The Scientific Temper (2024) Vol. 15 (3): 2899-2911

E-ISSN: 2231-6396, ISSN: 0976-8653

Doi: 10.58414/SCIENTIFICTEMPER.2024.15.3.62

https://scientifictemper.com/

RESEARCH ARTICLE

Brower blowfish nash secured stochastic neural network based disease diagnosis for medical WBAN in cloud environment

M. Iniyan*, A. Banumathi

Abstract

The trending technology in Wireless Sensor Networks (WSN) is to improve the healthcare system by using wireless body area networks (WBANs). Implantable Sensor and wearable sensors are inexpensive technology, which are designed to track the body signals and to get intermediate physical activity status. This is considered as an unremarkable choice for continuous health monitoring. In recent years, various routing protocols had been designed to provide reliable data transmission in WBAN. However, many of these protocols are not focused more on security aspects such as data confidentiality and data integrity in medical data transmission. And also, the energy efficient communication methods have significantly vulnerable to various attacks due to the lack of computationally efficient authentication and authorization process. To rectify the drawbacks of existing system a new approach Brower Blowfish Nash-secured Stochastic Neural Network-based (Brower BNSNN) is proposed for medical data transmission through WBAN in cloud environment. The Brower BNSNN method is designed to perform data collection, compression, encryption/decryption and anomaly detection for medical WBAN disease diagnosis in cloud environment. First, distinct numbers of sensor nodes that are attached in the bodies of multiple patients collected for further validation and anomaly detection. Secondly Fixed Point-based compression is performed in the cloud by the cloud user. The sensor nodes compress their sensed data into WBAN messages and sent to cloud server for further processing and from this data confidentiality and data integrity are ensured. Third step is Blowfish Nash Equilibrium-based encryption and decryption is applied to the compressed data to ensure security during the communication between devices or cloud server. Finally, Stochastic Neural Network-based anomaly detection model is designed to perform anomaly detection via authorization process. The designed network performs two-stage authorization such as validating sub-keys and checking kernel process attacks and network logs attacks. Simulations are performed to measure and validate the performance metrics in terms of data confidentiality, data integrity, disease diagnosis accuracy, authentication, in Health Monitoring System.

Keywords: Wireless Body Area Networks, Cloud, Brouwer Fixed Point, Blowfish Nash Equilibrium, Stochastic Neural Network.

Introduction

Wireless networks are a revolutionary advancement in the world of computer networking. By using wireless data connections between network nodes, they have successfully eliminated the need for physical cabling. This has resulted in unparalleled flexibility and convenience for users and network administrators alike. The concept of wireless communication is not new, its roots can be traced back to the 19th century with the advent of the telegraph and radio. However, the modern era of wireless networking as we know it began to take shape in the 1970s and 1980s, marked by significant developments in wireless LAN technologies.

One of the landmark achievements in this field was the creation of the ALOHAnet in 1971. This was followed by the release of the IEEE 802.11 standard in 1997, more commonly known as Wi-Fi. These milestones marked the beginning of a new era in data communication, paving the way for the evolution and widespread adoption of wireless networks in various sectors, ranging from education and commerce to healthcare and defense.

WSN networks consist of spatially distributed autonomous sensors that work collaboratively to monitor

PG & Research Department of Computer Science, Government Arts College (Autonomous), Karur, Affiliated to Bharathidasan University, Tiruchirappalli, India.

***Corresponding Author:** M. Iniyan, PG & Research Department of Computer Science, Government Arts College (Autonomous), Karur, Affiliated to Bharathidasan University, Tiruchirappalli, India., E-Mail: iniyanmohan.r@gmail.com

How to cite this article: Iniyan, M., Banumathi, A. (2024). Brower blowfish nash secured stochastic neural network based disease diagnosis for medical WBAN in cloud environment. The Scientific Temper, **15**(3):2899-2911.

Doi: 10.58414/SCIENTIFICTEMPER.2024.15.3.62

Source of support: Nil

Conflict of interest: None.

© The Scientific Temper. 2024

Received: 12/07/2024 **Accepted:** 10/08/2024 **Published** : 20/09/2024

a wide range of physical or environmental conditions such as temperature, sound, vibration, pressure, motion, or pollutants. Originally developed for military applications like battlefield surveillance, WSNs have since found their way into numerous industrial and civilian applications. These include industrial process monitoring and control, machine health monitoring, environmental and habitat monitoring, healthcare, home automation, and traffic control. This demonstrates the versatility and potential of WSNs, revolutionizing how interact with our environment.

The extensive advancements in wireless communication have led to the progression and delegation of a specialized form of WSNs, known as Wireless Body Area Networks (WBANs). By integrating wearable and implantable sensors, WBANs have enhanced healthcare applications, enabling continuous monitoring of patients and the potential diagnosis of life-threatening diseases. This real-time data transmission capability not only enhances the quality of care and patient outcomes but also introduces the concept of remote patient monitoring. This allows patients to recover in the comfort of their homes, reducing the need for frequent hospital visits and enabling more efficient management of hospital resources.

However, like any technology, WBANs come with their own set of challenges. They face issues like quality of service (QoS) and network security issues such as authentication, access control, and privacy concerns. Network security is a set of technologies that safeguard the viability and integrity of a WBAN's infrastructure by circumventing the proliferation of a wide variety of potential threats within a network. Network security is said to be compromised when attacks persist in the WBAN, leading to unauthorized actions wherein malicious users execute network attacks with the purpose of altering, destroying, or acquiring private data.

In the broader perspective, WBANs are part of the Internet of Things (IoT) revolution. The proliferation of sensors and wireless networking technologies is ushering in a new era of connected. Despite the challenges, the continuous advancement of technology offers solutions, reinforcing the role of WBANs as an increasingly vital component of modern healthcare systems.

Related works

The remarkable advancements in wireless communication and smart devices have paved the way for innovative solutions in everyday life. As these technologies become increasingly intertwined with our daily routines, people are growing more conscious about their personal health and privacy. Consequently, medical security and privacy have emerged as significant concerns for both individuals and societies at large.

Wireless Body Area Networks (WBAN), a product of this technological evolution, have seen substantial progress in recent years, significantly enhancing healthcare applications. These networks employ a variety of sensors to monitor patients, aiming to diagnose life-threatening diseases to a certain extent. However, WBANs are not without their challenges and it grapple with issues such as Quality of Service (QoS) and more critically, network security authentication, access control, and privacy.

Network security is essentially a collection of technologies designed to protect the network's functionality and integrity. Its primary role is to prevent an array of potential threats from disrupting the network. When attacks persist, network security is compromised. This leads to unauthorized actions within the WBAN, where malicious users aim to alter, destroy, or acquire private data.

In recent years, E-healthcare has been confronting significant security issues. This is primarily due to the sensitive nature of medical data. Incorrect patient information can lead to critical decisions, potentially resulting in severe health complications and even mortality. Therefore, ensuring the security and privacy of such data is of paramount importance.

In light of these challenges, it is crucial to address the issues of QoS and network security in WBANs. Doing so will not only enhance the effectiveness of healthcare applications but also ensure the protection of sensitive patient data, thereby contributing to the overall health and wellbeing of society.

Now, let's review some literature on this topic: Enhanced Probabilistic Route Stability (EPRS) method to address issues relating to link reliability and minimizing delay in transmission. A cost function called, Link Assessment Cost (LAC) was designed that in turn made inherent decisions relating to route reliability by determining whether the selected route is a good candidate or not. Also, two critical factors, like, Route Stability Factor and Expected Probability of link. On the basis of these factors, a score was employed in determining link likelihood. In this manner, EPRS selected reliable routes, therefore enhancing route stability and reducing the end-to-end delay. Despite improvements observed in terms of the above-said factors, the important security aspects involved in medical data transmission such as data confidentiality and data integrity were not focused.

To address these aspects, Brouwer Fixed Point-based compression is employed in the cloud environment where the cloud server communicates and collects data from other WBAN sensor nodes (i.e., the cloud users). In turn, the sensor nodes compress their sensed data into WBAN messages or frames and forward them to the cloud server for further processing (i.e., performing encryption). This ensures security and therefore improves data confidentiality and data integrity. However, one-hop neighbor-based clustering methods do not ensure connectivity and reachability due to dynamic node mobility. Prevailing works focused on

centralized based methods that were found to be unsuitable for arbitrary Wireless Body Area Networks.

