig. 1. IoT-based Block Chain Technology (BCT) system for health care data secure and privacy

- A transaction is requested in a block chain network by an individual.
- A request to transaction is then published to the other members.
- The transaction is then approved by the network of nodes using certified algorithms.
- They finalize the transaction after the nodes have approved the request.
- A new irreversible block is appended to block chain network instantly after the transaction.
- After that, the validated transaction is merged with others to create a new data block.
- The private key signs the transaction if everyone who wants to add content to the block chain needs an open address with a unique key to log in. This type of data is extremely safe from hackers.

The remainder of this paper is organized as follows: Section 2 reviews the available literature and provides a comparison of some existing EHR security methods that use block chain. The incorporation of block chain technology-based IoT for the health-care system is discussed in Section 3. Sections 4 and 5 detail the experiment results, while Section 5 discusses the conclusion.

II. Literature Survey

This section discusses the motivations for performing this study on block chain and IoT in the healthcare system model, as well as the review technique followed.

Health information has accurately recorded people's ailments, and health records, safe storing and exchange of protecting medical data and patient confidentiality has become increasingly crucial as intelligent hospitals are built. Conventional method for controlling accessibility constructs and performs a secure access strategy based on a perfectly trustworthy server, thus challenging to adapt to today's distributed network scenario. Block chain through dispersed data storage, has given individuals a brand-new design, an agreement algorithm, with encryption techniques [8], which are characterized by decentralization and trustless-ness. Recently, ABE has become an essential technological approach in the cloud computing environment, and ABE method has been thoroughly investigated in the computer scenario. Like an encryption technique that employs the characteristic as a public key, it connects users to cypher texts via the characteristic. Its controlling accessibility and encryption, adaptability has significantly improved the cloud strage security [9]. Furthermore, it has acquired fine-grained accessibility and has emerged as the primary method for controlling cloud storage availability in a secured manner. The classic ABE mechanism, on the other hand, fails to provide total data secrecy, potentially stop collision attacks, or fulfill the forward and retrograde security of attribute revocation, as well as the high cost of computing associated with revocation. The application of block chain to cloud computing and the usage of block chain's security solution to improve cloud computing's secure storage and efficiency will be a major focus of research. The tension among data sharing and privacy could resolve by integrating block chain as well as cloud computing, with solid security policy [10].

The literature review revealed a few constraints in current block chain systems for healthcare systems that must be recognized and efficiently leveraged in order to fully employ IoT-centric health services. We discovered that there is no effective research on the use of IoT and block chain technology to improve the quality of healthcare. As a result, this work attempted to overcome the limits in order to foster a comparable interest within the scientific community.

III. Integration of Block Chain Technology with IoT for Health Care Model

The development and integration of block chain technology with IoT for the health care model is discussed in this section. It presents a strong platform for constructing a tangible health-care system that must incorporate medical IoTs [11-16]. Its structure, as shown in figure 2, positions

health system information in IoT as system's fundamental seed. The goal is to control and coordinate big data in healthcare that respects data seclusion with exploits data interoperability, and to make it easy to monitor and manage the data created by health care systems and IoT devices for a long time [17].

A. IoT Based Block Chain Technology Integrated System for Health Care

Figure 2 depicts the IoB Health's basic process in order: first, the EHR is placed keen on the supplier's, and then EHR is submitted with framework's core to be mined. Three sub-tasks complete the mining and related tasks: sum contract resolution, distributing newly added patient relations, as well as embedded Sum Con to detailed PR. The miners mine and harvest the underlying sub processes. The patient's node's crypto-client modifies the respective Sum Con after successful mining. Similar procedures are used to notify patients of such situations. The Sum Con's PR is adjusted in response to the patient's acknowledgements (or rejections). As a result, the EHR engine of the provider updates the data in its local database to match the dynamic trends. It then asks for to gain accessibility to the current chain. After that, the choice is made to change the patient's local database. As a result, all sides have the same copy of the EHR data, resulting in a situation where transparency and fraud-free features can be significantly strengthened. The architecture now includes a novel technique that can send/receive requests/replies from/to the patients' node's back-end library using the DB gatekeeper of the providers' node. The Internet of Business Health (IoB Health) allows three key stakeholders to participate: (i) government agencies, (ii) healthcare providers, and (iii) e-healthcare planners. They have the ability to interfere in the proposed framework by voting a predetermined level of agreement between the network participants. The architecture determines Sensible contract information and medical transaction data implementation in such a way that all required operations, such as identity probing, possession, interpretations, stewardship, and inquiry referencing, may be carried out. IoB Health is expected to be able to handle both real-time and off-line EHR data in order to deliver a seamless healthcare service [18].

