**International Journal of Data Informatics and Intelligent Computing (IJDIIC)**
Vol.2, No.2, June 2023, pp. 63~71
DOI: 10.59461/ijdiic.v2i2.59

# IoT-Based Secure Healthcare Framework Using Blockchain Technology with A Novel Simplified Swarm-Optimized Bayesian Normalized Neural Networks

**Shivi Chaturvedi**[1]
[1]Computer Science and Engineering, GCRG Group of Institutions, Lucknow, Uttar Pradesh, India

**Article Info**

***Article history:***

Received May 19, 2023
Revised June 19, 2023
Accepted June 22, 2023

***Keywords:***

Internet of Things (IoT)
healthcare sector
blockchain technology
simplified swarm-optimized
Bayesian normalized neural
networks (SSO-BNNN)

**ABSTRACT**

The Internet of Things (IoT) is growing in popularity nowadays and has many potential uses, particularly in healthcare. A large amount of sensing data is generated from a variety of sensing devices as a result of the growing needs of the IoT. The use of artificial intelligence (AI) methods is crucial for real-time, scalable, and accurate data processing. However, there are certain obstacles in the way of the layout and implementation of a successful analysis of the big data approach. These include a lack of suitable training data, resource limits, and a centralized architecture for the data. However, emerging blockchain technology provides a distributed system. It is advocated for getting rid of centralized control and solving AI issues, and it allows for safe data and resource exchange across the many nodes of the IoT network. Thus, this research develops a novel simplified swarm-optimized Bayesian normalized neural network (SSO-BNNN) for the secret transmission of medical images to address the aforementioned challenge. The neighborhood indexing sequence (NIS) approach is also used to encrypt the hash value. Several experiments were conducted to verify the outcomes of the suggested approach, and several facets of those results are discussed. Experimental results show that the proposed excellent findings with the best accuracy, sensitivity, and specificity were produced by the model.

*This is an open-access article under the CC BY-SA license.*

***Corresponding Author:***

Shivi Chaturvedi
Computer Scince and Engineering
GCRG Groupof Institutions
Lucknow
Uttar Pradesh , India
Email: shivi.chaturvedi@gmail.com

## 1. INTRODUCTION

The Internet of Things (IoT)-based medical applications of today have advanced to the point where any user may get medical services instantly. One of them, known as remote patient management (RPM), entails a variety of uses for therapy, including regular signal monitoring utilizing implanted sensors, Heart Failure detection, fall screening, frequent oxygenation, tracking of expectant mothers, chemotherapy response monitoring, glucose level management, and so on [1]. Nevertheless, because of its lack of stability, fault tolerance, and security, this model is not as frequently utilized as it might be. Medical IoT tools are used in e-health applications to collect the health of the patient data, which is subsequently sent to where it might be accessible by hackers or attackers are edge or cloud units and cause security problems. At times, particularly when managing a huge volume of specialized contacts, the systems are quite susceptible. Cyberattacks such as ransomware, denial of service (DoS), and many others may significantly disrupt medical services and diminish the efficacy of conventional e-Health models [2]. The IoT healthcare

applications growth stage, which is connected to the whole linked healthcare system and spans the years 2017 to 2022, is accelerating the healthcare sectors and many stakeholders who are ramping up their efforts.Therefore, there is little doubt that IoT affects the healthcare sector by drastically altering how people live, the applications, and the equipment used in healthcare solutions are connected to one another [3]. IoT-based secure healthcare systems that make use of different security and privacy techniques, such as access control, encryption, and authentication, have been presented in a number of research studies and articles as solutions to these problems. These systems seek in order to assure the security, integrity, and accessibility of patient data while enabling secure and dependable communication between medical equipment, healthcare professionals, and patients [4]. Figure 1 describes the structure of the blockchain model.