Distributed Energy-efficient two-hop-based Clustering and Routing protocol (DECR) targeting WIoT-enabled WBAN. In DECR, during the cluster formation phase, each node or user acquired the neighbor nodes' information within the two-hop range. In addition, an enhanced grey-wolf optimization algorithm was employed for selecting the cluster head and performing optimal routing. Despite improvements observed in terms of energy-efficient packet delivery and reducing the number of transmissions, the authentication and authorization of the cloud user was not performed. To focus on this issue, a Stochastic Neural Network-based anomaly detection model is designed where it performs two-stage authorization, therefore ensuring the objective of secure and computationally efficient data transmission in the cloud environment, Arafat, M. Y., Pan, S., & Bak, E. (2023).

The Internet of Things (IoT) technologies evolve ceaselessly with time due to advancements in automation, high mobility due to topology changes, and wide access to information. IoT refers to the gathering of several associated devices due to their eccentric characteristics like scalability, reliability, accuracy, and fault tolerance. With the increasing number of hybrid devices in big organizations, security and privacy concerns are becoming more demanding, Memon, S., Wang, J., Ahmed, A., Rajab, A., Al Reshan, M. S., Shaikh, A., & Rajput, M. A. (2023).

To comparative approach to ensure security requirements and for safeguarding from unauthenticated devices. Conventional encryption methods also utilize significant mechanisms to construct cloud network security, however, not foolproof against IaaS. Designed a membrane infrastructure on the basis of quantum inspiration to address network security aspects. Here, distributed computational methods were employed to provide membrane systems as a suitable mechanism for cloud environments, therefore ensuring unique security between cloud users Khan, H. U., Sohail, M., Ali, F., Nazir, S., Ghadi, Y. Y., & Ullah, I. (2023), Visalaxi, G., & Muthukumaravel, A. (2023).

Enhanced system security methods are laborious and time-consuming due to the different potentialities of IoT devices and the ever-changing environment, hence simply applying fundamental security mechanisms are said to be dangerous. A malware detection and prevention method for secure data transmission between IoT devices using a deep learning approach. By employing an Improved Elliptic Curve Cryptography algorithm, there was an improvement of both accuracy and precision. Yet another keyword mechanism employing for specific devices using a conjunctive keyword. But as far as highly susceptible cloud servers are concerned, the IoT data can be easily modified due to the centralization mechanism. Also, the cloud servers are highly susceptible to attacks due to their homogeneous nature. To address this issue, a secret sharing mechanism employing collaborative blockchain. Also, a depth-first search algorithm was presented to ensure data retrieval efficiency Devi, R. A., & Arunachalam, A. R. (2023), Zhou, R., Zhang, X., Wang, X., Yang, G., Dai, H.-N., & Liu, M. (2022), Wang, N., Fu, J., Zhang, S., Zhang, Z., Qiao, J., Liu, J., & Bhargava, B. K. (2023).

A comprehensive survey on WBAN was investigated. Several research works have been discussed in detail concerning the uses of WBAN in Health Monitoring on the basis of real-world health monitoring methods. Numerous types of research are also done in WBAN on the basis of security and energy efficiency mechanism. A novel heart disease prediction under WBAN employing an optimization algorithm. Owing to the untrustworthy wireless media, communication in WBAN is said to be highly vulnerable to different types of attacks and hence pose major threats. To fill this gap, an energy-efficient key management method for WBANs taking into consideration the accessible resources during key management to not only ensure security but also improve the overall network lifetime Zou, S., Xu, Y., Wang, H., Li, Z., Chen, S., & Hu, B. (2017), Veerabaku, M. G., Nithiyanantham, J., Urooj, S., Md, A. Q., Sivaraman, A. K., & Tee, K. F. (2023), Ali, A., & Khan, F. A. (2023).

In numerous methods in WBAN relating to reliability, safety, transmission, and security. Medical data is exceedingly sensitive and personal in nature and hence it must be safeguarded while being communicated between nodes. lightweight mutual authentication mechanism on the basis of key agreement technique. One of the major unaddressed issues inside WBAN or during transmission is security and privacy protection that demands for security and privacy. Two significant data security mechanisms for sensitive and private patient medical data using fine-grained distributed access control. Several security mechanisms in WBANs along with the extensive review on prevailing secure routing methods were reported. Introduced an efficient monitoring mechanism via a cloud platform to address issues concerning computing cost and communication overhead. However, data confidentiality was not focused Ananthi, J. V., & Jose, P. S. H. (2021), Kumar, M., & Hussain, S. Z. (2023), Li, M., & Lou, W. (2010), Singla, R., Kaur, N., Koundal, D., & Bharadwaj, A. (2022), Abubeker, K. M., & Baskar, S. (2022).

Currently, Internet of Things (IoT)-based E-healthcare constitutes a budding research area owing to the swift evolution of wireless technologies and cloud computing environment. These characteristics made it useful in WBAN for healthcare-related applications. Nevertheless, both data security and privacy remain demanding issues in WBANs that have to be addressed. In this purview, several authentication mechanisms have been designed attempting to persuade both security and performance requisites. Enhanced authentication mechanism employing elliptic curve digital signature with message recovery. Using this mechanism ensured reliable data security with minimal storage cost. Yet

another multi-tier secured architecture making use of Elliptic Curve Key Agreement Scheme to both improve accuracy and reduce encryption latency subsequently. An overview of prevailing security and privacy mechanisms in WBAN Abubeker, K. M., & Baskar, S. (2022), Pavithra, D., Nidhya, R., Shanthi, S., & Priya, P. (2023), Auko, J. (2023).

The security of IoT using federated and deep learning. By employing these learning techniques, data privacy was maintained while sharing information between users in an accurate and precise manner. Despite improvement in both accuracy and precision, the data integrity was not focused. Emphasized a secured data processing mechanism on efficient health service where both tumor detection and secured transmission between patients were performed using deep learning-based SHA-256 encryption algorithm. With this encryption algorithm, there was an improvement of overall accuracy and ensured secured data management. An elaborate review on federated learning for secure IoMT application. Yet another method to ensure quality of service with high throughput and low energy consumption. Though quality of service was ensured, the authentication mechanism was not included Gugueoth, V., Safavat, S., & Shetty, S. (2023), Mohanty, M. D., Das, A., Mohanty, M. N., Altameem, A., Nayak, S. R., Saudagar, A. K. J., & Poonia, R. C. (2022), Rani, S., Kataria, A., Kumar, S., & Tiwari, P. (2023), Singla, R., Kaur, N., Koundal, D., Lashari, S. A., Bhatia, S., & Rahmani, M. K. I. (2021).

Current hospital management techniques are often overly complex or lack comprehensive deep learning analysis, limiting their practical application potential. Additionally, many of these methods employ changeable storage solutions, which further restricts their trustworthiness. To bridge these gaps, a novel method, which utilizes deep learning for secure, distributed hospital management, leveraging context-aware side-chains, Reddy, V. S., & Debasis, K. (2023).

In various studies, it was found that methods based on deep learning and optimization outperformed traditional approaches in ensuring secure disease diagnosis in a cloud computing environment. Therefore, it's vital to adopt a method that guarantees security and efficient disease diagnosis. This can be achieved by incorporating anomaly detection through compression with neural network techniques, which will enhance and refine the existing mechanisms.

Research gap

According to the above literature, the research gap identified is listed as given below.

- Some of the research gaps identified in DECR and EPRS are to use on improvements observed in terms of energy-efficient packet delivery, minimizing end-to-end delay and re-transmission rates but more importantly the network security aspects like data confidentiality, data integrity and verification aspects like authentication and authorization was not focused.

Research Contribution

To fill research gap to address on these aspects a Brower Blowfish Nash-secured Stochastic Neural Network-based (Brower BN-SNN) in medical domain area for disease diagnosis is designed. The contributions of the Brower Blowfish Nash-secured Stochastic Neural Network-based (BBN-SNN) are listed as given below.

