International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 10-No.4 (2024) pp. 671-681
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

Secured Fog-Body-Torrent : A Hybrid Symmetric Cryptography with Multi-layer Feed Forward Networks Tuned Chaotic Maps for Physiological Data Transmission in Fog-BAN Environment

S. Parvathy[1,*] and A. Packialatha[2]

[1] Department of CSE, Vels Institute of Science, Technology and Advanced Studies, Chennai, 600117, India ,
*** Corresponding Author Email:** maheshsparvathy@gmail.com - **ORCID:** 0009-0004-0666-5924

[2] Department of CSE, Vels Institute of Science, Technology and Advanced Studies, Chennai, 600117, India ,
Email: packialatha.se@velsuniv.ac.in - **ORCID:** 0000-0001-7374-1262

Article Info:

DOI: 10.22399/ijcesen.490
Received : 08 October 2024
Accepted : 10 October 2024

Keywords :

Wireless Body Area Network,
Internet of Things (IoT),
Scroll Chaotic maps,
Feed Forward layers

Abstract:

Recently, the Wireless Body Area Networks (WBAN) have become a promising and practical option in the tele-care medicine information system that aids for the better clinical monitoring and diagnosis. The trend of using Internet of Things (IoT) has propelled the WBAN technology to new dimension in terms of its network characteristics and efficient data transmission. However, these networks demand the strong authentication protocol to enhance the confidentiality, integrity, recoverability and dependability against the emerging cyber-physical attacks owing to the exposure of the IoT ecosystem and the confidentiality of biometric data. Hence this study proposes the Fog based WBAN infrastructure which incorporates the hybrid symmetric cryptography schemes with the chaotic maps and feed forward networks to achieve the physiological data info security without consuming the characteristics of power hungry WBAN devices. In the proposed model, scroll chaotic maps are iterated to produce the high dynamic keys streams for the real time applications and feed-forward layers are leveraged to align the complex input-output associations of cipher data for subsequent mathematical tasks. The feed forward layers are constructed which relies on the principle of Adaptive Extreme Learning Machines (AELM) thereby increasing randomness in the cipher keys thereby increasing its defensive nature against the different cyber-physical attacks and ensuring the high secured encrypted-decrypted data communication between the users and fog nodes. The real time analysis is conducted during live scenarios. BAN-IoT test beds interfaced with the heterogeneous healthcare sensors and various security metrics are analysed and compared with the various residing cryptographic algorithms. Results demonstrates that the recommended methodology has exhibited the high randomness characteristics and low computational overhead compared with the other traditional BAN oriented cryptography protocol schemes.

1. Introduction

A wireless Body Area Network (WBAN) is considered as the one of the recent innovations that can dispatch real-time preventative and proactive diagnosis at a affordable cost [1]. For an effective data collection used for monitoring and clinical applications, WBANs are equipped with the low – power, intelligent bio medical healthcare sensors that are attached to the human body that collects the physiological data and then transmits wirelessly to the remote area that can be used for the further clinical processing [2-4]. The recent advances in Internet of things (IoT) coupled with miniature sensors and pervasive wireless connectivity has contributed emergence of WBANs. Today, BAN – IoT may be considered as the most favoured options for transmitting the medical data due to its high data rate and its cost of implementation [5-7].
In BAN-IoT systems, the protection of patient-related information and medical communications is of utmost importance, as these data must be safeguarded against potential malfunctions. However, due to the inherently open nature of BAN-IoT networks, they are susceptible to a

variety of cyber threats. As a result, a robust and secure architecture is essential to ensure the safety of physiological data transmitted via BAN-IoT networks. Two primary security concerns in WBANs are confidentiality and authentication, which require careful consideration. Typically, encryption techniques [8-12] and digital signatures [13-16] serve as solutions to these issues. When both confidentiality and authenticity need to be ensured simultaneously, the sign-then-encrypt method [17-18] is frequently utilized. Nevertheless, BAN-IoT devices are often constrained by limited energy and processing capabilities, which pose challenges to implementing complex cryptographic methods.

Hence the traditional mathematical encryption operation such as substitution and transposition methods such as shift cipher, affine cipher, exclusive XOR, Hill cipher and hash functions are adopted to ensure the high-end security to medical data transmitted. But these methods suffer from the following drawbacks:

1. Usage of Traditional encryption techniques may lead to the formation of the fixed keys which can be easily broken by the intruders.
2. Since the BAN-IoT networks are battery hungry devices, deploying the more mathematical operations to perform the strong encryption algorithms in the BAN devices suffers from more computational overhead.

