International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
DOI: https://doi.org/10.17762/ijritcc.v11i9.8335
***Article Received:** 10 July 2023 **Revised:** 08 September 2023 **Accepted:** 21 September 2023*

Developed A Hybrid Optimal Feature Vector Selection with Blockchain Technology for Smart Healthcare 4.0

Gunanidhi G S[1], P.Selvi Rajendiran[2]
[1]School of Computing Sciences
Hindustan Institute of Technology and Science
Padur,India
gsgunanidhi.03@gmail.com
[2]School of Computing Sciences
Hindustan Institute of Technology and Science
Padur,India
selvir@hindustanuniv.ac.in,

Abstract— The health economy has been an innovative technology since time-honored. Preserving and maintaining patient data are essential in a routine life. Patient's medical information is very important for every individual not only for patients but also for doctors who are examining them. Advances in sensing technology, processing of data, and communication protocols have transformed the healthcare industry. Patients, physicians, hospitals, and other stakeholder may keep vital data and medical records with the use of electronic healthcare records (EHR). The goal of research should be to develop a Hybrid Optimal Feature Vector Selection with Blockchain Technology (HOFVS-BT) for smart healthcare 4.0 to improve the secure transmission of data which is supported intelligent IoT and medical detection platform possible. For Feature vector selection, proposed an Orthogonal Wolf Optimization (OWO) algorithm. Furthermore, safeguarding private patient details is taken into account by establishing an upgraded Blockchain-based IoT data security solution that not only secures the data, but also fosters trust between patients/users and healthcare service providers.

Keywords- Blockchain, Orthogonal Wolf Optimization, IOT, Data Security, HOFVS-BT Blockchain, Orthogonal Wolf Optimization, IOT, Data Security, HOFVS-BT.

I. INTRODUCTION

Despite the rapidly expanding deployment of IoT and connectivity, information continues to be a top goal for achieving smart healthcare in a city that is smart. The Internet of Medical Things (IoMT) is a new trend that offers a variety of effective and efficient solutions for the patients and healthcare practitioners for the treatment of various ailments. Internet of things (IoT) technology have become commonplace in the healthcare industry. Because of the growing need for IoT, a vast amount of patient data is being collected and used for diagnostic reasons [1].

The primary challenges that are currently faced by healthcare observing frameworks include the following: reducing the risk of exposure due to the highly confidential nature of health data; restricting delay, especially with delay-sensitive conditions such as unanticipated coronary artery disease; establishing health situations in an effective and precise manner while associated to physical signs as well as surroundings data [2]; and limiting the latency for delay-sensitive diseases like unexpected heart disease.

The electronic healthcare monitoring system has played a critical role in the management of monitoring the health care. E-health can offer operative and helpful monitoring services for patients [3]. However, there are security concerns in the present E-Health system. In contrast, the present e-health system includes security flaws [4]. The technology of Blockchain is an unmistakable record system that maintains activities in high-security blocks chain. Blockchain has the potential to tackle safety and privacy challenges in a wide range of areas [5]. With the fast growth of smart atmospheres and complex contracts among users and strategies with intelligence, federated learning (FL) is a new pattern for improving data mining accuracy and precision by supporting information privacy and security [6].

As it provides novel and increased features in the smart health care framework, a smart gadget contains a large quantity of sensitive patient data.

Furthermore, healthcare system components are networked through the Internet, resulting in substantial changes in the establishment of healthcare facilities to people [7]. With the extraordinary advancement of internet technology, the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
DOI: https://doi.org/10.17762/ijritcc.v11i9.8335
***Article Received:** 10 July 2023 **Revised:** 08 September 2023 **Accepted:** 21 September 2023*

acceptance of smart healthcare has consistently risen. Smart healthcare employs new technology to completely replace the existing medical system, providing healthcare more effective, convenient, and personalized [8].

The transfer of emerging technical invention in the direction of e-Health is a global significance for guaranteeing people's quality of life [9]. As a result, safe sharing and analysis of medical data across various organizations will improve the effectiveness of e-Health schemes in addressing medical occurrences such as epidemics and serious patient problems. AI programmes are used in diagnostic processes, treatment protocol creation, patient monitoring, medication discovery, personalized medicine in healthcare, and epidemic prediction in global health [10].

II. RELATED WORKS

In order to provide precise medical care to patients, a medical facility located in a future smart city will need data security and confidentiality. This strategy is not very outstanding due to the fact that protecting the confidentiality of patients' medical information is an essential component of providing medical care.