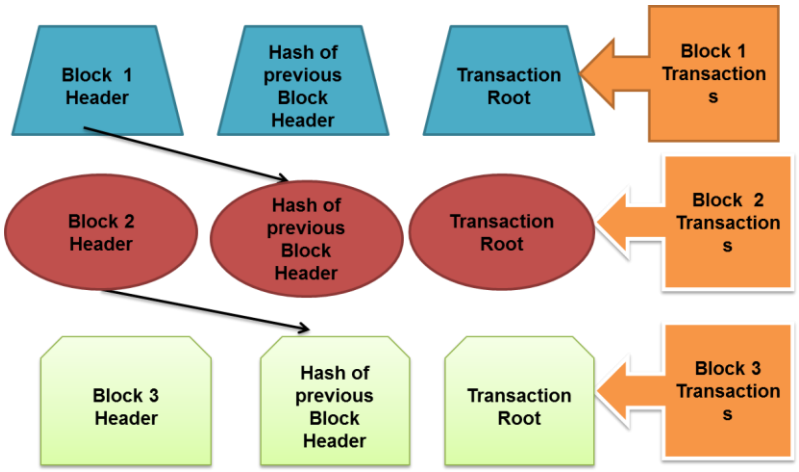


Figure 1. Structure of the Blockchain model

The whole administration of access, transactions, and storage was recently taken over by technology with the introduction of Blockchain. Additionally, blockchain has shown immense potential and hold across a variety of industries, including retail, supply chain management, finance, healthcare, and others. As data is often used by several stakeholders for pursuing different objectives, privacy, and security of the data are the main problems that arise in healthcare [5]. Blockchain technology can store and process patient data across a fog or cloud, doing away with the necessity for centralized fog or cloud authentication. Many developers have been motivated by blockchain technology to create privacy-preserving e-Health modules [6]. Developed a patient agent (PA) that resides in a smart gateway and can assess the user's memory, permissions, and security while uploading their medical information to a unique blockchain.

The other sections of the essay are as follows: section 2 describesrelated works, section 3 presents the suggested method, section 4 result and discussion, and section 5 concludes the paper.

## 2. RELATED WORKS

The paper [7]identified the IoT network intrusion. Initially, a blockchain-based method was used to build the protection of privacy. Due to the value and significance of patient health records (PHR), the “Internet of Medical Things (IoMT)” in particular, the security of PHR is the most important feature of cryptography over the Internet. The “Wireless Body Area Network (WBAN)” based IoTthe current network architecture and application advances for IoT-based healthcare solutions are reviewed in this article together with the healthcare system. Additionally, this article explores the security and privacy characteristics, which include real-time wireless health monitoring, energy, power, authentication, privacy,Quality of Services, and resource management which are highly challenging in many IoT healthcare systems [8]. The study [9] developed an effective “Lightweight Integrated Blockchain (ELIB)” model to address IoT requirements. The deployed model is used inside a smart house setting as a crucial example to confirm its suitability in different IoT situations. For a smart home's limited resources, a central manager that generates shared keys for data transmission and manages all incoming and outgoing requests is advantageous. Excellent customer service, availability, and ease of use are lacking in the current healthcare system. Blockchain technology has been demonstrated to be relevant in almost every area because of its advantages including crypto-security, transparency, data integrity, and a decentralized data network. In the modern world, a blockchain-based smart healthcare system offers transparency, quick and easy access, privacy, dependability, and more [9].The study [10], suggested big data and its use in healthcare applications are briefly introduced. It has been noted that the healthcare industry's rapid data development is being managed with the help of big data architecture and approaches. Here, empirical research is first conducted to examine the function of big data in the healthcare

sector. The study [11] used blockchain technology to secure Internet of Things (IoT) systems based on remote patient monitoring. And the advantages of adopting IoT devices for remote patient monitoring as well as the practical challenges that may arise. The article also assesses several cryptographic systems that may be used in the Internet of Things. The paper [12],suggestedaHomomorphic Cryptosystem-based Secure Data Processing Model (HC-SDPM), which enables safe collection of data and aggregate on nodes offloading at the edges for our envisioned healthcare IoT system with edge support. We provide end-to-end secrecy and data reliability throughout aggregationand transmission using Homomorphic encryption by Paillier and certificates linear homomorphic ID-based signatures. Health data security and privacy become more of an issue in a cloud-based, ubiquitous healthcare environment. The primary contribution of this work is the provision regarding health data, the proposed access control approach achieves a high level of privacy, data confidentiality, and accessibility, which employs a PR-based strategy for granting control of access to different system users. In order to provide access to any requested data, privacy ratings (PR) are computed for both the user and the data. The results demonstrate that the suggested architecture delivers a high degree of privacy and security for the information held in the healthcare system [13]. The suggested method [14] uses a blockchain to securely handle and analyze massive data in healthcare. Blockchains, on the other hand, are operationally costly, demand a large amount of data transfer, and need additional processing power; as a result, they are not entirely suited for the majority of constrained resources IoT devices intended for smart cities[15].