- To improve the authentication, authorization and access control with minimal response, the Brower BN-SNN is designed based on three major processes namely compression, encryption/decryption and anomaly detection.
- To improve data confidentiality and data integrity, therefore ensuring the objective of security, Brouwer Fixed Point-based compression is employed in the cloud environment.
- To ensure energy efficient packet delivery and reduce number of transmissions with endpoint detection and response for IoT enabled WBAN Blowfish Nash Equilibrium-based encryption and decryption is applied to the compressed data. By using this algorithm efficient communication between devices or cloud users are said to be ensured that in turn improves accuracy.
- To design Stochastic Neural Network for anomaly detection with improved endpoint detection and minimal response.
- Finally, comprehensive experimental assessment is carried out with five different performance factors, data confidentiality, data integrity, authentication accuracy, disease diagnosis accuracy and response time to illustrate the proposed Brower BN-SNN method over traditional methods.

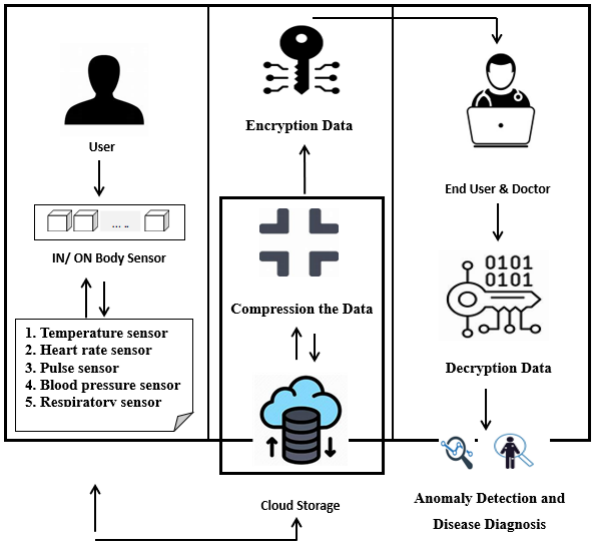

Figure 1: Structure of BBN-SNN

Organization of the Paper

The overall work is arranged into different sections as follows. Section 2 reviews the related works in the area of authentication, authorization, access control from WBAN data in cloud computing environment. A detailed representation of the proposed Brower BN-SNN method with the aid of figurative representation and pseudo code is elaborated in Section 3. In Section 4 the experimental settings is described followed by implementation details in Section 5. Section 6 discusses on the performance results of the proposed and traditional methods with numerous performance metrics. Finally, Section 7 concludes the paper.

Methodology

In this section the overview of the proposed method called, Brower Blowfish Nash-secured Stochastic Neural Network-based (Brower BN-SNN) disease diagnosis for medical WBAN in cloud environment is presented. Figure 1 shows the structure of Brower BN-SNN method for medical WBAN in

As illustrated in the above figure, two different datasets, Health monitoring dataset and BETH dataset are used for performing disease diagnosis in a secured manner. Here, health monitoring dataset is applied for training purpose whereas using the BETH dataset testing and validation is performed for detection of any anomalies. (i.e., Purpose of Anomaly Detection: Zigbee and Bluetooth devices are vulnerable to attacks using a Flipper Zero device, which can easily exploit these technologies. When a Flipper Zero device targets a specific frequency, it can compromise the communication. To counter this, hash value system is implemented. If there are any changes in the data, the hash value will automatically change. This change in the hash value indicates an anomaly, representing a potential attack detection. By monitoring these hash values, effectively detect and respond to anomalies in the system.) For this purpose, the data obtained via different sensors like temperature sensor, heart rate sensor, pulse sensor, blood pressure sensor respiratory rate sensor and so on for different sets of WBAN users from the Health Monitoring System dataset are provided as input and stored in cloud.

Table 1: Health monitoring system dataset vital signs description

S. No.	*Vital signs*	*Normal values in adults*
1	Temperature	$37^{\circ}C$
2	Heart rate	$60-99$ *beats per minute*
3	Pulse	$60-99$ *beats per minute*
4	Blood pressure	$\frac{120}{80mm}Hg$
5	Respiratory rate	$12-16$ *breaths per minute*
6	Oxygen saturation	$95-100\%$
7	pH	$7.3-7.5$

Second with the samples obtained from different sensors the cloud user performs compression using Brouwer Fixed Point and stores these compressed medical sensed data for further processing. Next to ensure security while communication between sensors, Blowfish Nash Equilibrium-based encryption and decryption are then applied. The cloud server next aggregates data packets acquired from different sensors with the purpose for disease diagnosis. Finally, anomaly detection if any in presence is done using Stochastic Neural Network-based anomaly detection model in an accurate manner.

Data collection

Initially, distinct numbers of sensor nodes attached to bodies of multiple patient's data acquired from the Health Monitoring System dataset and stored in cloud environment. Also, a table listing the vital signs normal values in adult is also provided for reference.

With the above initialization the input vector matrix for health monitoring dataset is mathematically represented as given in Table 1.

$$IV[HM]=\begin{bmatrix} S_1F_1 & S_1F_2 & \dots & S_1F_n \\ S_2F_1 & S_2F_2 & \dots & S_2F_n \\ \dots & \dots & \dots & \dots \\ S_mF_1 & S_mF_2 & \dots & S_mF_n \end{bmatrix}, m=4000, n=20 \quad (1)$$

From the above equation (1), the input vector 'IV' for the corresponding Health Monitoring dataset 'HM' is formulated on the basis of 'm' samples and 'n' features respectively. Also another dataset, Real Cybersecurity Data for Anomaly Detection Research BETH (BPF-extended tracking honeypot (BETH) dataset) is employed for validation and analysis.

With this initialization the input vector matrix for BETH dataset is mathematically represented as given below.

$$IV[BETH]=\begin{bmatrix} S_1F_1 & S_1F_2 & \dots & S_1F_v \\ S_2F_1 & S_2F_2 & \dots & S_2F_v \\ \dots & \dots & \dots & \dots \\ S_uF_1 & S_uF_2 & \dots & S_uF_v \end{bmatrix}, u=4000, v=16 \quad (2)$$

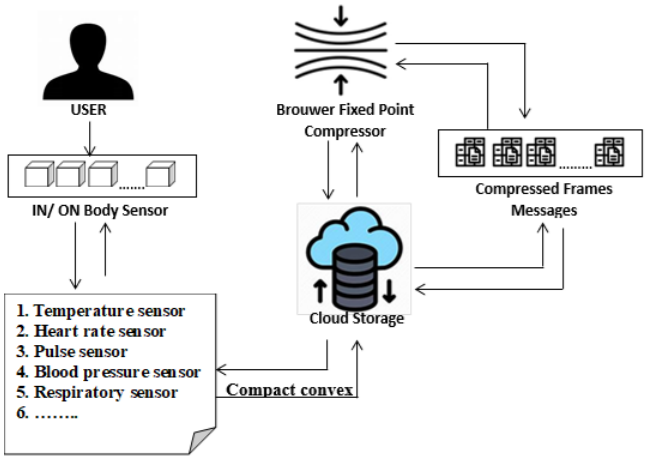

Figure 2: Structure of brouwer fixed point-based compression model

From the above equation (2), the input vector 'IV' for the corresponding BETH dataset '$BETH$' is formulated on the basis of 'u' samples and 'v' features respectively.

Brouwer Fixed Point-based compression

In this section with the data collected from both the dataset (i.e., training dataset for processing and testing dataset for validation), data compression is performed for each WBAN sensor nodes with the objective of ensuring deduplication (i.e., ensuring dataset redundant data) and providing a mechanism for data confidentiality and data integrity. This is performed in our work using Brouwer Fixed Point-based compression model. Figure 2 shows the structure of Brouwer Fixed Point-based compression model.