The framework that has been developed takes into consideration the recommendations of specialists from many different medical facilities in order to provide patients with the most appropriate treatment. Internet of Medical Things (IoMT) based Cyber-Physical Systems (CPS) play a key part in the age of smart healthcare, which involves accessing, monitoring, evaluating, and prescribing patients in a ubiquitous manner. Maintaining credibility among customers, healthcare professionals, pharmacologists, and any other linked organizations requires addressing the significant challenges posed by these networks, the most important of which are the need for efficient authentication and safe data transfer.

In this paper [11], In this architecture, Blockchain-based IoT cloud platforms are used for the purposes of ensuring both security and privacy. The IoMT does have quite a few advantages; yet, there is still the problem of maintaining its security [12]. The usage of IoMT is put in a precarious position since inexperienced users of IoMT often have poor security knowledge, and there is a possibility that several intermediate assaults might be used to get access to private health information. Blockchain technology, which is a decentralized architecture that is now in widespread use, was recently created to achieve security. In light of this purpose, the study [13] presents a novel model for the safe transfer and diagnosis of medical data using blockchain technology that is supported by deep learning.

A data collecting layer, a diagnostic and security layer (edge cloud), and a health service layer are included in the framework [14]. Recent years have seen the emergence of block-chain technology as one of the most effective strategies in the privacy and security industries [15]. Block of patient information sent to several different medical facilities.

Each treatment centre has the ability to provide a recommendation on the suggested mode of therapy and blockchain attachment, and then transmit that recommendation to the other treatment centres and nodes [16].

IoT should be composed and acquired to train and check in a high possible privacy and protected way [17]. This includes smart city, smart healthcare, and smart industrial. The use of blockchain technology to the development of intelligent learning has the potential to have an impact on the preservation and upkeep of information security and privacy. The decentralized authentication of valid patient wearable devices for the purpose of characteristics of patient wearable devices [18]. Furthermore, a significant number of varied devices store data in a variety of sizes and setups, which makes it difficult to succeed the data in the healthcare source and protect it from aggressors that want to make money off of the data [19].

The basic perspective of the proposed system is presented in this study [20], IoT is prepared to play a significant role in all aspects of the healthcare business [21], thanks to rapid advancements in the configuration of IoT devices and an increasing desire to make medical treatment more financially smart, customized, and proactive. This article [22] gives a detailed assessment on state-of-the-art strategies for on how these techniques might be used to protect sensitive patient information.

Using the power of blockchain technology and an online intelligent decision-making RL algorithm, the health chain-RL framework [23] that was presented combines several types of healthcare organizations, each of which has varied needs. This is accomplished while still maintaining an optimized framework [24]. The design makes use of the Blockchain technology so that users' data may be kept private and secure. Wearable medical gadgets are used in the process of continually monitoring an individual's health state and storing this information in the cloud [25].

III. PROPOSED METHODOLOGY

IoT devices such as wearables, sensors, and other medical devices can collect real-time data on patient health and transmit it securely to the blockchain network. This data can be encrypted and stored in a tamper-proof manner, ensuring patient privacy and security. Smart contracts can be used to automate

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
DOI: https://doi.org/10.17762/ijritcc.v11i9.8335
Article Received: *10 July 2023* ***Revised:*** *08 September 2023* ***Accepted:*** *21 September 2023*

and enforce rules for data access and usage, ensuring that patient data is only accessed by authorized parties.

Private data were shared via the Orthogonal Wolf Optimization (OWO) algorithm in feature vector selection model. OWO stands for population-based optimization method in this context. OWO was supplied with an arbitrary collection of objects and searches for the optimal outcomes. Every component in the search area was given a position-based distance from the associated perfect situation and a range from the wolf's ideal component.

3.1 BC Technology

BC technology is utilized to facilitate safe interactions in IoT networks. BC technology is a decentralized network of peers in which every activity is validated and recorded in a distributed and immutable ledger by a registered node. The consensus technique ensures the network's integrity. In particular, there is no centralized authority in this system to verify the generated event: each and every transaction must be validated by the BC node via collaboration (consensus). Here are some examples of common sorts of agreements.

A blockchain is a database or ledger of digital transactions that are stored in blocks and connected in a chronological chain. Each block contains a cryptographic hash that links it to the previous block, creating a permanent and unalterable record of all transactions as shown in fig 1. This makes blockchain a secure and transparent way to store data and conduct transactions, as each block in the chain is verified and validated by a network of nodes, rather than a single central authority.