## 3. METHOD

This section, we discuss in detail the Blockchain and IoT-based safe healthcare architecture with unique, simplified swarm-optimized Networks with Bayesian normalization. A blockchain is often explained as a collection of blocks. Data regarding the transaction value of the hash preceding block, the current block, and the date and time are the four components that make up a single block. A blockchain is also a widely used electronic register that has historically been used to record transactional information. Since every block carries a cryptographic measure of the previous block, an attacker is unable to obtain the contents. Using this method, one may access any transactions by utilizing a cryptographic hash value that each miner in the network verifies. In addition, blockchain can be used to securely store patient medical data and enable the secure sharing of data between different healthcare providers. By using blockchain, patients can have greater control over their own medical data, and healthcare providers can access that data securely and with the patient's consent.It is constructed of blocks for each transaction and is able to record the values that are the same across the whole ledger. Figure 2 denotes the block diagram of SSO-BNNN.

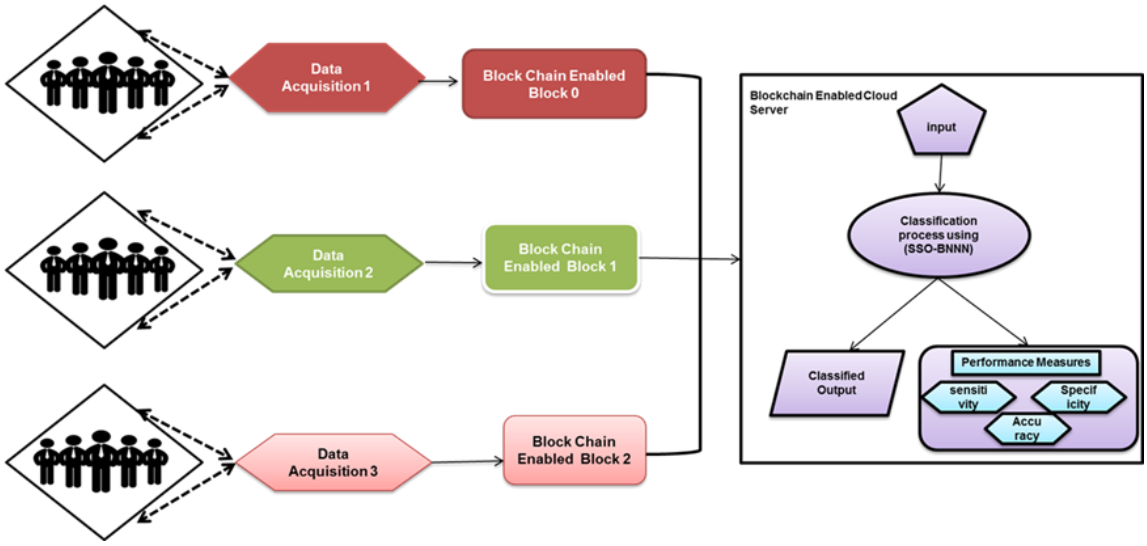


Figure 2. Block diagram of SSO-BNNN

### 3.1. Bayesian normalized neural network (BNNN)

By introducing Bayes' theorem into the normalization process, Bayesian normalization NNNs (BNNNs) make an effort to resolve these issues.
Where α and β instead of λ as

$$T(U) = \beta \sum_{j=i}^{m_c} [z_j - e(V_j]^2 + \alpha \sum_{i=j}^{m_u} u_j^2 \quad (1)$$

Where $M_u$stands for the number of the weights. With regard to the weights u, the Cost-based function, T($u$), is minimized given the starting values of the hyperparameters. Areestimate of α and β is the maximization of the available evidence.

$$O(U|\alpha, G) = \frac{1}{Y_{u(\alpha)}} exp(-\beta f_c) \quad (2)$$

One way to express the likelihood of mistakes is as follows:

$$F_u \sum_{j=1}^{Nw} u_i^2 \quad (3)$$

$$O(C|u, \beta, G) = \frac{1}{Y_{C(\beta)}} \exp(-\beta f_c) \quad (4)$$

With

$$F_C = \sum_{j=1}^{m} [z_J - E(v_j)]^2 \quad (5)$$

The weights' Bayesian inference U, for a certain model G may be expressed as

$$o(u|c|\alpha, \beta, G) = \frac{O(C|u,\beta,G)O(u|\alpha,G)}{O(C\ |\alpha,\beta,G)} = \frac{1}{Y_T} \exp[-T(U)] \quad (6)$$