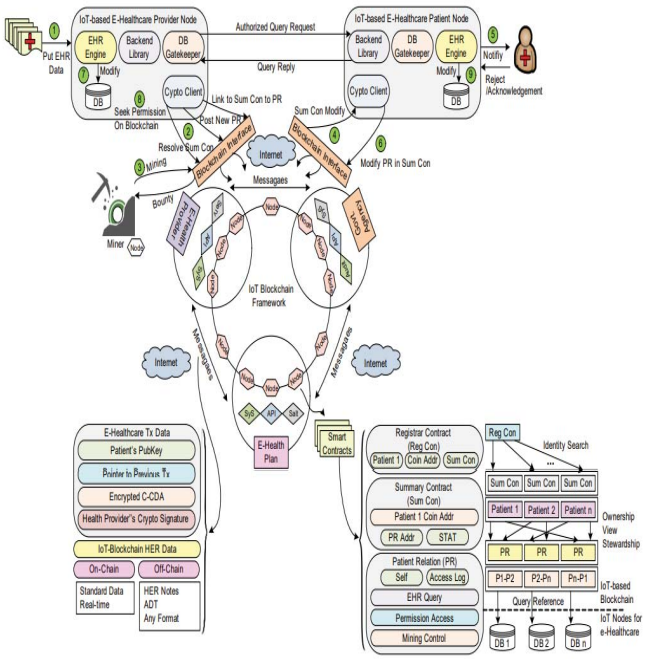

Fig. 2. Integration of Block Chain Technology with IoT for health care system

B. Capsule Networks

The notion of convolutional neural networks (CNN) has multiple flaws: (1) The max-pooling process discards information regarding the location of an entity that the network is attempting to recognise, as well as (2) convolutional neural networks ignore numerous spatial relationships between smaller objects. CNNs with max-pooling layers, on the other hand, have resulted in the rapid development of the deep learning area. So it was only a matter of time until a system has CNN capabilities and none of its drawbacks - capsule network using dynamic routing [7] - was devised. The concept of capsules is not new; G. E. Hinton, a prominent figure in the field of deep learning, has been thinking about it for some time. Until the route optimization algorithm was presented [7], it had never worked previously. The notion of Convolutional capsule network (CapsNet) would be discussed in further depth in the following sections. To begin with, a capsule is a collection of neurons that outputs are perceived as different aspects of the same item. A posture matrix as well as an activation probability is both included in each capsule. These activities are similar to those of a typical neural network. The length of a capsule's output vector can be regarded as the likelihood that the entity it represents is applicable to the present input. Capsules can be stacked in many layers. We employed a layer of main capsules (the output of the final convolutional layer reshaped and compressed) as well as a level of Cancer-Caps (capsules representing four sorts of images: regular, benign, in-situ, and invasive) in our design.