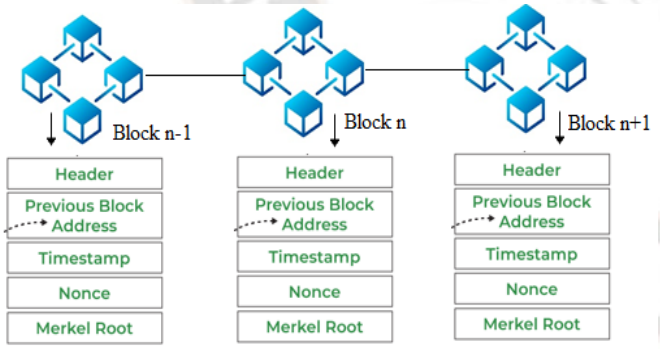

Figure. 1: Working of Block chain

3.2 Blockchain-Enabled Medical System in IOT Environment

Figure 2 shows an example of the blockchain scheme to process healthcare data, where different kinds of data archives, including data regarding mobile clinics, life insurance, family medical histories, and doctor's prescriptions, are gathered in the blockchain server on the cloud. Such data can be accessed by licensed medical professionals, patients, and academics with the patient's consensus.

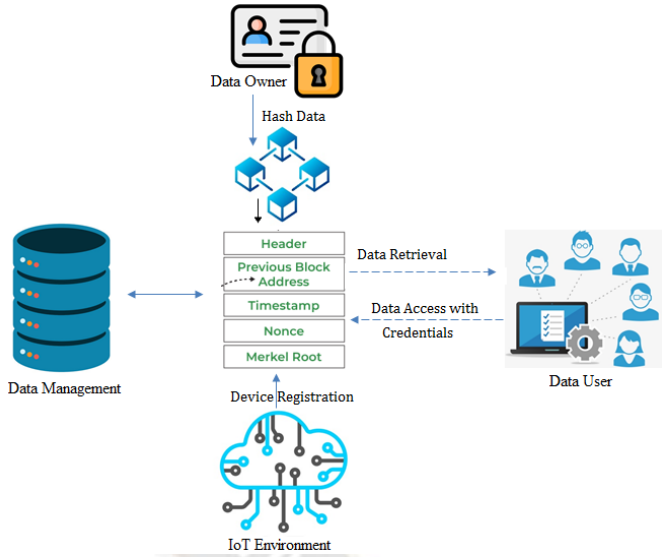

Figure. 2: Blockchain in Medical IoT

Permissioned parties (such as hospitals and government institutions) operate hybrid and encrypted blockchains. Secret health-care data is stored on-site and managed by trustworthy hospitals, labs, or other comparable entities. Patients regain control of their health-care data, and they may allow clinics, research institutions, and insurance to use it for certain interval periods and monitored on distributed ledgers that are visible, immutable, and traceable using a popular agreement consensus system.

All participants are integrated to create a whole healthcare network in the proposed framework.

i) User Registration: The user registration process within the blockchain-enabled healthcare system begins when the healthcare user wants to register for the first time. User registration involves three steps: submitting a transaction proposal, verifying the transaction, and updating the blockchain after successful verification. The steps involved in user registration are summarized as follows:

- Using the application interface, new healthcare user submits transactions to Blockchain middleware.
- The application interface uploads user data and transactions to blockchain middleware using smart contracts.
- The consensus algorithm decodes transactions through blockchain middleware and extracts the user's public key and user ID.
- Middleware calculates the hash value of a registered user and then publishes it on a private blockchain network for tracking purposes.

Steps for user registration process in the proposed system:

1. Application for user's registration.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
DOI: https://doi.org/10.17762/ijritcc.v11i9.8335
Article Received: 10 July 2023 Revised: 08 September 2023 Accepted: 21 September 2023

2. Submit transaction proposal for registration along with user's details.
3. Execute consensus algorithm.
4. If consensus successful then update blockchain record.
5. If consensus failed, then return error.
6. If consensus successful, generate user's portal.
7. Issue medical account to user.

ii) Access Control: This process facilitates the users to access their medical records. Access Control is a three-step process that prompts transactions with user information, verifies users, and gives them access to medical records after completing the verification process. The main steps of the access control process are highlighted as follows:

- A healthcare user prepares an access control request involving a target user ID.
- Using the application interface, each healthcare user submits transactions to Blockchain middleware.
- The application interface uploads user data and transactions to blockchain middleware using smart contracts.
- The consensus algorithm decodes transactions through blockchain middleware and gets the user's public key and ID.
- Middleware authenticates the private key of a registered user and then unlocks the user account on a private blockchain network.