$T(u)$ may be expressed as Taylor's clarification regarding the weights' probably (NO) value, $U_{NO}$.

$$T(u) \approx T(u_{NO}) + \frac{1}{2}(u - u_{NO})^S H(u - u_{NO}) \quad (7)$$

If T($U_{NO}$), the total error function's Hessian matrix, is H,

$$H = \nabla\nabla T(u_{No}) = \beta\nabla\nabla FC(uNO) + \alpha\ |\} = aC + \alpha| \quad (8)$$

The pattern of U might be thought of as roughly Gaussian if and only if G is the Hessian of the data alone.

$$O(u|c, \alpha, \beta, G) \cong \frac{1}{u*_s} exp[-T(u_{no})] - \frac{1}{2}(\Delta\, u^s H \Delta u) \quad (9)$$

Δu = u - $u_{No}$ and $u *_s$ are normalization functions, respectively. The inference for the hyperparameters is made by deleting the model identifier H from Eq. 6.

$$(\alpha, \beta \mid C) = (O(C \mid \alpha, \beta) O(\alpha, \beta))/(O(D)) \quad (10)$$

$O(C \mid \alpha, \beta)$ must be increased, and the previous $O(D)$ and $O(\alpha, \beta)$ be disregarded. Consequently, the evidence log for and may be expressed as

$$LogO(C|\ \alpha, \beta) = \alpha F_u^{NO} - 1/2\ Jm(|H|) - M_u/2\ log\beta - L/2\ log\ 2\pi \quad (11)$$

This, with relation to α and β, is maximized. The number of weights is $M_u$, while the quantity of data points is$M_C$. It is necessary to when self-consistency is established, maximize Eq. 1 with respect to and then decrease Eq. 1 With relation to the weights. The updated values of α and β are assessed inside the double loop of equations 1 and 11.

$$\alpha = \frac{\gamma}{2F_u}$$

$$\beta = (M_{C-\gamma})/2F_C$$

$$\gamma \sum_{J=I}^{M_u} \frac{\lambda_j}{\lambda_{j+\alpha}} = m_{o-\alpha trace\ (H^{-1})} \quad (12)$$

The term γ is the time-consuming process of minimizing Equation 1 requires an effective number of parameters. It is necessary to utilize a technique like the conjugate-gradient approach, and it may also be necessary to produce and invert h since this cannot be accomplished via backpropagation as for a basic NNN. The data Hessian's inverse c which has previously been considered in the evidence maximization loop may be used to provide error bars to predictions generated using BNNN models. A finite difference approach is used to derive the weights derivative (h) of the forecasts (x) value by evaluating the network following the addition of u to each weight individually. Next, each prediction's variance is supplied by

$$\sigma^2 = \frac{1}{\beta} + G^S C_H^{-1} \tag{13}$$

### 3.2. Simplified Swarm Optimization (SSO)

SSO is a brand-new populationbased soft computing technique that Yeh first created in 2009 to address the limitations of particle swarm optimization (PSO) when it comes to tackling discrete tasks. Swarm intelligence and computational evolution are integrated, using the advantages of each. Since its debut, it has been effectively used in a variety of optimization issues. At the initiation phase, the search space contains all possible solutions in SSO. Each variable is iterated through the evolution phase t times. It is updated repeatedly by putting in $v_{j,1}^s, v_{j,2}^s \ldots \ldots, v_{j,i,}^s, \ldots \ldots v_{j,i,Mvar}^s$ to the same index's value.