As illustrated in the above Figure 2, the cloud server 'CS' communicates and collects data from the other WBAN sensor nodes the cloud users 'CU'. Followed by which each cloud users applies Brouwer Fixed Point-based compression function via compact convex set to perform the compression. Finally, the compressed WBAN messages or frames are sent to the cloud server for further processing. Let '$S \subseteq \mathbb{R}^n$' represent a compact convex set. Here, compact and convex set refers to a set of points (i.e., the set of samples '$S = \{S_1, S_2, \dots, S_m\}$') that follow the property, the set is convex, that is, any line that connects any and all the two points (i.e., chosen sample pairs communicate between WBAN sensor nodes or the cloud users) chosen from the set (i.e., the set of samples) lies in the set '$\mathbb{R}^n$'. Let us further consider that '$\Phi: S \to \mathbb{R}^n$' represents a continuous function (i.e., where the cloud server receives the sensed data continuously from different cloud users) that maps 'S' into itself and is mathematically formulated as given below.

$$\Phi(S) \subseteq S \quad (3)$$

From the above equation (3) it is inferred that 'Φ' has a fixed point 'P' on 'S' such that '$P = \Phi(S)$'. Every system of 'm' equations (i.e., with 'm' samples) and 'n' unknown variables (i.e., with 'n' features) as given below.

$$F(P) = 0 \quad (4)$$

$$F(P) = \left(F_1(P), F_2(P), \dots, F_n(P)\right)^T, P = (P_1, P_2, .., P_n)^T \quad (5)$$

From the above two formulations (4) and (5), according to the compact convex set, Brouwer Fixed Point is said to be reduced to equivalent form as given below.

$$P = \Phi(P) = Frames(S_1), Frames(S_2), \dots, Frames(S_m) \quad (6)$$

Then, by modeling Brouwer Fixed Point, 'P' on 'S' as given in the above equation (6), compression is said to be performed concurrently by the WBAN sensor nodes for all the features of a specific sample into a single entity into WBAN messages or frames and forward them to cloud server for further processing (i.e., performing encryption).

In this manner a prototype of WBANs, including WBAN sensors (i.e., cloud users) and server (i.e., cloud server) has been designed for simulation characterizing efficient data storage in cloud computing (CC) environment. Using the prototype system (i.e., WBAN sensors and server), a scalable and efficient data analysis/storage and processing infrastructure for large scale WBANs system using Brouwer Fixed Point-based compression is said to be ensured that in turn reduces the deduplication also considerably. The pseudo code representation of Brouwer Fixed Point-based compression is given in Algorithm 1.

Algorithm 1: Brouwer fixed point-based compression

Input: Dataset $Data\ Set = HM, BETH$, Samples $S = \{S_1, S_2, \dots, S_m\}$, Features $F[HM] = \{F_1, F_2, \dots, F_n\}$, Features $F[BETH] = \{F_1, F_2, \dots, F_l\}$

Output: confidential and highly integrated compressed messages 'CM'

1: Initialize $m = 4000$, $n = 20$, $l = 16$' cloud server CS, cloud users $CU = \{CU_1, CU_2, .., CU_m\}$
2: Begin
3: For each Dataset $DS[HM]$ with Samples 'S' and Features $F[HM]$
4: Formulate input vector matrix separately for health monitoring dataset and BETH dataset as given in equations

$$IV[HM] = \begin{bmatrix} S_1F_1 & S_1F_2 & \dots & S_1F_n \\ S_2F_1 & S_2F_2 & \dots & S_2F_n \\ \dots & \dots & \dots & \dots \\ S_mF_1 & S_mF_2 & \dots & S_mF_n \end{bmatrix} \dots (1) \text{ and}$$

$$IV[BETH] = \begin{bmatrix} S_1F_1 & S_1F_2 & \dots & S_1F_v \\ S_2F_1 & S_2F_2 & \dots & S_2F_v \\ \dots & \dots & \dots & \dots \\ S_uF_1 & S_uF_2 & \dots & S_uF_v \end{bmatrix} \dots (2)$$

5: Formulate fixed point continuous function as given in equation $\Phi(S) \subseteq S \dots (3)$
6: Formulate fixed point continuous function for all the featured samples using compact convex set as given in equations $F(P) = 0$ … (4) and $F(P) = \left(F_1(P), F_2(P), \dots, F_n(P)\right)^T, P = (P_1, P_2, .., P_n)^T \dots (5)$
7: Formulate Brouwer Fixed Point to reduced form into WBAN messages or frames as given in equation
$P = \Phi(P) = Frames(S_1), Frames(S_2), \dots, Frames(S_m) \dots (6)$
8: Return WBAN messages or frames 'CM' to cloud server 'CS'
9: End for
10: End

As given in the above algorithm with the input vector matrix formulating separately for health monitoring and

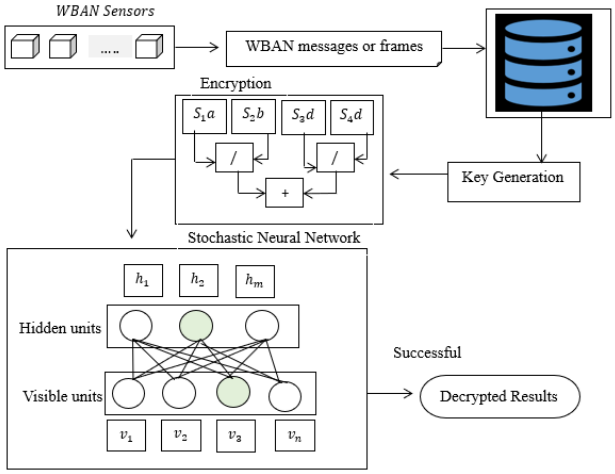

Figure 3: Structure of Stochastic Neural Network and Blowfish Nash Equilibrium-based encryption and decryption

BETH datasets. Second, using compact convex set and employing fixed point continuous function for all the featured samples are acquired as input for different set of WBAN users. Finally, Brouwer Fixed Point function is applied to produce the reduced form therefore obtaining WBAN messages or frames in a most confidential manner. By applying this Brouwer Fixed Point-based compression model even large data size are said to be handled in an efficient manner by the WBANs by storing these compressed medical sensed data and performing analysis (i.e., encryption) operations on it.

Stochastic Neural Network and Blowfish Nash Equilibrium-based encryption and decryption

The process of Blowfish Nash Equilibrium-based encryption and decryption is split into three sections, key expansion, data encryption and decryption. The requirement to safeguard the WBAN compressed messages 'CM' from unauthorized cloud users is in the increasing trend. Security provisioning and disease diagnosis in a timely manner is one of the most demanding characteristics in healthcare applications.

In this section with the obtained confidential and highly integrated compressed messages, Blowfish Nash Equilibrium-based encryption and decryption is then applied to ensure security while communication between WBAN sensors or cloud users for early disease diagnosis. The cloud server in turn aggregates data packets received from distinct sensors into a single frame for monitoring vital parameters, like temperature sensor, pressure sensor that requires to be measured ceaselessly processed immediately and transmitted in a timely manner for disease diagnosis.

Here, security is ensured by means of authentication and authorization by providing access control to only the valid cloud users so that that results of disease (i.e., CKD or no CKD) is also communicated between valid cloud users. With this objective, the security of the Blowfish cryptography is enhanced by Nash Equilibrium. The compressed and encrypted medical data i.e., combining multiple wearable sensors in the WBANs are then provided to the cloud server in one signal from different sensors before transmission for detecting anomaly. Figure shows the structure of Stochastic Neural Network and Blowfish Nash Equilibrium-based encryption and decryption model.

As illustrated in the above figure, with the compressed WBAN messages 'CM' obtained from different cloud users 'CU', is then subjected to three processes, namely, key expansion, encryption and decryption. In the key expansion stage, sub-keys are generated by cloud server between cloud user with which the authorization are said to be made in the further process. Second, the actual data encryption is performed using Blowfish cryptography enhanced by Nash Equilibrium.

Next the authorization is done where two-stage authorization is performed by first validating the sub-keys and then measuring the anomaly detection (i.e., checking kernel process attacks and network logs attacks) via hidden units in the Stochastic Neural Network. Finally, decrypted diagnosed results are provided to the authorized cloud users by the cloud server.

To start with initially, each compressed WBAN messages 'CM' different cloud users 'CU' from each '$64-bit$' plaintext message is split into '$32\ bits$'. Now the sub-key each comprising of '$32\ bits$' are stored as '$s-box$' and '$p-box$', where '$s-box$', is used in the encryption process, whereas '$p-box$', is used in the decryption process.

Now the plain text or the compressed WBAN messages 'CM' is split into two equal pieces '(L_0, R_0)', where 'L_0' denotes the left 32 bits and 'R_0' denotes the right 32 bits respectively.

$$XL\ [p-box] = XOR(L_0) \tag{7}$$

$$XR[p-box] = XOR(R_0) \tag{8}$$

From the above equations (7) and (8), the two equal pieces are XOR with left '$32\ bits$' to produce a new value 'XL' and XOR with right '$32\ bits$' to produce new value 'XR' respectively. The process is repeated for 15 times with successive bits of the '$p-array$'. Let 'RF' represent the round function and 'SK' denotes the sub-keys initialized for different numbers of cloud users 'CU' arbitrarily.