Steps for access control process in the proposed system:

1. Application for user authentication.
2. Submit transaction proposal for authentication along with login details.
3. Execute consensus algorithm.
4. If consensus successful then update block chain record.
5. If consensus failed, then return error.
6. If consensus successful, unlocks user's account.
7. Issues account to user.

3.3. HYBRID FEATURE VECTOR SELECTION MODEL

In modern years, hybrid algorithms have gained a lot of attention when it comes to tackling optimisation difficulties. Hybrid algorithms combine several algorithms to create a new or better algorithm that can tackle more difficult optimisation issues.The problem of feature selection has been addressed through the use of hybrid algorithms to find an appropriate data. It is possible to combine the benefits of other methods when using the hybrid feature selection approach. As a result of the hybrid scheme that incorporates numerous algorithms, there is a significant increase in the likelihood of obtaining an ideal answer quickly and efficiently. Furthermore, hybrid algorithms can be created by combining the best features of several algorithms. As a result, the hybrid method may significantly limit the search space for the subset as shown in fig 3.

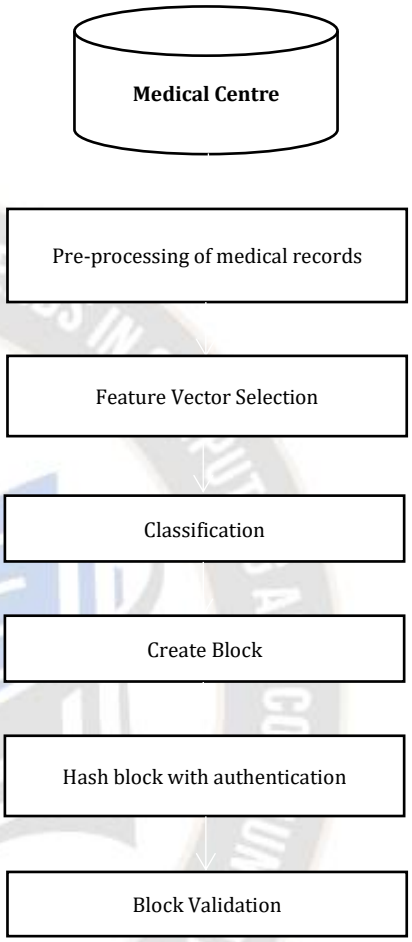

Figure. 3: Flow Diagram of Proposed Model

Algorithm:

Step 1: Population P initialized and parameters a, 8

Step 2: do while

Determine fitness function values Pbest (1)

Identify the best solution achieved

Step 3: for x ranges from 1 to N

Average value of the present solution P(r) is updated

Modify the value x, y, H_1, H_2, Levy(R)

if r<= (2/3) then

if random 0.5 then

Expanding (P1)

Current solution updated by using Equation 4.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
DOI: https://doi.org/10.17762/ijritcc.v11i9.8335
Article Received: *10 July 2023* ***Revised:*** *08 September 2023* ***Accepted:*** *21 September 2023*

if Fitness (Pi (r+1)) < Fitness (P(r)) then

P(r) (P(+1))

if Fitness (P, (r+1)) < Fitness (Post (1)) then

Pbest (r) = P(+1)

end

end

else

Step 4: return the value

An important aspect of an algorithm is the definition of a feature vector with n components. There is no feature selection in the features vector, because all of the features are set to zero and one, respectively, indicating that there is no feature selection.

$$X_i = \ll X_i^1, X_i^2, X_i^3, , X_i^n \quad (1)$$

Xi is a feature vector in this equation 1. It is important to note that Xji is a feature vector with component i and component j. Each feature vector is made up of n components. In the present repetition or t, a feature vector is supposed to be X(t). It is expected that this feature vector will be included $X(t+1)$ during the next phase of the development process. In Eq. (2), the suitable goal purpose for feature assortment is defined:

$$f = \alpha.\frac{1}{n}\sum_{i=1}^{n} |\bar{y}_i - Y_i| + \beta.\frac{F}{A} \quad (2)$$