Where, $v_{j,}^{s-1}$, $gBest, pBest$ or a viable random value x based on a uniform random integer in the range [0, 1] in comparison to three specified criteria $Dh$ , $Do$, and $Dq$ as follows:

$$V_{ji}^S = \begin{cases} h_i if \rho\epsilon\ [0, D_h) \\ o_{ji} if \rho\epsilon\ [D_h, D_O) \\ vif \rho\varepsilon [D_O D_Q) \\ v_{ji}^{s-1}\ if \rho\varepsilon [D_Q, 1) \end{cases} \tag{14}$$

Equation (7) represents the first SSO update mechanism (UMo). It is possible to forgo the pBest scheme in UMo in favor of updating solutions more quickly without sacrificing the quality of the solutions, as seen in Eq. (8), referred to as UMf in this study.

$$V_{ji}^s \begin{cases} h_i if \rho\epsilon\ [0, D_h) \\ o_{ji} if \rho\epsilon\ [D_h, D_O) \\ v_{ji}^{s-1}\ if \rho\varepsilon [D_Q, 1) \end{cases} \tag{15}$$

The main SSO stages are outlined as follows:

#### 3.2.1. SSO Protocol:

**Phase of Initialization:**

Step 0: Arbitrarily produce $Y_j^0$ ,determine $L(Y_j^0)$, and let $bBestb_{j=}Y_j^0$ for j=1, 2….,$Ngqf$; find $sBestS$ among all sollutions such that S=arg min$L(Y_j^0)$, and let d=1.

**Evolutionary Stage:**

Step 1: Let $j = 1$

Step 2: Improve $Y_j^d$ according to Eq. (14)

Step 3: if $Y_j^d < L(B_j)$ let $B_j = Y_j^d$ go on to step 4. Otherwise, go to step 5.

Step 4: if $L(B_j) < L(S)$, let $S = B_j$.

Step 5: if $j < Ngqf$, let $j = j + 1$ go on to step 2.

Step 6: if $d < Njdk$, let $d = d + 1$ go on to step 1. Or else, halt and $sBest$ is the last solution.

### 3.3. Encryption of the hash value by means of the HVE-NIS algorithm

#### 3.3.1. Overview

A particular character encoding approach is focused on navigating through data utilizing 0s and 1s is what the recently established HVE-NIS model is. This model was recently developed. It does this by taking valid data from the bits that are next to each letter in the input sequence and allocating the shortest possible code words for each character in the sequence. The two very short code words that have been formed as a result of traversing the 0s and 1s are compared to one another, and the most effective code is chosen according to the needed bit count. In the event that the input pattern is N bits long, the HVE-NIS model will need C bits to store the details in its compacted form, as shown in the following:

$$D_{bits} = \sum_{j=1}^{M} NIS_{opr^{(j)}} + controlbits \quad (16)$$

Where $NIS_{opr^{(j)}}$ is used to indicate that bits are included in a code word. In order to get the best possible bit count in the compressed data, the suggested method requires the insertion of eight control bits. The equation that determines the highest possible amount of bits that are required to save one character when employing the HVE-NIS method is referred to as Equation 17.

$$NIS_{dg_{bx}} = \frac{D_{bits}}{M}, 1 \leq NIS_{dg_{bx}} \leq 4 \quad (17)$$

The performance of compression is improved when the rates of Cbits and $NIS_{dg_{bx}}$ are reduced to their lowest possible values. To be more specific, Equation (17) demonstrates that in order to store one character that utilizes the HVE-NIS approach, it is necessary to use four bits. Because of this, it only needs to store a character in one bit and offers the highest possible level of compression.

### 3.3.2. The basic operation of HVE-NIS algorithm

The HVE-NIS algorithm's procedure is described in this section. The word "thank you" is used as an illustration. The input text is first started with alphanumeric letters and special symbols in the model that is being provided. The model picks up on the text flow's characters and converts the ASCII values for them. The values of ASCII are then translated into a binary representation that is comparable. The traverse of bits is started with a primary bit that defines the bit as either 0 or 1 and is the binary representation of the input character.

Once loaded, 0-based traversal stores 00 (if the first bit found is 0) or 10 is the control bit (if bit one is the first one detected). In order to identify 0s and store their locations when exploring 0 values, the model traverses from the second bit using the first bit as a reference. Following the discovery of the number 0, the location (x) is saved (00-x) in a code, and the procedure is loaded once again until the seventh bit is attained. The neighboring code word is preserved if the traversal successfully reaches the last bit. After the 0-based processes have been traversed, the 1-based processes are traversed. The procedure is identical to that of a 0-based traversal, except that a 1-based traversal identifies a binary number 1 as a 1. There are two codes created. The code word with fewer bits is chosen by the model after comparison. As a result, the control bits are added to each ideal code word of encoded characters to create the compressed file.