$$v_j = \frac{\|S_j\|^2}{1 + \|S_j\|^2} \frac{S_j}{\|S_j\|'}$$

C. IoT Based Health Care system

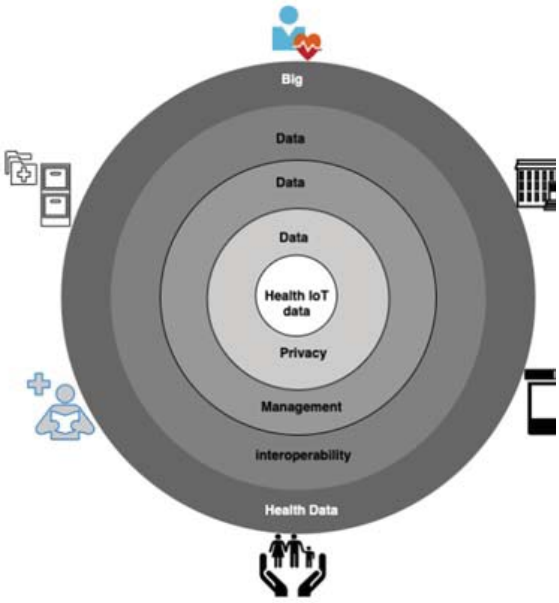

Fig. 3. The layered architecture for a feasible IoT Health Care record

The six layers of the proposed approach are as follows:

- Health IoT Devices layer: As the primary sources of personal health data, devices are at the heart of the architecture. To improve the well-being of patients, a variety of health IoT systems are employed. They should make good use of the huge volumes of health data they generate.
- Data Management Layer: A good data management system includes data privacy and secure methodologies as well as the ability to share data with other parties. This layer addresses and develops encryption and anonymization technologies while keeping data protection standards in mind.
- Data Interoperability Layer: This layer applies proper interoperability standards, such as FHIR interoperability standards in our situation. This means that data may be exchanged between multiple systems, such as IoTs and EHRs, in a straightforward and intelligible manner, saving time and money.
- Big Health Data layer: this layer contains big data and data analysis technologies and techniques that are used to maximise the value of health data. The bulk data produced by health IoT devices should be able to be used by reliable personal health record systems.
- The Health Services and Stakeholders benefit from the system's overall framework. Patients, physicians, and other health maintenance benefactors are included, as well as other parties involved in the healthcare area, such as research centres and commercial firms [19].

D. Block Chain Technology

The block body is made up of transactions that have been validated over a certain amount of time. The Merkle tree, where every leaf node represents a transaction and every non-leaf node is the hash value of its two concatenated child nodes is used to record all the legitimate transactions. Because every node can check the validity of any transaction by the hash value of the related branches instead of the complete Merkle tree, such a tree structure is efficient for verifying transaction presence and integrity. Nevertheless, any changes to the transaction would cause an original hash value to be generated in the top layer, resulting in a faked root hash. Furthermore, a block's maximal amount of transactions can include is determined by the transaction size as well as the block size [20].

Applying a cryptographic hash function, such blocks are joined into append-only structures. New data is only contributed in the shape of supplementary blocks chained with preceding blocks because it is difficult to edit or delete already confirmed data. Every update to one of the blocks, as previously stated, results in an unique hash value and link connection. Permanence and confidentiality are gained as a result [21].

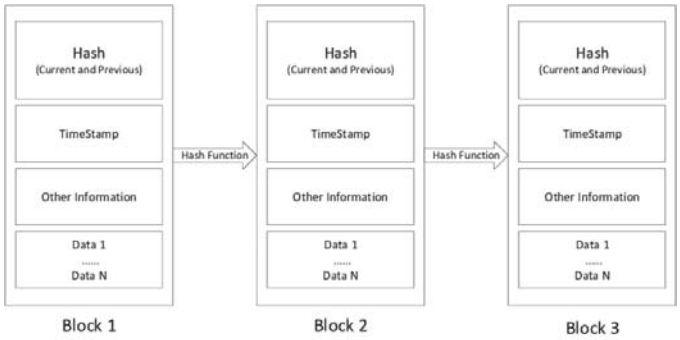

Fig. 4. Block Chain Technology architecture

1) Improved Block Chain Technology

Nonetheless, because of the high costs of processing, storage, and bandwidth, block chain technology may not be viable for real application development. High data volumes, recurrent queries, and the reliability of block chain cannot be overlooked when many firms engage in the network. To mitigate these drawbacks, the suggested homomorphism encryption and zero-knowledge verifications can be used to avoid data forensics by implication, retain the discretion of personal data, and permit calculations to be executed without the leaking of input and output.