The actual assessment and forecast value of a sample are presented in the objective function using Yi and Yi, respectively. The number of samples is specified by the parameter n. The values F and A represent the characteristics that were chosen and the total number of features that may be chosen. The OWO algorithm is used to minimize this vector. This method attempts to update the feature vectors in each iteration. The algorithm of OWO then chooses the best feature vector and minimizes the importance of the impartial function.

$$X(t+1) = \begin{cases} X_{rand}(t) - r_1|X_{rand}(t) - 2r_2.X(t)| \; rand \geq 0.5 \\ \left(X_{rabbit}(t) - X_m(t)\right) - r_3\left(LB + r_4(UB - LB)\right) \; rand < 0.5 \end{cases} \quad (3)$$

In the problem space of a feature vector, the value of Xrandt can be roughly translated to a random point. A point of gravity or a mean of the characteristic vectors is which is represented by the value of XMt, whereas r1, r2, r3, and r4 are uniform random integers between zero and one.

$$X(t+1) = \begin{cases} X(t) - r_1|X(t) - 2r_2.X(t)| \; rand \geq 0.5 \\ \left(X(t) - X_m(t)\right) - r_3.r_4 \; rand < 0.5 \end{cases} \quad (4)$$

$$X(t+1) = \left(X(t) - X(t)\right) - E|J.X(t) - X(t)| \quad (5)$$

A diminishing component in iteration is the coefficient E, also called energy measurement. Another sort of update is connected to update feature vectors, as illustrated in Eq. (6):

$$X(t) = X(t) - E|X(t+1) - X(t+1)| \quad (6)$$

OWO algorithms can modernize each feature vector based on average population locations or population centres of gravity, as shown in Eq. (7):

$$X(t) = X(t+1) - E|J.X(t) - X_m(t)| \quad (7)$$

The most optimum feature vector is used in the last iteration to minimize illness diagnosis error. The objective function assesses illness diagnosis error and quantity of features based on random states of the ideal feature vector.

IV. RESULTS AND DISCUSSIONS

The HOFVS-BT framework was validated using a performance database in Python 3.6.5 on a PC with 16 GB OS memory, 4 GB RAM, 250 GB SSD document sharing, i5-8600 k computer, a GeForce 1050Ti graphics card, and a 1 TB HDD. It is made up of 900 photos organized into three categories, to 300 images: benign, malignant, and normal. The following would be the variable setup for the proposed model. The sample size was 30, and the gradient descent is 0.001. 100 input nodes, 50 hidden layers, 0.5 mean reactivation, 0.0001 weight decay, 100 particle shape, 0.9–0.4 inertia value In furthermore, the database was separated into training and validation halves to fivefold classification technique. The patient can view their record in the EHR system and safely use it for the rest of their lives. The patient is given the secret key, which can be used to access the results later.

4.1 Evaluating Fitness

To represent the feature selection issue in this research, a multi-objective optimisation technique is adopted. The goal is to acquire a subset of characteristics with fewer features while attempting to attain greater classification accuracy. As the fitness function, this study produces the following formula using the multi-objective optimisation model mentioned above. The fitness function building approach is also commonly used to assess the quality of feature subsets.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
DOI: https://doi.org/10.17762/ijritcc.v11i9.8335
Article Received: *10 July 2023* ***Revised:*** *08 September 2023* ***Accepted:*** *21 September 2023*

$$fitness = \omega \times E_r + (1 - \omega) \times \left(\frac{p}{q}\right) \qquad (8)$$

Among them, (0, 1) is a specific real number. Er stands for the error rate classification. It is produced by having an evaluator (often a classifier) evaluate this subset of characteristics.

4.2 Service Execution Time

The total amount of time is required to process and verify all transactions through the Blockchain framework. Execution time is calculated based on the number of transactions, and the experiments and execution time evaluation as shown in fig 4. The user registration procedure consists of three main operations: submitting a proposal, transactional confirmation, and blockchain update following successful consensus.

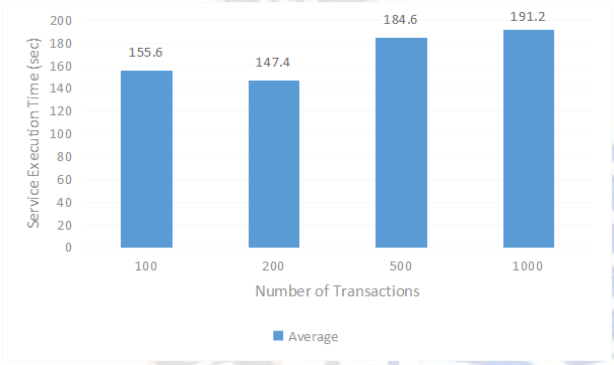

Figure. 4: Service processing time for the user registration procedure

The service execution time for user access control operation through the proposed framework was analysed. This is also a three-step procedure that includes submitting a proposal with user information, verifying the user, and giving them with access to medical data following successful authentication. Again, the size of transaction groups is maintained as shown in fig 5.