Symmetrical compression, used by the HVE-NIS model, involves doing the decompression process exactly backward from how it was performed during compression. Additionally, the decoding end does not need any extra data to be delivered along with the compressed data. The suggested model first picks up code words in 0 and 1 seconds to learn the compressed file. The reformation procedure is then carried out. For instance, the compression process is initiated when the 00 control bit serves as a signal that the initial seven bits are zero. The duration of 0 seconds is used by the equivalent location with reference when the code word is 0-based. A printable character is chosen from the seven bits, and the first bit is reconfigured as control bits. The last step is to fill the remaining spots with values of 1 second. Similar to this, for 1-based traversal, 1 is utilized at the code word's spots, and 0s are filled in at the remaining positions. The codes for each character are then changed and converted to ASCII values. Finally, the actual text is reformatted without losing any data by converting the ASCII values into alphanumeric characters.

## 4. RESULTS AND DISCUSSION

In the section, we finding of the simplified swarm optimized Bayesian normalized neural networks. One application of blockchain and IoT in healthcare is medical device tracking. By using IoT sensors and blockchain technology, healthcare providers can track medical devices, such as pacemakers or insulin pumps, in real time. This can improve patient safety by ensuring that devices are working correctly and preventing unauthorized access or tampering.The parameters are accuracy, sensitivity, and specificity and the existing methods are Convolution Neural Networks (CNN), Deep Neural Networks (DNN), and Artificial Neural Networks (ANN).

### 4.1. Accuracy

Ensuring the accuracy of secure healthcare data is essential to providing high-quality care and protecting patient privacy. Errors or inaccuracies in patient data can lead to incorrect diagnoses, inappropriate treatments, and other adverse outcomes. Figure 3 and table 1 depict the accuracy of the proposed and existing method. To maintain the accuracy of secure healthcare data, healthcare providers must ensure that they have robust data collection, storage, and processing systems in place, as well as mechanisms for detecting and correcting errors.

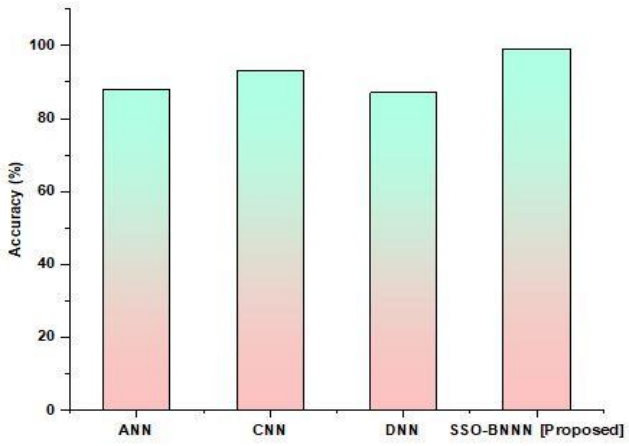


Figure 3. Accuracy of the proposed and existing method

Table 1. Comparison of accuracy

| Methods | Accuracy (%) |
|---|---|
| ANN | 88 |
| CNN | 93 |
| DNN | 87 |
| SSO-BNNN [Proposed] | 99 |

### 4.2. Sensitivity

The sensitivity parameter in secure healthcare refers to the level of sensitivity or confidentiality of the patient data that is being managed and protected. Healthcare data is considered highly sensitive due to the personal and sensitive nature of the information contained within it, including personal identifiers, medical histories, diagnoses, treatments, and other sensitive information. The sensitivity parameter in secure healthcare is a critical consideration, as the consequences of a data breach or unauthorized access to patient data can be severe. Figure 4 and table 2 shows the sensitivity of the proposed and existing method.