Algorithm: Block Chain Technology formation to secure health care data

Input: Readings from a patient's electronic health record (EHR) Pat1

Output : Forming the Patient Pat1 Block Chain and adding Blocks to the Patient Pat1 Block Chain

Step 1 : Patient Pat1 EHR Readings in the EHR

Step 2 : RSA cryptography is used to generate public and private keys.

Step 3 : The public key is used by the patient to encrypt data. For the purpose of decryption, the secret key was shared with the recommended doctor and the insurance agent.

Step 4 : Encrypted EHR encrypts EHRs using a public key.

Step 5 : Using HMAC-SHA1, generate a hash for encrypted EHR.

Step 6 : Create a bilinear mapping for an encrypted EHR with patient data ID

Step 7 : Utilizing the patient name, password, and patient ID, establish a Genesis block for the Patient Pat1 block chain.

Step 8 : Put encrypted EHR in a block and hash with a Bilinear Map.

Step 9 : Add this Block to the chain of Patient Pat1 Blocks.

Step 10 : Development of the Doctor Doc1 Block chain and the addition of blocks to the Doctor Doc1 Block chain, as well as the formation of the Insurance Agent IS1 Block chain and the addition of blocks to the Insurance Agent IS1 Block chain.

2) Benefits of Improved Block chain Technology for health care System

In the BSF-EHR system, block chain offers numerous advantages. These include the following:

- Improved health-record interchange
- Data security and privacy have been improved.
- Enable the medical supply chain to function more effectively.

This comprehensive proposed framework is expected to enable the following benefits over traditional healthcare systems: (i) immutability and traceability for patients regarding IoT systems enabling ease of receiving health care data that isn't in danger of being tampered with or corrupted, (ii) assurance of safety for health care data, (iii) (iv) incentivizing patients whose health care data is flawlessly utilized, (v) issuing and withdrawing rights by patients to people who need access to their health care information, (v) provide a cohesive framework for various healthcare organizations and pharmaceutical companies to participate in clinical investigation and trials relating to drug design, medicines, and distribution via the global DLT database, (vi) relatively inexpensive costs, enhanced interoperability, universal coverage, and high level of integrity, and (vii) offering alternatives for healthcare conformity and remote patient monitoring via the global DLT database, and chronic health conditions based on the suggested IoT-based block chains for the healthcare environment.

IV. RESULTS AND DISCUSSION

Using the BCT with IoT technology, this work intends to preserve patients' privacy and maintain the uniformity of health records. The block chain used in this experiment was developed in Java [22]. Block chain is a technique that allows non-trusted parties to conduct transactions. A block chain is a collection of blocks that each includes one or several transactions. After hashing each block, the hashes are joined together, hashed again and the process is repeated until a new hash occurs, known as Merkle root of a Merkle tree. By joining the blocks together, every block records the hash of a preceding block. This assures that if one block is altered, all subsequent blocks will be changed as well. This experiment stores data in the form of a string that includes Ethereum-style smart contracts. The BCT with IoT for health care system was explored in this experiment, and the effectiveness of the BCT with IoT for health care system sharing framework was determined using two key metrics for evaluation: controlling accessibility and time consumption.

A. Controlling accessibility

As shown in Figure 5, two cases are experimented: unauthorized access and allowed accessibility, to evaluate the BSF-EHR architecture's performance having planned the control for accessibility. The purpose of the BCT-based health-care system is to allow permissioned parties (like insurance agents or doctors) to quickly extract EHRs from the block chain while preventing illegal access to EHR resources.