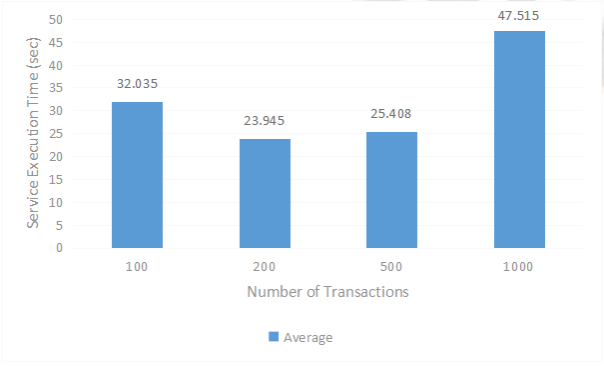

Figure. 5: Service execution time for an access control process

4.3 Transaction Throughput

The transaction throughput represents the number of transactions completed per second based on the time and place of the transaction as shown in fig 6. Transaction throughput is a cycle of processing and verifying all requests through the blockchain framework. Users are categorized into four groups of transactions such as 100, 200, 500, and 1000.

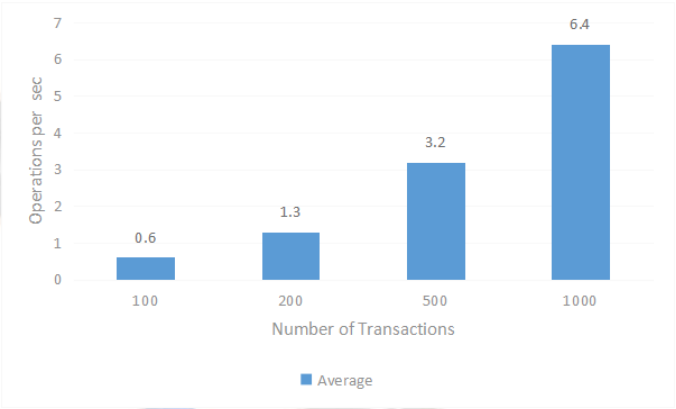

Figure. 6: A comparison of transaction throughput for the user registration process

The mean user-perceived latency of the proposed and existing shard-blockchain systems are shown in fig 7.

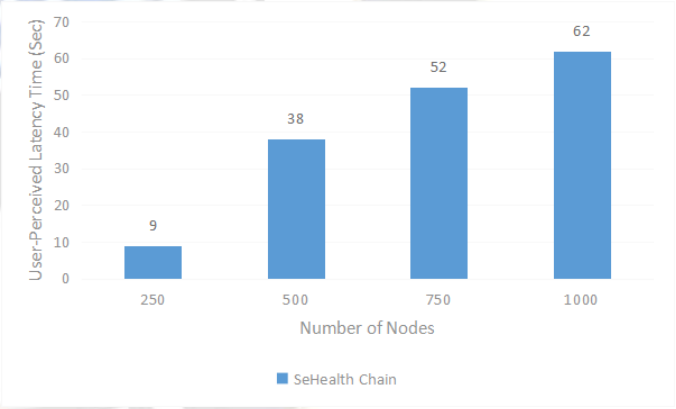

Figure. 7: Latency Time

	100 B	1 KB	10 KB	100 KB	1 MB	10 MB	100 MB	1 GB
Generation of Sibling path	**0.0020**	**0.0028**	**0.06**	**0.08**	**0.01**	**0.02**	**0.02**	**0.05**
Authentication	**0.0012**	**0.0041**	**0.09**	**0.01**	**0.02**	**0.02**	**0.20**	**0.03**

Table I: Calculation time (in milliseconds) on average for authentication using Merkle trees, sorted by data size

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
DOI: https://doi.org/10.17762/ijritcc.v11i9.8335
***Article Received:** 10 July 2023 **Revised:** 08 September 2023 **Accepted:** 21 September 2023*