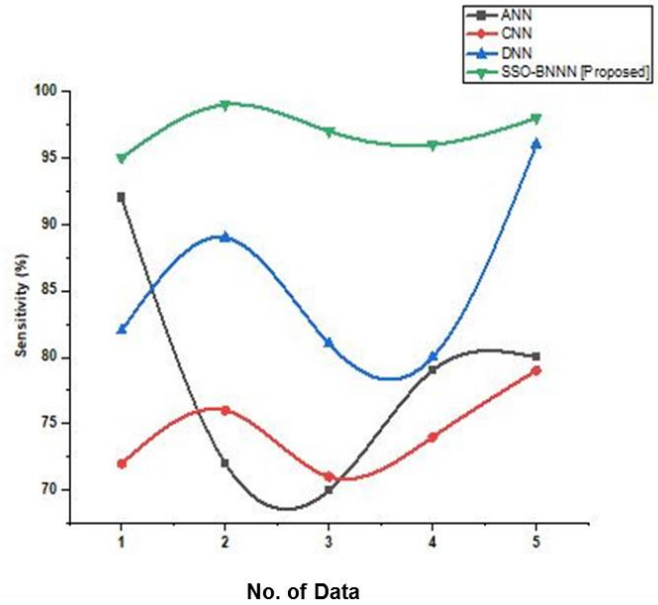


Figure 4. Sensitivity of the proposed and existing method

Table 2. Result of sensitivity

| No. of Data | ANN | CNN | DNN | SSO-BNNN [Proposed] |
|---|---|---|---|---|
| **1** | 92 | 72 | 82 | 95 |
| **2** | 72 | 76 | 89 | 99 |
| **3** | 70 | 71 | 81 | 97 |
| **4** | 79 | 74 | 80 | 96 |
| **5** | 80 | 79 | 96 | 98 |

### 4.3. Specificity

The specificity parameter in secure healthcare refers to the ability of the security measures in place to correctly identify and authorize legitimate users and activities while preventing unauthorized access or activities. In secure healthcare, specificity is critical to ensuring that patient data is protected from unauthorized access, theft, or misuse. Specificity is achieved through a range of technical, administrative, and physical safeguards, including access controls, authentication, and authorization mechanisms. Figure 5 and table 3 denote the specificity of the proposed and existing method.

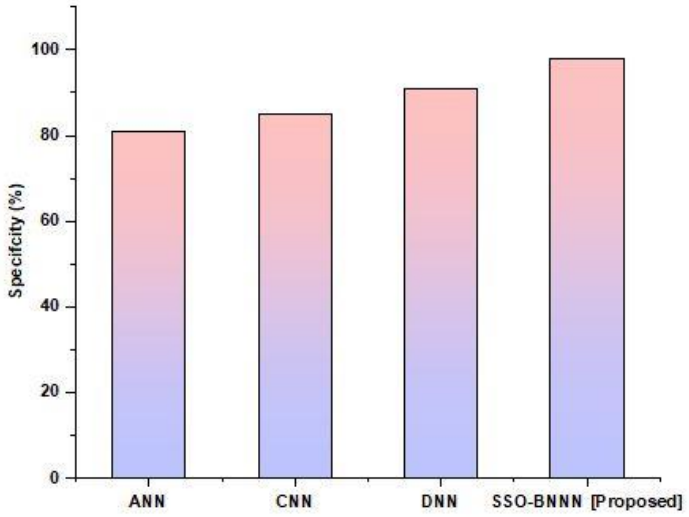


Figure 5. Specificity of the proposed and existing method

Table 3: Comparison of Specificity

| Methods | Specificity (%) |
|---|---|
| ANN | 81 |
| CNN | 85 |
| DNN | 91 |
| SSO-BNNN [Proposed] | 98 |

## 5. CONCLUSION

The SSO-BNNN concept for an intelligent IoT and healthcare blockchain that is a secure approach is proposed in this study. IoT devices are first used to gather data from consumers. Then SSO algorithm-based covert picture sharing happens. After that, the HVE-NIS method is used to encrypt the hash value. The suggested model has successfully transmitted medical pictures in a secure manner and has the highest value among the models taken into consideration. The SSO-BNNN would use machine learning algorithms to detect patterns and anomalies in the data, helping to improve accuracy and identify potential health issues early on. The SSO-BNNN model produced the best results throughout the procedure, with the greatest sensitivity (98%), specificity (98%), and accuracy (99%). In the future, dictionary-based encoding approaches may be used to improve performance.

## REFERENCES

[1] A. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A Decentralized Privacy-Preserving Healthcare Blockchain for IoT," *Sensors*, vol. 19, no. 2, p. 326, Jan. 2019, doi: 10.3390/s19020326.

[2] R. Abdolkhani, K. Gray, A. Borda, and R. DeSouza, "Patient-generated health data management and quality challenges in remote patient monitoring," *JAMIA Open*, vol. 2, no. 4, pp. 471–478, Dec. 2019, doi: 10.1093/jamiaopen/ooz036.