Then, for each round, data encryption along with the diagnosed results is performed in the encryption stage as given below.

$$L_{i+1} = XR_i[(S_3, c), (S_4, d)] \tag{9}$$

$$R_{i+1} = XL_i[(S_1, a), (S_2, b)] \oplus RF(R_i) \tag{10}$$

$$CT = (R_{n+1}, L_{n+1}) \tag{11}$$

From the above equations (9), (10) and (11), the cipher text 'CT' for different cloud users 'CU' are generated according to the corresponding left and right successive bits using arbitrary sub-keys 'a', 'b', 'c' and 'd'. These sub keys are generated by the cloud server 'CS' and provided to each of the cloud users (i.e., cloud user 'CU_i' and cloud user 'CU_j') ready for transmission and reception. Only upon successful authorization between cloud user's performed on behalf of the cloud server the corresponding decryption process is performed and vice versa.

As previously discussed, a two-stage authorization process is initiated to validate the model. In the two-stage authorization process, first the sub-keys are analyzed. Next, in the second-stage authorization process two different types of network attacks kernel process attacks and network logs attacks are focused. Kernel attacks exploit the zero-day operating system vulnerabilities in the kernel.

In a typical kernel attack, adversaries install and load a known vulnerable driver to gain access to the system, elevate their privileges and then make changes. On the other hand, network logs attacks refer to the DDoS attacks. In case of

the kernel attack is verified and validated by means of the process table size and if the process table size is not modified then no kernel process attacks is said to be generated. In a similar manner the presence of DDoS attacks are validated by means of the request size. If the request size is found to be higher, then a possibility of DDoS is said to be generated and in contrary authorization is said to be successful and proceeded with other set of cloud users.

The activation condition of hidden units for stochastic neural network towards authorization for second hidden unit 'Act_2' as illustrated in the above Figure 3 is as given below

$$Prob(h_2 = 1|v) = \sigma(Act_2 + \sum_{i=1}^{m} w_{2i} v_i) \quad (12)$$

In a similar manner, the activation condition of visible units for stochastic neural network towards authorization for third visible 'Act_3' as illustrated in the above Figure 3 is given below

$$Prob(v_3 = 1|h) = \sigma(Act_3 + \sum_{i=1}^{m} w_{3i} h_i) \quad (13)$$

Finally, according to the above activation results in case of successful authorization, the decryption process, '$p - box$', is employed upon successful authorization between the cloud users. The decryption process is formulated as given below.

$$R_i[(S_3, c), (S_4, d)] = XL_{i+1} \quad (14)$$

$$L_i[(S_1, a), (S_2, b)] = XR_{i+1} \oplus RF(XL_{i+1}) \quad (15)$$

Finally with the above plain text, with the presence of malicious cloud users anomalous data points are identified in an accurate manner. The pseudo code representation of stochastic neural network and blowfish nash equilibrium-based encryption and decryption is given in Algorithm 2.

As given in the above algorithm, the overall process is split into four sections. First, with the compressed messages or frames obtained as input from the WBAN sensors or cloud users by the cloud server the input is subjected to key expansion. As given above in the key expansion stage, sub-keys are generated by the cloud server separately for each cloud users according to left shift and right shift. Followed by which encryption process is performed by means of Blowfish Nash Equilibrium function. In addition to the validation is also made for diagnosing disease so that the compressed encrypted diagnosed resultant messages are provided as input in the next stage. Third, authorization is performed in a two-stage process. First, sub-keys are validated and followed by which, presence of kernel process and network log attacks are validated via hidden units of the Stochastic Neural Network. Only upon successful validation of the condition authorization is provided to the cloud user for decrypting the cipher text. Finally, decryption is made that by introducing random variations into the network help the network in identifying anomalous data points in an accurate manner.

Algorithm 2: Stochastic neural network and blowfish nash equilibrium-based encryption and decryption

Input: Dataset $Data\ Set = HM, BETH$, Samples $S = \{S_1, S_2, \ldots, S_m\}$, Features $F[HM] = \{F_1, F_2, \ldots, F_n\}$, Features $F[BETH] = \{F_1, F_2, \ldots, F_i\}$

Output: secure authentication and authorization

1: Initialize $m = 4000$, $n = 20$, $l = 16$, cloud server CS, cloud users $CU = \{CU_1, CU_2, .., CU_m\}$
2: Initialize WBAN messages or frames CM, sub keys $SK = \{a, b, c, d\}$
3: Initialize size of process table $SizeOf[PT] = PT_{size}$ to store compressed messages CM
4: Initialize request size Req_{size}
5: Begin
6: For each Dataset $Data\ Set[HM]$ with Samples S, Features $F[HM]$ and compressed messages
CM (i.e., plain text)
//Key expansion
7: Split the compressed messages CM (i.e., plain text) into two equal pieces (L_0, R_0)
8: Perform left shift as given in equation $\boldsymbol{XL}\ [\boldsymbol{p - box}] = \boldsymbol{XOR}(\boldsymbol{L_0})$ … (7)
9: Perform right shift as given in equation $\boldsymbol{XR}[\boldsymbol{p - box}] = \boldsymbol{XOR}(\boldsymbol{R_0})$… (8)
10: Generate sub keys for each set of cloud users to be ready for communication (i.e., performed by cloud server)
//Data encryption $[\boldsymbol{s - box}]$
11: If
$HR, Pulse = 60 - 99$ && $BP = \left(\frac{120}{80}\right)$ && $RR = 12 - 16$ && $OS = 95 - 100$ && $pH = 7.3 - 7.5$
12: Then no disease diagnosed '$Res = Normal$'
13: Else
14: Disease diagnosed '$Res = Chronic$'
14: End if
15: Perform encryption using equations $\boldsymbol{L_{i+1}} = \boldsymbol{XR_i}[(\boldsymbol{S_3}, \boldsymbol{c}), (\boldsymbol{S_4}, \boldsymbol{d})]$ … (9), $\boldsymbol{R_{i+1}} = \boldsymbol{XL_i}[(\boldsymbol{S_1}, \boldsymbol{a}), (\boldsymbol{S_2}, \boldsymbol{b})] \oplus \boldsymbol{RF}(\boldsymbol{R_i})$ … (10) and $\boldsymbol{CT} = (\boldsymbol{R_{n+1}}, \boldsymbol{L_{n+1}})$ … (11)
16: Return cipher text
//authorization and decryption ['$\boldsymbol{p - box}$']
17: If sub keys '$SK[CU_i] = SK[CU_j]$' and '$SizeOf[PT] = PT_{size}$' and '$Req_{size} < m$'
18: Then authorization successful
19: Perform activation as given in equations
$\boldsymbol{Prob}(\boldsymbol{h_2} = \boldsymbol{1}|\boldsymbol{v}) = \boldsymbol{\sigma}(\boldsymbol{Act_2} + \sum_{i=1}^{m} \boldsymbol{w_{2i}} \boldsymbol{v_i})$ … (12)
and $\boldsymbol{Prob}(\boldsymbol{v_3} = \boldsymbol{1}|\boldsymbol{h}) = \boldsymbol{\sigma}(\boldsymbol{Act_3} + \sum_{i=1}^{m} \boldsymbol{w_{3i}} \boldsymbol{h_i})$ … (13)
20: Perform decryption process as given in equations
$\boldsymbol{R_i}[(\boldsymbol{S_3}, \boldsymbol{c}), (\boldsymbol{S_4}, \boldsymbol{d})] = \boldsymbol{XL_{i+1}}$ … (14) and
$\boldsymbol{L_i}[(\boldsymbol{S_1}, \boldsymbol{a}), (\boldsymbol{S_2}, \boldsymbol{b})] = \boldsymbol{XR_{i+1}} \oplus \boldsymbol{RF}(\boldsymbol{XL_{i+1}})$ … (15)
21: Return plain text
22: Else
//Authorization not successful
23: Perform decryption with other set of cloud users
24: End for
25: End

Experimental setup

The proposed Brower Blowfish Nash-secured Stochastic Neural Network-based (Brower BN-SNN) disease diagnosis for medical WBAN in cloud environment is evaluated using python working on MS Window platform on computer with AMD Ryzen A6 processor and 4 GB RAM and the results are compared with the existing methods, Enhanced Probabilistic Route Stability (DECR) and Enhanced Probabilistic Route Stability (EPRS). The results are evaluated based on the metrics such as, data confidentiality, data integrity (i.e., network security aspects), disease diagnosis accuracy, authentication accuracy and response time using BETH dataset. The performance of Brower BN-SNN method is compared with the other competing methods, DECR and EPRS using the BETH and Health Monitoring System dataset to ensure fair comparison and validation, Arafat, M. Y., Pan,

S., & Bak, E. (2023), Memon, S., Wang, J., Ahmed, A., Rajab, A., Al Reshan, M. S., Shaikh, A., & Rajput, M. A. (2023).