TABLE I. SUMMARIZATION OF PREDICTION TECHNIQUES WITH PERFORMANCE

Prediction Techniques	Accuracy	Precision	Recall	Specificity
SVM [19]	0.66%	0.63%	0.60%	0.58%
KNN [20]	0.70%	0.69%	0.64%	0.60%
Decision Tree [21]	0.75%	0.70%	0.68%	0.65%
CNN [22]	0.80%	0.77%	0.74%	0.70%
Proposed Capsule Networks	**0.97%**	**0.94%**	**0.93%**	**0.92%**

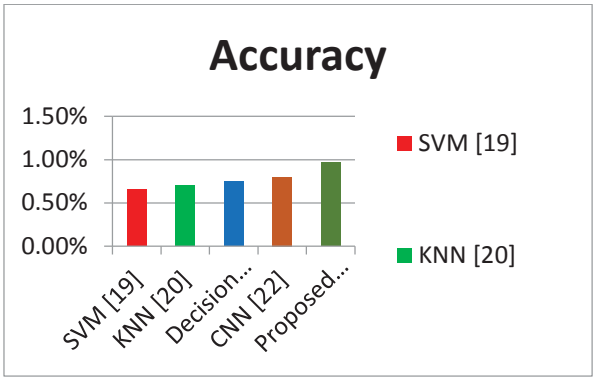

Fig. 5. Average Accuracy Comparison performance of Existing Model with Proposed Model in graphical representation

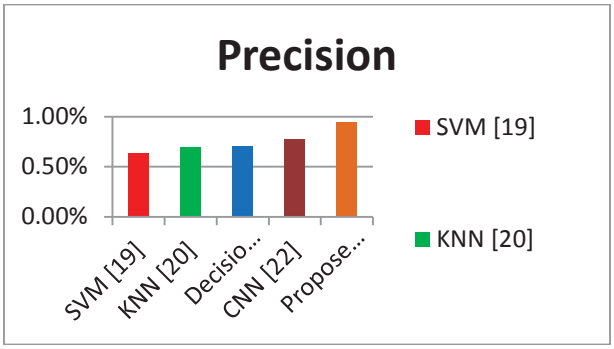

Fig. 6. Average Precision Comparison performance of Existing Model with Proposed Model in graphical representation

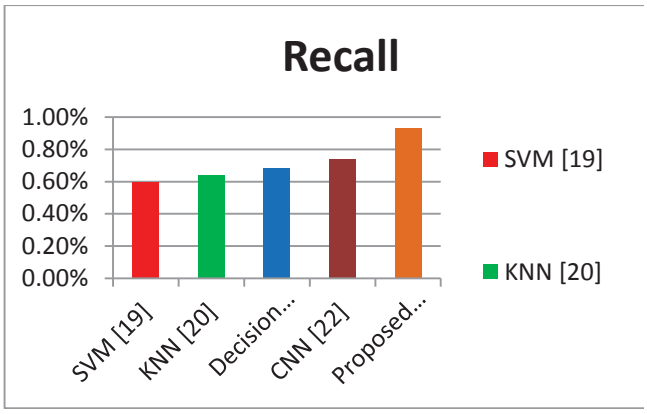

Fig. 7. Average recall comparison performance of existing model with proposed model in graphical representation

TABLE II. SUMMARIZATION OF CPU TIME TEST FOR ALL CLASSIFICATION ALGORITHMS

Prediction Techniques	Running Time (ms)
SVM [19]	4.63 ms
KNN [20]	2.75 ms
Decision Tree [21]	1.19 ms
CNN [22]	0.94 ms
Proposed Capsule Networks	0.19 ms

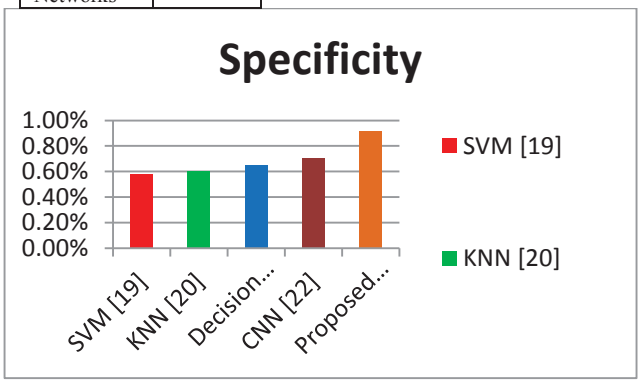

Fig. 8. Average specificity comparison performance of existing model with proposed model in graphical representation

B. Time Consumption

The time consumed for retrieving EHRs on block chain against centralized storage, as illustrated in Figure 6, was used to measure the efficiency of the BSF-EHR framework.