Motivated by the above drawbacks, this research article proposes the Hybrid Secure Fog-Body Torrent (Secure Fog-Body Torrents) protocol to combat the different cyber-attacks, by incorporating the principle of Chaos Maps and Adaptive Extreme Learning Feed Forward Networks to produce the high randomness and unpredictable cryptography protocols with less computational overhead. The fundamental contribution of this work is outlined below

1. Replaces the conventional BAN-IoT structure with the Fog Based BAN-IoT to enable the high-speed communication between the BAN-users, Fog gateways and Cloud.
2. Proposes the Hybrid Encryption Scheme based on Scroll Maps to produce the High randomness keys to defend against the multiple-attacks.
3. Deploys the powerful Feed forward Networks based on Adaptive Extreme Learning Machines (AELM) for non-linear mapping of the input and output features which can fuelled to produce the high randomness key.
4. Performance is evaluated using the NIST standard techniques and computational overhead is calculated and assessed with the various residing encryption-decryption methodologies for BAN-IoT networks
5. Conducts the BAN Formulation analysis for the proposed protocol

The organization of this paper is as follows: Section 2 surveys the related work proposed by different researchers. Section 3 details the proposed methodology. Section 4 covers the experiments, evaluation criteria, and results analysis. Lastly, Section 5 presents the conclusions and future work.

2. Related Work

In this section, various encryption methods designed for Wireless Body Area Networks (WBAN) are examined, focusing on their research objectives, security criteria, and computational efficiency. Amin et al. [19] introduce an innovative hybrid key establishment method tailored for Body Area Networks (BAN), which combines symmetric cryptography with sign-encryption techniques. This approach involves the selection of a cluster head, session key generation, and offers the benefits of reduced computational costs and communication overhead. The proposed algorithm effectively addresses key security concerns, including confidentiality, protection against replay attacks, integrity, and authentication. Nevertheless, the scheme is energy-intensive and requires higher bandwidth due to the use of the Elliptic Curve Cryptosystem (ECC). Additionally, it faces challenges related to certificate renewal and revocation.

Wang and Liu [20] introduced a ring signature encryption technique employing an attribute-based cryptosystem tailored for Wireless Body Area Networks (WBANs). This scheme's robustness and efficiency hinge on the computational Diffie-Hellman (CDH) assumption within the context of bilinear pairing. It fulfills multiple security criteria, including authenticity, non-repudiation, and confidentiality. Nevertheless, this approach does not resolve the key escrow issue since the Hospital Authority (HA) acts as the Private Key Generation (PKG) center, responsible for creating the private keys for both the controller and data users (such as doctors, researchers, and emergency personnel). Consequently, the HA could potentially misuse the user’s private key to forge signatures. Additionally, the scheme’s efficiency relies on bilinear pairing, which demands substantial energy and bandwidth

Jothi and Srinivasan [21] proposed the methodology which is based on the attribute-based cryptosystem with ring encryption. The authors deployed ant-colony optimization with fuzzy ontology in WBAN to achieve the better security applications when compared with the existing

elliptic curve-based encryption schemes. Their methodology also accommodates multiple security features including authentication, resistance to forgery, confidentiality, public verification, data integrity, non-repudiation, and forward secrecy. However, it has two significant limitations: the unreliable distribution of keys and the necessity for a secure channel to distribute private keys.

Prameela [22] introduced an enhanced approach leveraging certificateless signcryption combined with anonymous mutual authentication to manage access control in Wireless Body Area Networks (WBANs). This method incorporates a chaos baker map scheme along with an XOR operation and a one-way hash chain function for robust authentication. Experimental findings reveal that this technique outperforms existing algorithms in terms of energy efficiency, end-to-end latency, coverage duration, packet delivery ratio, and throughput. However, it faces challenges such as elevated computational overhead and bandwidth consumption due to the use of bilinear pairing. Additionally, it demonstrates weaker resistance to replay attacks. Khan et al. [23] proposed a diverse encryption strategy for Wireless Body Area Networks (WBANs) that shifts from an identity-based cryptosystem to a public key infrastructure (PKI) incorporating an equality test (HSCIP-ET). This approach allows sensors in the identity-based cryptosystem to secure crucial information using the management center's public key within the PKI framework before transmitting it to the cloud server. But this methodology again suffers from the high computational overhead and fulfilling the security goals. Amudha et.al [24] proposed chaotic encryption scheme for Fog based BAN –IoT networks in which the logistic maps are incorporated to achieve the better security goals. The experimental results demonstrated that the recommended model has shown the better security performance than the residing algorithm. But the authors fail to elaborate their model in achieving the security goals. Moreover, computational overhead and energy consumption is not been considered as the major parameter for evaluating the model in which these parameters are affected badly when deploying the model in the real time clinical applications.