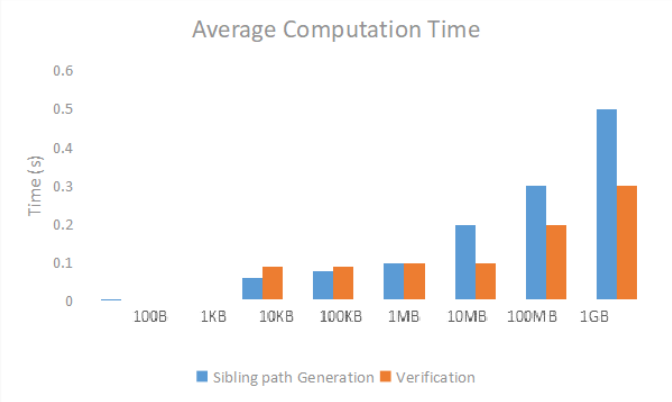

Figure. 8: Average Computational Time

The durations of the average computation time of processes are represented by the sibling path generation and verification methods respectively as shown in fig 8. OWO for secure communication, an excellent hash code decryption methodology, and parameter estimation of the HOFVS-BT model, the proposed approach surpassed the existing techniques.

V. CONCLUSION

Privacy is a critical issue when it comes in smart cities, big data is being used to improve health and be processed. Blockchain technology appears to be extremely distributive, according to our research. The Internet of Things is well suited to this technology. This problem can be handled to a considerable part using blockchain technology. In this study, a mechanism for protecting patient privacy using blockchain technology is being developed. The goal of research should be to develop a Hybrid Optimal Feature Vector Selection with Blockchain Technology (HOFVS-BT) for smart healthcare 4.0 to improve the secure transmission of data which is supported intelligent IoT and medical detection platform possible. An Orthogonal Wolf Optimization (OWO) technique was presented for feature vector selection. Additionally, patients' private information is protected by using an improved Blockchain-based IoT data security approach.

REFERENCES

[1] Vaiyapuri, T., Binbusayyis, A., & Varadarajan, V. (2021). "Security, privacy and trust in IoMT enabled smart healthcare system: a systematic review of current and future trends". International Journal of Advanced Computer Science and Applications, 12(2).

[2] Al-Shammari, N. K., Syed, T. H., & Syed, M. B. (2021). "An Edge–IoT framework and prototype based on blockchain for smart healthcare applications". Engineering, Technology & Applied Science Research, 11(4), 7326-7331.

[3] Bharimalla, P. K., Choudhury, H., Parida, S., Mallick, D. K., & Dash, S. R. (2021). "A Blockchain and NLP Based Electronic Health Record System": Indian Subcontinent Context. Informatica, 45(4).

[4] Iwendi, C., Anajemba, J. H., Biamba, C., & Ngabo, D. (2021). "Security of things intrusion detection system for smart healthcare". Electronics, 10(12), 1375.

[5] Srinivasu, P. N., Bhoi, A. K., Nayak, S. R., Bhutta, M. R., & Woźniak, M. (2021). "Blockchain technology for secured healthcare data communication among the non-terminal nodes in IoT architecture in 5G network". Electronics, 10(12), 1437.

[6] Kaushal, R. K., Bhardwaj, R., Kumar, N., Aljohani, A. A., Gupta, S. K., Singh, P., & Purohit, N. (2022). "Using Mobile Computing to Provide a Smart and Secure Internet of Things (IoT) Framework for Medical Applications". Wireless Communications and Mobile Computing, 2022.

[7] Shinde, R., Patil, S., Kotecha, K., Potdar, V., Selvachandran, G., & Abraham, A. (2022). "Securing AI-based Healthcare Systems using Blockchain Technology": A State-of-the-Art Systematic Literature Review and Future Research Directions. arXiv preprint arXiv:2206.04793.

[8] Zellar, P. I. . (2021). Business Security Design Improvement Using Digitization. International Journal of New Practices in Management and Engineering, 10(01), 19–21. https://doi.org/10.17762/ijnpme.v10i01.98

[9] Namasudra, S., & Sharma, P. (2022). "Achieving a decentralized and secure cab sharing system using blockchain technology". IEEE Transactions on Intelligent Transportation Systems.

[10] Teimoori, Z., Yassine, A., & Hossain, M. S. (2022). "A secure cloudlet-based charging station recommendation for electric vehicles empowered by federated learning". IEEE Transactions on Industrial Informatics, 18(9), 6464-6473.