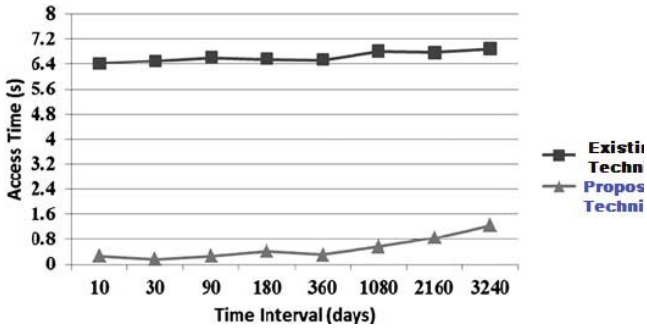

Fig. 9. Comparison of time consumption between centralized storage and BSF-EHR

The time spent by the EHRs access method, from request to receipt, was calculated in this experiment. The procedure for calculating time usage was as follows: EHRs are kept in a centralized server in centralized storage. When a patient requests access to his or her EHR, he or she submits an EHR request. The current time (T1) is then noted, and the person transmits the EHR request to the centralized server. Following the receipt of the patient's EHR request, the centralized server searches for and collects the patient's EHR, which is sent to the patient. After that, we take note of the present time (T2). As a result, the time spent accessing EHR is (T2 T1) seconds. Additionally, time consumption is related to the size of health-care data. The time it takes to obtain health care data is substantial if the EHR is huge. In contrast, if the amount of health care data is modest, the time it takes to obtain it is also small. The amount of time spent varies depending on the magnitude of the health-care data.

V. CONCLUSION

Medical care has become an indispensable aspect of our lives, and medical data, such as medications and previous medical records, has become an essential component of patients' diagnosis and subsequent procedures. Medical data was previously stored on paper, which was easily damaged and altered. As a result, the data had to be saved electronically. The medical information, on the other hand, may be altered with or permanently wiped. Then there was the issue of information censorship. When a body (or) individual has the purpose or not to retrieve data that should not have been observed without the concern of patients or hospitals, information blocking happens. As a result, this study examined how Block Chain and Internet of Things technologies might be used to improve healthcare systems in terms of data security and privacy. Upgraded IoT-based block chain e-healthcare architecture has also been reported for obtaining and administering e-healthcare information of EHR in a trustworthy, secure, transparent, and efficient manner.

REFERENCES

[1] H. Liang, J. Zou, K. Zuo, and M. J. Khan,"An improved genetic algorithm optimization fuzzy controller applied to the well head back pressure control system," Mechanical Systems and Signal Processing, vol. 142, p. 106708, 2020.

[2] R. He, N. Xiong, L. T. Yang, and J. H. Park, "Using multimodal semantic association rules to fuse keywords and visual features automatically for web image retrieval," Information Fusion, vol. 12, no. 3, pp. 223–230, 2011.

[3] Z. Wan, N. Xiong, N. Ghani, A. V. Vasilakos, and L. Zhou, "Adaptive unequal protection for wireless video transmission over IEEE 802.11e networks," Multimedia Tools and Applications, vol. 72, no. 1, pp. 541–571, 2014.

[4] H. Liang, J. Zou, Z. Li, M. J. Khan, and Y. Lu, "Dynamic evaluation of drilling leakage risk based on fuzzy theory and PSO-SVR algorithm," Future Generation Computer Systems, vol. 95, pp. 454–466, 2019.

[5] S. Tanwar, K. Parekh, and R. Evans, "Blockchain-based electronic healthcare record system for healthcare 4.0 applications," Journal of Information Security and Applications, vol. 50, no. 2, p. 102407, 2020.

[6] A. Farouk, A. Alahmadi, S. Ghose, and A. Mashatan, "Blockchain platform for industrial healthcare: vision and future opportunities," Computer Communications, vol. 154, no. 15, pp. 223–235, 2020.

[7] S. Cao, G. Zhang, P. Liu, X. Zhang, and F. Neri, "Cloudassisted secure eHealth systems for tamper-proofing EHR via blockchain," Information Sciences, vol. 485, no. 6, pp. 427– 440, 2019.