Implementation details

In this study, we developed a method called Brower Blowfish Nash-secured Stochastic Neural Network-based disease diagnosis for medical WBAN in cloud computing environment with improved data confidentiality, data integrity, authentication accuracy, response time and disease diagnosis accuracy.

- The Brower BN-SNN method comprises of four sections, namely, data collection, compression, encryption/decryption-based disease diagnosis and anomaly detection.
- The Brower BN-SNN method is compared with two existing methods, Enhanced Probabilistic Route Stability (DECR) and Enhanced Probabilistic Route Stability (EPRS) Health monitoring and BETH dataset to validate the results Arafat, M. Y., Pan, S., & Bak, E. (2023), Memon, S., Wang, J., Ahmed, A., Rajab, A., Al Reshan, M. S., Shaikh, A., & Rajput, M. A. (2023).
- Initially, raw data from Health monitoring and BETH dataset were obtained from the input datasets.
- In the second part, Brouwer Fixed Point-based compression algorithm is employed to generate WBAN messages or frames using compact convex set from different WBAN sensors or cloud users as input. Next, with the aid of Brouwer Fixed Point for the corresponding samples obtained from different WBAN sensors efficient data analysis/storage and processing infrastructure is generated with improved data confidentiality and data integrity.
- Third, Blowfish Nash Equilibrium-based encryption and decryption algorithm is applied to first encrypt the WBAN messages or frames via key expansion and Blowfish Nash function and also corresponding disease diagnosed results are generated in an encrypted manner. The process undergoes key expansion by generating left and right keys separately and accordingly Blowfish Nash function was applied for different numbers of cloud users arbitrarily.
- Finally, the Stochastic Neural Network based Classifier is applied as input for performing authorization. Here, two-stage authorization was performed, wherein the first stage, sub key validation was made and in the second stage the detection of anomaly for two different types of attacks were made, therefore ensuring robust and accurate anomaly detection.

According to the above implementation patterns, five different evaluation metrics are detailed in the next section.

Discussion

In this section the performance analysis of the proposed method, Blowfish Nash-secured Stochastic Neural Network-based disease diagnose is and anomaly detection is validated and analyzed by making a fair comparison between two state-of-the-art methods, Enhanced Probabilistic Route Stability (DECR) and Enhanced Probabilistic Route Stability (EPRS). Fair comparison is ensured by employing same dataset with similar samples for detailing discussion Arafat, M. Y., Pan, S., & Bak, E. (2023), Memon, S., Wang, J., Ahmed, A., Rajab, A., Al Reshan, M. S., Shaikh, A., & Rajput, M. A. (2023).

Table 2: Tabulation of data confidentiality and data integrity

Samples	*Data confidentiality (%)*			*Data integrity (%)*		
	Brower BN-SNN	*DECR*	*EPRS*	*BBN-SNN*	*DECR*	*EPRS*
400	97.36	95.26	92.1	2.63	4.75	7.89
800	95.25	87.35	75.45	3.15	5	7.95
1200	94	86.1	74.2	3.55	5.35	8.35
1600	92.15	84.25	72.35	3.85	5.55	8.55
2000	90	82.15	70.25	4	5.86	8.85
2400	91.35	83.45	71.55	4.35	6	9
2800	93	85.15	73.25	3.15	5.15	7.35
3200	94.25	86.35	74.45	3	4.64	6.15
3600	95	87.12	75.22	2.75	3.55	5.25
4000	96.15	88.25	76.35	2.55	3	4

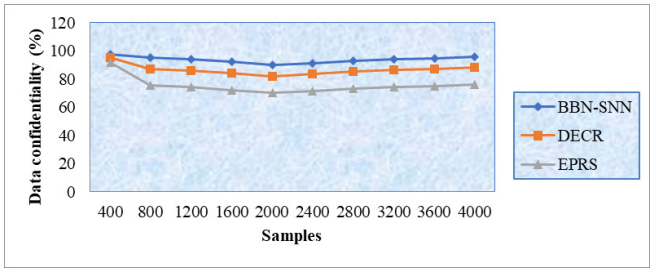

Figure 4: Data confidentiality versus samples

Performance analysis of data confidentiality and data integrity

While designing secured medical diagnosis for WBAN in cloud computing environment, one of the most signfiicant performance metric is the data confidentialiy. The data confidentilaity rate here is referred to as the percentage ratio of the number of data (i.e., here data represents the samples aggregated featured values) that are received by the authorized receiver (i.e., WBAN sensors or cloud users) and is mathematically stated as given below:

$$DC = \sum_{i=1}^{m} \frac{S_{CU}}{S_i} * 100 \quad (16)$$

From the above equation (16), data confidentiality 'DC' is evaluated by considering the sample data involved in the simulation 'S_i' and the sample instances received by the intended recipient or the intended cloud users 'S_{CU}'. It is

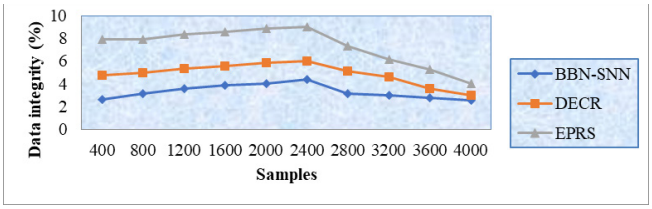

Figure 5: Data integrity versus samples

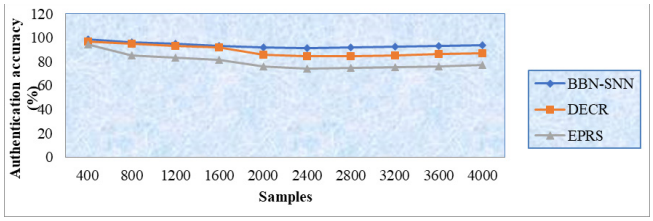

Figure 6: Authentication accuracies versus samples

measured in terms of percentage. Higher value ensures the efficiency of the method. Data integrity on the other hand refers to the analysis of the integrity of data (i.e., samples aggregated featured values). To be more specific, data integrity is evaluated as the percentage ratio of data that are not modified by any cloud users to the overall sample instances. The data integrity is mathematically represented as given below.

$$DI = \sum_{i=1}^{m} \frac{S_{NM}}{S_i} * 100 \quad (17)$$

From the above equation (17) the data integrity 'DI' is evaluated by considering the sample instances considered for simulation 'S_i' and the number of sample data that were not modified by any malicious cloud users 'S_{NM}'. It is measured in terms of percentage and higher rate ensures the efficiency of the method. Comparison table of the proposed Brower BN-SNN method with existing methods DECR and EPRS in terms of data confidentiality and data integrity is shown in Table 2 for data sample ranging between 400 and 4000.

Figure 4 given above illustrates the data confidentiality rate using the three methods, proposed Brower BN-SNN method with existing methods DECR and EPRS respectively. From the above figure it is observed that increasing the sample size from 400 to 800 observed an initial declining inclination using all the three methods. However, with the increase in samples again a stable result was observed using the proposed Brower BN-SNN method that corroborates the objective that increasing samples does not compromise data confidentiality rate. Nevertheless, simulations performed for the three methods saw comparatively better results using the proposed Brower BN-SNN method than and. This is inferred from the simulation results with 400 samples provided as input and actually 380 samples to be the intended cloud users to receive the data, using the proposed Brower BN-SNN method it was observed to be 370 and 360, 350 using and respectively, therefore the overall data confidentiality was found to be 97.36%, 95.26% and 92.10% respectively. This inference shows that the data confidentiality using Brower BN-SNN method to be comparatively better. The reason was by applying the Brouwer Fixed Point-based compression algorithm for each input samples obtained from different WBAN sensors, via compact convex set compression was performed in an efficient manner. This in turn protected the sensitive medical data from the unauthorized access, therefore improving the overall data confidentiality using Brower BN-SNN method by 9% compared to and 25% compared to respectively.