3. Proposed Methodology

This segment introduces the system model, overview of the Fog-BAN-IoT encryption and decryption process using the proposed hybrid scroll maps and adaptive extreme learning machines.

3.1 System Model:

The system model considered for Fog-BAN-IoT topology is shown in Figure 1. The setup features multiple IoT devices interfaced with a fog gateway and analytical outputs are fed into the cloud for the further processing. Devices can only communicate with other devices through the Fogs by means of wireless communication approaches such as WIFI, LORA, and BLE. The IoT devices involved in this model are small-size, memory and energy constraint devices.

Encryption process take place in the BAN-IoT devices whereas decryption process take place in Fog gateways. A small amount of megabytes (MB) of RAM is also essential for facilitating communication between the device and Fog gateway. The system model presumes that the suggested protocol network topology is established in a safeguarded area where attackers do not have physical access to the devices. Thus, they cannot access the configured secret keys that are preserved on the devices.

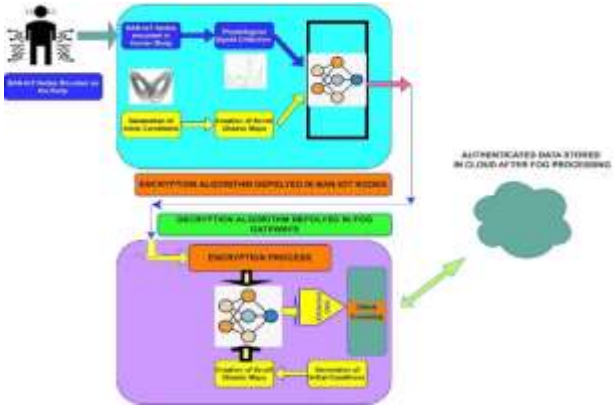


Figure 1: *Secured Fog-Body Torrents Proposed Deployment Architecture*

3.2 System Overview:

The proposed protocol provides a secure encryption and decryption process between the BAN devices, Fog gateways and users. It enhances the security robustness of IoT network. As mentioned in the System Model, intermediate Fog gateways are deployed between the BAN devices gateways and cloud. The recommended protocol has the following attributes (i) This protocol assures secure encryption and decryption process between the BAN devices and Fog gateways. (ii) The protocol relies on two primary secret keys such as encryption key (E_e) and decryption key (E_d). The keys are upgraded after a pre-defined session time due to the chaotic

characteristics that are incorporated in the key formation. The encryption keys are deployed in the BAN-IoT nodes [25-29] whereas decryption will be in Fog gateways(iii) The proposed protocol used novel encryption and decryption process which is primarily based on the scroll chaotic maps with adaptive extreme learning machines. Hence the key which is formulated will exhibit the high randomness nature in which prevents the attackers to get the information (iv). The proposed protocol has been designed between the IoT devices [30] fog gateways and users which reduces the energy consumption and minimizes the message exchange in the mean time of data transportation and communication phase [31]. The list of abbreviations are utilized in this research is listed in table 1.

Table 1 *List of Abbreviations Used in the Article*

Sl.no	Notations	Description
1	E_e	Permanent Encryption Key stored in the IoT devices and Fog gateways
2	E_d	Decryption Key Updated for the Each and Every Session
3	E_i	Initial key used for the Up-dation
6	$Session_{(T)}$	Session time for the updating the key
7	$Session_{(T+1)}$	Session time for the updating the key at the next time
8	$Seq_{\{i\}}$	Random Sequence generated for the session time-key update
9	$Seq_{\{i+1\}}$	Random Sequence generated for the session {i+1} time-key update
10	M	Key length
11	B1, B2	Random sequences generated for each challenge.
12	SCAELM	Scroll chaotic Maps based on adaptive ELM (Extreme Learning Machines)

3.3 Scroll Chaotic Key Generation:

For the development of extremely random and non-periodic sequences, this paper employs scroll maps, which rely on the principle of multi-scroll attractors. Multi-scroll attractors are chosen over other chaotic maps, including sine, circle, tent, and logistic maps, because they offer greater randomness and the ability to control chaotic behavior through initial conditions. The properties of the scroll maps for key generation are outlined in the preceding section.

3.4 Multi-Scroll Attractors:

Systems characterized by multiple-scroll attractors can exhibit more complex behaviors than standard chaotic systems with mono-scroll attractors. The State Space representation for these automated chaotic systems is provided by

$$i_1 = -ai_1 + bi_2 i_3 \quad (1)$$

$$i_2 = -ci_2^3 + di_1 i_3 \quad (2)$$

$$i_3 = ei_3 - fi_1 i_2 \quad (3)$$

The equation (1), (2), (3) can be altered by the adding the hyperbolic equation $p_1\, tanh(i_2 + g)$ which is given in eqn

$$i_1 = -ai_1 + bi_2 i_3 \quad (4)$$

$$i_2 = -ci_2^3 + di_1 i_3 \quad (5)$$

$$i_3 = ei_3 - fi_1 i_2 + p_1\, tanh(i_2 + g) \quad (6)$$

Chaotic attractor is obtained when $a = 2$, $b = 6$, $c = 6$, $d = 3$, $e = 3$, $f = 1$, $p_1 = 1$, $g = 2$.