[3] M. M. Dhanvijay and S. C. Patil, "Internet of Things: A survey of enabling technologies in healthcare and its applications," *Comput. Networks*, vol. 153, pp. 113–131, Apr. 2019, doi: 10.1016/j.comnet.2019.03.006.

[4] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "A Patient Agent to Manage Blockchains for Remote Patient Monitoring.," *Stud. Health Technol. Inform.*, vol. 254, pp. 105–115, 2018, [Online]. Available: http://www.ncbi.nlm.nih.gov/pubmed/30306963

[5] S. Chakraborty, S. Aich, and H.-C. Kim, "A Secure Healthcare System Design Framework using Blockchain Technology," in *2019 21st International Conference on Advanced Communication Technology (ICACT)*, IEEE, Feb. 2019, pp. 260–264. doi: 10.23919/ICACT.2019.8701983.

[6] T. Veeramakali, R. Siva, B. Sivakumar, P. C. Senthil Mahesh, and N. Krishnaraj, "An intelligent internet of things-based secure healthcare framework using blockchain technology with an optimal deep learning model," *J. Supercomput.*, vol. 77, no. 9, pp. 9576–9596, Sep. 2021, doi: 10.1007/s11227-021-03637-3.

[7] A. Ali *et al.*, "An Industrial IoT-Based Blockchain-Enabled Secure Searchable Encryption Approach for Healthcare Systems Using Neural Network," *Sensors*, vol. 22, no. 2, p. 572, Jan. 2022, doi: 10.3390/s22020572.

[8] K. Hasan, K. Biswas, K. Ahmed, N. S. Nafi, and M. S. Islam, "A comprehensive review of wireless body area network," *J. Netw. Comput. Appl.*, vol. 143, pp. 178–198, Oct. 2019, doi: 10.1016/j.jnca.2019.06.016.

[9] R. R. Chandan, A. Balobaid, N. L. S. Cherukupalli, G. H L, F. Flammini, and R. Natarajan, "Secure Modern Wireless Communication Network Based on Blockchain Technology," *Electronics*, vol. 12, no. 5, p. 1095, Feb. 2023, doi: 10.3390/electronics12051095.

[10] S. N. Mohanty *et al.*, "An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy," *Futur. Gener. Comput. Syst.*, vol. 102, pp. 1027–1037, Jan. 2020, doi: 10.1016/j.future.2019.09.050.

[11] P. Kaur, M. Sharma, and M. Mittal, "Big Data and Machine Learning Based Secure Healthcare Framework," *Procedia Comput. Sci.*, vol. 132, pp. 1049–1059, 2018, doi: 10.1016/j.procs.2018.05.020.

[12] G. Srivastava, J. Crichigno, and S. Dhar, "A Light and Secure Healthcare Blockchain for IoT Medical Devices," in *2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE)*, IEEE, May 2019, pp. 1–5. doi: 10.1109/CCECE.2019.8861593.

[13] H. S. Trivedi and S. J. Patel, "Homomorphic cryptosystem-based secure data processing model for edge-assisted IoT healthcare systems," *Internet of Things*, vol. 22, p. 100693, Jul. 2023, doi: 10.1016/j.iot.2023.100693.

[14] P. B. Prince and S. P. J. Lovesum, "Privacy Enforced Access Control Model for Secured Data Handling in Cloud-Based Pervasive Health Care System," *SN Comput. Sci.*, vol. 1, no. 5, p. 239, Sep. 2020, doi: 10.1007/s42979-020-00246-4.

[15] P. Tyagi and S. K. Manju Bargavi, "Using Federated Artificial Intelligence System of Intrusion Detection for IoT Healthcare System Based on Blockchain," Int. J. Data Informatics Intell. Comput., vol. 2, no. 1, pp. 1–10, Mar. 2023, doi: 10.59461/ijdiic.v2i1.42.

## BIOGRAPHIES OF AUTHORS

**Shivi Chaturvedi** did doctorate in Electronics & Communication Engineering and M.Tech in Computer Science Engineering and received Bachelor's degree in Electronics and Communication Engineering in the year 2002 from R.G.P.V ,Bhopal (M.P) India. Presently, she is working as an Associate Professor in the Department of Computer Science Engineering , G.C.R.G Memorial Trust Group of Institutions , Lucknow, (U.P.), India. She can be contacted at email: shivi.chaturvedi@gmail.com