Figure 5 given illustrates the data integrity using the three methods, proposed Brower BN-SNN method, DECR and EPRS respectively. Fair comparison between the three methods were ensured by employing similar numbers of health sample featured data as input to evaluate the data integrity for an average of 10 simulations runs. From the above figure though an increasing trend was found increasing the sample sizes between 400 and 2400, following a decreasing trend between 2400 and 2800, however the data integrity rate rose for the final set of samples, therefore validating the proposed method that increased sample size does not compromises the overall data integrity for all the three methods for an average of 4000 samples. Nevertheless, relative figurative representation showed a significant improvement was inferred when applying proposed Brower BN-SNN method. The contributing improving factor for data integrity was owing to the application of Brouwer Fixed Point-based compression that with the aid of fixed-point continuous function was initially applied to all the featured samples obtained at different time intervals. Second, the resultant function was subjected to compact convex set. Finally, Brouwer Fixed Point function was applied to generate the corresponding results into reduced form, therefore forming WBAN messages or frames, therefore assuring that the information is trustworthy. This in turn assisted in reducing the WBAN messages not to be changed by the malicious users, therefore improving the data integrity using Brower BN-SNN method by 32% compared and 54% compared Arafat, M. Y., Pan, S., & Bak, E. (2023), Memon, S., Wang, J., Ahmed, A., Rajab, A., Al Reshan, M. S., Shaikh, A., & Rajput, M. A. (2023).

Performance analysis of authentication accuracy and disease diagnosis accuracy

Authentication accuracy is defined as the percentage ratio of number of cloud users correctly authenticated as authorized or unauthorized to the total number of cloud users in the cloud environment by the cloud server. The mathematical formulates for measuring the authentication accuracy is expressed as given below

$$AA = \sum_{i=1}^{m} \frac{(CU|Auth, NAuth \rightarrow CS)}{CU_i} * 100 \quad (18)$$

Table 3: Tabulation of authentication accuracy and disease diagnosis accuracy

Samples	Authentication accuracy (%)			Disease diagnosis accuracy (%)		
	Brower BN-SNN	DECR	EPRS	Brower BN-SNN	DECR	EPRS
400	98.61	96.66	94.44	85	80	75
800	96.36	95.25	85.2	83.35	73.25	68.15
1200	95	93.25	83.2	81	70	65
1600	93.15	91.85	81.8	79.55	65.45	60.35
2000	92	86	76	77.25	67.15	62.05
2400	91.35	84.35	74.3	75	65	60
2800	91.85	84.85	74.8	75.85	65.75	60.65
3200	92.35	85.15	75.1	77	67	62
3600	93.35	86.35	76.3	79.35	69.25	64.15
4000	94	87.25	77.2	82.45	72.35	67.25

From the above equation (18) authentication accuracy 'AA' is measured based on the number of cloud users involved in the simulation process 'CU_i' and the number of cloud users correctly authenticated as either authorized or not authorized by the cloud server '$CU|Auth, NAuth \rightarrow CS$'. The authentication accuracy is measured in terms of percentage (%). Next, disease diagnosis accuracy is formulated as given below.

$$DD_{Acc} = \sum_{i=1}^{m} \frac{S_{AD}}{S_i} * 100 \quad (19)$$

From the above equation (19) the disease diagnosis accuracy 'DD_{Acc}' is measured by considering the samples 'S_i' and the samples accurately detected 'S_{AD}' as it is. It is measured in terms of percentage (%). Comparison table of the proposed Brower BN-SNN method with existing methods DECR and EPRS in terms of authentication accuracy and disease diagnosis accuracy is shown in Table 3 for sample ranging between 400 and 4000 Arafat, M. Y., Pan, S., & Bak, E. (2023), Memon, S., Wang, J., Ahmed, A., Rajab, A., Al Reshan, M. S., Shaikh, A., & Rajput, M. A. (2023).

Figure 6 given above shows the graphical representations of authentication accuracy using the three methods. From the figurative representation it is evident that the authentication accuracy and disease diagnosis accuracy using proposed Brower BN-SNN method is found to be comparatively higher. Also with sample provided as 400 and actually authenticated cloud users being 360 using the proposed Brower BN-SNN method it was observed to be 355 and using existing methods it was found to be 348 and 340 respectively, therefore the overall authentication accuracy rate using the three methods were observed to be 98.61%, 96.66% and 94.44% respectively. The reason for the improvement when applied with the proposed Brower BN-SNN method was owing to the application of Blowfish cryptography enhanced by Nash Equilibrium the security was enhanced and therefore reduced the false acceptance and false rejection rate subsequently. Also, sub-keys was

Table 4: Tabulation of response time

Samples	Response time (ms)		
	Brower BN-SNN	DECR	EPRS
400	10	13.2	16
800	15.85	21.25	28.95
1200	21	28.35	35
1600	25.85	35.55	48.65
2000	35	48.35	60.35
2400	41.25	55.25	70.35
2800	48	62.15	80.35
3200	55.35	68.35	95.25
3600	60	75.25	100.35
4000	65.85	82	115.25

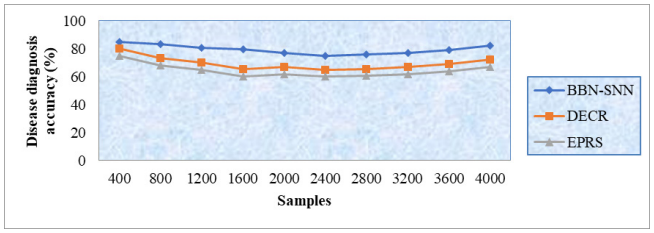

Figure 7: Disease diagnosis accuracies versus samples

generated by cloud server with which the communication between the cloud users have to be performed and also the sub-keys generated by cloud server are different for different iterations, therefore ensuring confirmation of the cloud users. As a result only with the verified cloud users by the cloud server communication was established between them and transmission was made and also authorization was made via two-stage where access control was made via the generated sub-keys. This in turn improved the authentication accuracy using proposed Brower BN-SNN method by 5% Arafat, M. Y., Pan, S., & Bak, E. (2023), Memon, S., Wang, J., Ahmed, A., Rajab, A., Al Reshan, M. S., Shaikh, A., & Rajput, M. A. (2023).

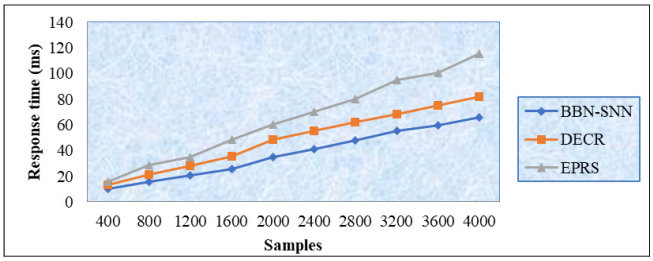

Figure 8: Response time versus samples

Figure 7 given above depicts the performance of the three methods in terms of disease diagnosis accuracy. It can be clearly seen that the disease diagnosis accuracy is improved using the proposed Brower BN-SNN method upon comparison. For a sample of 400 being tested for simulation and actual patient diagnosed with disease to be 20, 17 samples were identified using Brower BN-SNN method and 16, 11 using existing methods. There, fore the overall disease diagnosis accuracy using the three methods were found to be 855, 80% and 75% respectively, therefore improvement observed using BROWER BN-SNN method. This is because round function employed in our work via sub-key generation for each plain text or the compressed WBAN messages into two equal pieces XOR with left to obtain personal information of cloud users or patient whereas XOR with right to obtain the vital sign information that which are used in diagnosing the overall results. This in turn results in the enhancement in disease diagnosis accuracy using Brower BN-SNN method by 15% compared to 24% compared to Arafat, M. Y., Pan, S., & Bak, E. (2023), Memon, S., Wang, J., Ahmed, A., Rajab, A., Al Reshan, M. S., Shaikh, A., & Rajput, M. A. (2023).