[8] T. McGhin, K.-K. R. Choo, C. Z. Liu, and D. He, "Blockchain in healthcare applications: research challenges and opportunities," Journal of Network and Computer Applications, vol. 135, pp. 62–75, 2019.

[9] A. Al Omar, M. Z. A. Bhuiyan, A. Basu, S. Kiyomoto, and M. S. Rahman, "Privacy-friendly platform for healthcare data in cloud based

on blockchain environment," Future Generation Computer Systems, vol. 95, pp. 511–521, 2019.

[10] N. Islam, Y. Faheem, I. U. Din, M. Talha, M. Guizani, and M. Khalil, "A blockchain-based fog computing framework for activity recognition as an application to e-healthcare services," Future Generation Computer Systems, vol. 100, no. 11, pp. 569–578, 2019.

[11] Anand, R., Sindhwani, N., & Saini, A. (2021). Emerging Technologies for COVID-19. *Enabling Healthcare 4.0 for Pandemics: A Roadmap Using AI, Machine Learning, IoT and Cognitive Technologies*, 163-188.

[12] Gupta, A., Anand, R., Pandey, D., Sindhwani, N., Wairya, S., Pandey, B. K., & Sharma, M. (2021). Prediction of Breast Cancer Using Extremely Randomized Clustering Forests (ERCF) Technique: Prediction of Breast Cancer. *International Journal of Distributed Systems and Technologies (IJDST)*, *12*(4), 1-15.

[13] Singh, H., Rehman, T. B., Gangadhar, C., Anand, R., Sindhwani, N., & Babu, M. (2021). Accuracy detection of coronary artery disease using machine learning algorithms. *Applied Nanoscience*, 1-7.

[14] Meivel, S., Sindhwani, N., Anand, R., Pandey, D., Alnuaim, A. A., Altheneyan, A. S., ... & Lelisho, M. E. (2022). Mask Detection and Social Distance Identification Using Internet of Things and Faster R-CNN Algorithm. *Computational Intelligence and Neuroscience*, *2022*.

[15] Singh, H., Ramya, D., Saravanakumar, R., Sateesh, N., Anand, R., Singh, S., & Neelakandan, S. (2022). Artificial Intelligence based Quality of Transmission Predictive Model for Cognitive Optical Networks. *Optik*, 168789.

[16] Juneja, S., Juneja, A., & Anand, R. (2020). Healthcare 4.0-Digitizing Healthcare Using Big Data for Performance Improvisation. *Journal of Computational and Theoretical Nanoscience*, *17*(9-10), 4408-4410.

[17] R. Park, E. Lee, W. Na, S. Park, Y. Lee, and J.-H. Lee, "Is blockchain technology suitable for managing personal health records? mixed-methods study to test feasibility," J Med Internet Res, vol. 21, p. e12533, 2019.

[18] A. Roehrs, C. A. da Costa, and R. da Rosa Righi, "Omniphr: A distributed architecture model to integrate personal health records," Journal of Biomedical Informatics, vol. 71, pp. 70–81, 2017.

[19] A. Cernian, B. Tiganoaia, I. Sacala, A. Pavel, and A. Iftemi, "Patientdatachain: A blockchain-based approach to integrate personal health records," Sensors, vol. 20, p. 6538, Nov 2020.

[20] A. R. Rajput, Q. Li, M. Taleby Ahvanooey, and I. Masood, "Eacms: Emergency access control management system for personal health record based on blockchain," IEEE Access, vol. 7, pp. 84 304–84 317, 2019.

[21] N. B. Truong, K. Sun, G. M. Lee, and Y. Guo, "Gdpr-compliant personal data management: A blockchain-based solution," IEEE Transactions on Information Forensics and Security, vol. 15, pp. 1746–1761, 2020.

[22] B. Alamri, I. T. Javed, and T. Margaria, "Preserving patients' privacy in medical iot using blockchain," in Edge Computing. Springer, 2020, pp. 103–110