[11] Kumar, R., Singh, D., Srinivasan, K., & Hu, Y. C. (2022, December). "AI-Powered Blockchain Technology for Public Health: A Contemporary Review, Open Challenges, and Future Research Directions". In Healthcare (Vol. 11, No. 1, p. 81). MDPI.

[12] Singh, S., Rathore, S., Alfarraj, O., Tolba, A., & Yoon, B. (2022). "A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology". Future Generation Computer Systems, 129, 380-388.

[13] Kumar, M., Verma, S., Kumar, A., Ijaz, M. F., & Rawat, D. B. (2022). "ANAF-IoMT: A Novel Architectural Framework for IoMT-Enabled Smart Healthcare System by Enhancing Security Based on RECC-VC". IEEE Transactions on Industrial Informatics, 18(12), 8936-8943.

[14] Neelakandan, S., Beulah, J. R., Prathiba, L., Murthy, G. L. N., Irudaya Raj, E. F., & Arulkumar, N. (2022). "Blockchain with deep learning-enabled secure healthcare data transmission and diagnostic model". International Journal of Modeling, Simulation, and Scientific Computing, 13(04), 2241006.

[15] Hu, J., Liang, W., Hosam, O., Hsieh, M. Y., & Su, X. (2022). "5GSS: a framework for 5G-secure-smart healthcare monitoring". Connection Science, 34(1), 139-161.

[16] Ghazal, T. M., Hasan, M. K., Abdullah, S. N. H. S., Bakar, K. A. A., & Al Hamadi, H. (2022). "Private blockchain-based encryption framework using computational intelligence approach". Egyptian Informatics Journal, 23(4), 69-75.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
DOI: https://doi.org/10.17762/ijritcc.v11i9.8335
***Article Received:** 10 July 2023 **Revised:** 08 September 2023 **Accepted:** 21 September 2023*

[17] Al-Safi, H., Munilla, J., & Rahebi, J. (2022). "Patient privacy in smart cities by blockchain technology and feature selection with Harris Hawks Optimization (HHO) algorithm and machine learning". Multimedia Tools and Applications, 81(6), 8719-8743.

[18] Li, D., Luo, Z., & Cao, B. (2022). "Blockchain-based federated learning methodologies in smart environments". Cluster Computing, 25(4), 2585-2599.

[19] Adil, M., Khan, M. K., Jadoon, M. M., Attique, M., Song, H., & Farouk, A. (2022). "An AI-enabled hybrid lightweight Authentication scheme for intelligent IoMT based cyber-physical systems". IEEE Transactions on Network Science and Engineering.

[20] Alabdulatif, A., Khalil, I., & Saidur Rahman, M. (2022). "Security of Blockchain and AI-Empowered Smart Healthcare: Application-Based Analysis". Applied Sciences, 12(21), 11039.

[21] Amponsah, A. A., Adekoya, A. F., & Weyori, B. A. (2022). "Improving the financial security of national health insurance using Cloud-based blockchain technology application". International Journal of Information Management Data Insights, 2(1), 100081.

[22] Kshirsagar, D. P. R. ., Patil, D. N. N. ., & Makarand L., M. . (2022). User Profile Based on Spreading Activation Ontology Recommendation. Research Journal of Computer Systems and Engineering, 3(1), 73–77. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/45

[23] Tunc, M. A., Gures, E., & Shayea, I. (2021). "A survey on iot smart healthcare: Emerging technologies, applications, challenges, and future trends". arXiv preprint arXiv:2109.02042.

[24] Singh, A. K., Anand, A., Lv, Z., Ko, H., & Mohan, A. (2021). "A survey on healthcare data: a security perspective". ACM Transactions on Multimidia Computing Communications and Applications, 17(2s), 1-26.

[25] Al-Marridi, A. Z., Mohamed, A., & Erbad, A. (2021). "Reinforcement learning approaches for efficient and secure blockchain-powered smart health systems". Computer Networks, 197, 108279.

[26] Fetjah, L., Azbeg, K., Ouchetto, O., & Andaloussi, S. J. (2021). "Towards a smart healthcare system: an architecture based on IoT, blockchain, and fog computing". International Journal of Healthcare Information Systems and Informatics (IJHISI), 16(4), 1-18.

[27] Chattu, V. K. (2021). "A review of artificial intelligence, big data, and blockchain technology applications in medicine and global health". Big Data and Cognitive Computing, 5(3), 41.