Performance analysis of response time

With the objective of minimizing the number of transmissions with endpoint detection and response for IoT enabled encryption and decryption the response time has to be formulated. The response time is mathematically formulated as given below.

$$RT = \sum_{i=1}^{m} CU_i * Time\ [Enc + Dec] \quad (20)$$

From the above equation (20) response time 'RT' is measured by considering the cloud users 'CU_i' or WBAN sensors ready for communicating with other users and the time consumed in encrypting the decrypting '$Time\ [Enc + Dec]$'. Here, not only authorization should be successful but also the response time should be low that in turn reduce the number of transmission with endpoint detection in an accurate manner. Finally, comparison table of the proposed Brower BN-SNN method with existing methods DECR and EPRS in terms of response time is shown in Table 4 for 10 simulation runs Arafat, M. Y., Pan, S., & Bak, E. (2023), Memon, S., Wang, J., Ahmed, A., Rajab, A., Al Reshan, M. S., Shaikh, A., & Rajput, M. A. (2023).

Finally, Figure 8 given above shows the response time using the three methods, Brower BN-SNN, DECR and EPRS. The response time here refers to both the encryption and decryption process performed by the cloud server whenever communication between WBAN sensors has to be made. From the figure it is inferred that increase in sample size causes an increase in the overall WBAN compressed messages. However, with simulations performed for 400 samples the end point detection and the response was found to be better by observing an overall of 10ms using proposed BBN-SNN, 13.2ms using and 16ms using respectively. From this with the end point detection or the authentication accuracy with improved authorization playing a major role the response was also high using proposed Brower BN-SNN method. One of the reasons was by applying the Stochastic Neural Network a two-stage authorization wherein the second stage authorization performed the detection of any anomaly via activation condition of hidden units and activation condition of visible units. This in turn detected any anomaly at an early stage itself and therefore reducing the response time using proposed Brower BN-SNN method by 24% compared and 42% compared to Arafat, M. Y., Pan, S., & Bak, E. (2023), Memon, S., Wang, J., Ahmed, A., Rajab, A., Al Reshan, M. S., Shaikh, A., & Rajput, M. A. (2023).

Conclusion

WBAN is a new inclination in the technology that imparts remote mechanism for patient health monitoring making use of wearable sensors. It is extensively identified that an extremely high security and privacy play a major part in safeguarding these sensitive data when being utilized by the healthcare professionals and in the course of storage to make certain that patient's records are retained in a safe manner from malicious users. Recently, several secured disease diagnosis algorithms have been developed. In this work a suitable method called, Brower Blowfish Nash-secured Stochastic Neural Network-based (Brower BN-SNN) disease diagnosis and anomaly detection is developed to further improve the overall performance. First, the health monitoring and BETH raw dataset was obtained and subjected to Brouwer Fixed Point-based compression for ensuring data confidentiality and data integrity. Followed by which the compressed sample featured data was applied with a Blowfish Nash Equilibrium-based encryption and decryption wherein disease diagnosis results were encrypted and correspondingly decryption was performed for different WBAN sensors for further processing. Finally, using Stochastic Neural Network-based anomaly detection algorithm precise and accurate detection of anomaly was said to be ensured. A panoramic experimental assessment is done employing different performance metrics like, data confidentiality, data integrity, disease diagnosis accuracy, authentication accuracy and response time for different

numbers of samples. The comprehensive performance results exemplify that the presented Brower BN-SNN method achieves higher data confidentiality and data integrity with minimum response time than the traditional methods considered for comparison.

References

Abubeker, K. M., & Baskar, S. (2022). Wireless sensor and wireless body area network assisted biosensor network for effective monitoring and prevention of non-ventilator hospital-acquired pneumonia. *Frontiers in Sustainable Cities*, *4*, 1063067.

Ali, A., & Khan, F. A. (2013). Energy-efficient cluster-based security mechanism for intra-WBAN and inter-WBAN communications for healthcare applications. *EURASIP Journal on Wireless Communications and Networking*, *2013*, 1-19.

Ananthi, J. V., & Jose, P. S. H. (2021). A perspective review of security challenges in body area networks for healthcare applications. *International Journal of Wireless Information Networks*, *28*(4), 451-466.

Arafat, M. Y., Pan, S., & Bak, E. (2023). Distributed energy-efficient clustering and routing for wearable IoT enabled wireless body area networks. *IEEe Access*, *11*, 5047-5061.

Auko, J. (2023). Current security and privacy posture in wireless body area networks. *World Journal of Advanced Research and Reviews*, *18*(3), 1185-1206.

Devi, R. A., & Arunachalam, A. R. (2023). Enhancement of IoT device security using an Improved Elliptic Curve Cryptography algorithm and malware detection utilizing deep LSTM. *High-Confidence Computing*, *3*(2), 100117.

Gugueoth, V., Safavat, S., & Shetty, S. (2023). Security of Internet of Things (IoT) using federated learning and deep learning—Recent advancements, issues and prospects. *ICT Express*, *9*(5), 941-960.

Izza, S., Benssalah, M., & Drouiche, K. (2021). An enhanced scalable and secure RFID authentication protocol for WBAN within an IoT environment. *Journal of Information Security and Applications*, *58*, 102705.

Khan, H. U., Sohail, M., Ali, F., Nazir, S., Ghadi, Y. Y., & Ullah, I. (2023). Prioritizing the multi-criterial features based on comparative approaches for enhancing security of IoT devices. *Physical Communication*, *59*, 102084.

Kumar, M., & Hussain, S. Z. (2023). An efficient and secure mutual authentication protocol in wireless body area network. *EAI Endorsed Transactions on Pervasive Health and Technology*, *9*.

Li, M., Lou, W., & Ren, K. (2010). Data security and privacy in wireless body area networks. *IEEE Wireless communications*, *17*(1), 51-58.

Memon, S., Wang, J., Ahmed, A., Rajab, A., Al Reshan, M. S., Shaikh, A., & Rajput, M. A. (2023). Enhanced probabilistic route stability (EPRS) protocol for healthcare applications of WBAN. *IEEE Access*, *11*, 4466-4477.

Mohanty, M. D., Das, A., Mohanty, M. N., Altameem, A., Nayak, S. R., Saudagar, A. K. J., & Poonia, R. C. (2022, July). Design of smart and secured healthcare service using deep learning with modified SHA-256 algorithm. In *Healthcare* (Vol. 10, No. 7, p. 1275). MDPI.

Pavithra, D., Nidhya, R., Shanthi, S., & Priya, P. (2023). A secured and optimized deep recurrent neural network (DRNN) scheme for remote health monitoring system with edge computing. *Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije*, *64*(3), 508-517.

Rani, S., Kataria, A., Kumar, S., & Tiwari, P. (2023). Federated learning for secure IoMT-applications in smart healthcare systems: A comprehensive review. *Knowledge-based systems*, *274*, 110658.

Reddy, V. S., & Debasis, K. (2023). DLSDHMS: Design of a deep learning-based analysis model for secure and distributed hospital management using context-aware sidechains. *Heliyon*, *9*(11).

Singla, R., Kaur, N., Koundal, D., & Bharadwaj, A. (2022). Challenges and developments in secure routing protocols for healthcare in WBAN: A comparative analysis. *Wireless Personal Communications*, 1-40.

Singla, R., Kaur, N., Koundal, D., Lashari, S. A., Bhatia, S., & Rahmani, M. K. I. (2021). Optimized energy efficient secure routing protocol for wireless body area network. *IEEE Access*, *9*, 116745-116759.

Veerabaku, M. G., Nithiyanantham, J., Urooj, S., Md, A. Q., Sivaraman, A. K., & Tee, K. F. (2023). Intelligent Bi-LSTM with architecture optimization for heart disease prediction in WBAN through optimal channel selection and feature selection. *Biomedicines*, *11*(4), 1167.

Visalaxi, G., & Muthukumaravel, A. (2023). IOT monitoring membrane computing based on quantum inspiration to enhance security in cloud network. *Measurement: Sensors*, *27*, 100755.

Wang, N., Fu, J., Zhang, S., Zhang, Z., Qiao, J., Liu, J., & Bhargava, B. K. (2022). Secure and distributed IoT data storage in clouds based on secret sharing and collaborative blockchain. *IEEE/ACM Transactions on Networking*, *31*(4), 1550-1565.

Zhou, R., Zhang, X., Wang, X., Yang, G., Dai, H. N., & Liu, M. (2021). Device-oriented keyword-searchable encryption scheme for cloud-assisted industrial IoT. *IEEE Internet of Things Journal*, *9*(18), 17098-17109.

Zou, S., Xu, Y., Wang, H., Li, Z., Chen, S., & Hu, B. (2017). A survey on secure wireless body area networks. *Security and communication networks*, *2017*(1), 3721234.