In the first phase, the hyperbolic function with g=-3 and initial conditions [0.1, -0.1, -0.6] results in a double-scroll attractor, represented in Figure 1. In the second phase, with parameters p_1=-1, g=3 and the same initial conditions, a four-scroll attractor is evident, as shown in Figure 2. The third phase, with p_1=1, g=3 and initial conditions [0.1, 0.1, 0.6], reveals a single-scroll attractor, as depicted in Figure 3 and 4. Therefore, the system confirms its multiscroll nature. For the purpose of developing multi-scroll 3D fractional/integer-order chaotic systems, the equations are refined through derivative properties. The ultimate chaotic system that can show multi-scroll traits is given as:

$$\frac{d^q i_1}{dt^q} = -ai_1 + bi_2 i_3 \quad (7)$$

$$\frac{d^q i_2}{dt^q} = -ci_2^3 + di_1 i_3 \quad (8)$$

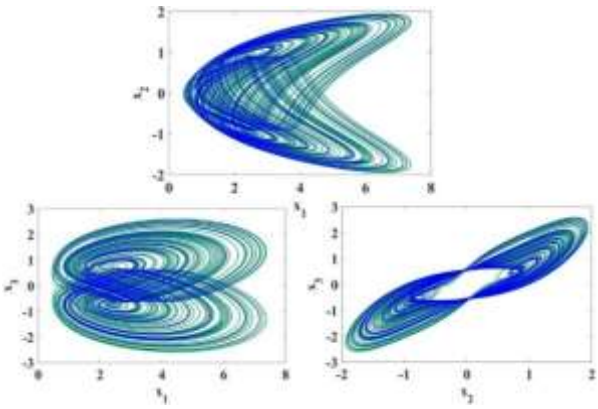


Figure 2: *Phase portraits of cubic nonlinear system with $p_1\, tanh(x_2 + g)$ function in 1st state*

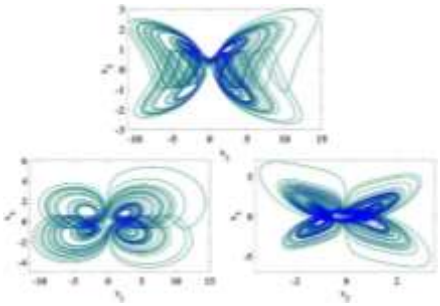


Figure 3: *Phase portraits of cubic nonlinear system with $p_1\ tanh(\ x_2 + g)$ function in 2nd state*

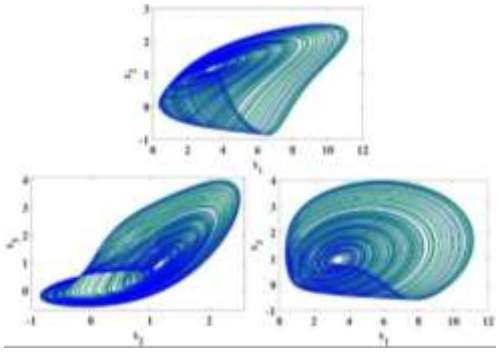


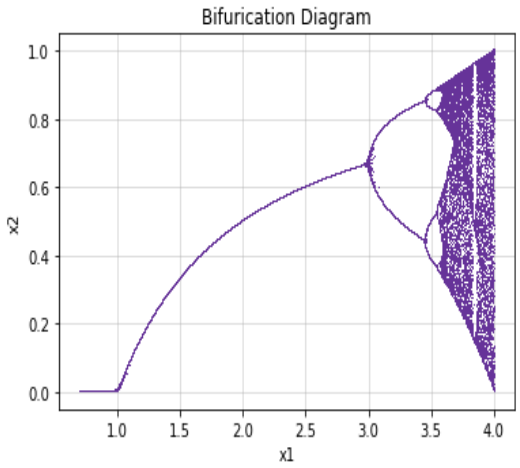
Figure 4: Phase portraits of cubic nonlinear system with $p_1\ tanh(\ x_2 + g)$ function in 3rd state

$$\frac{d^q i_3}{dt^q} = ex_3 - fi_1 i_2 + p_1\ tanh(\ i_2 + g) \quad (9)$$

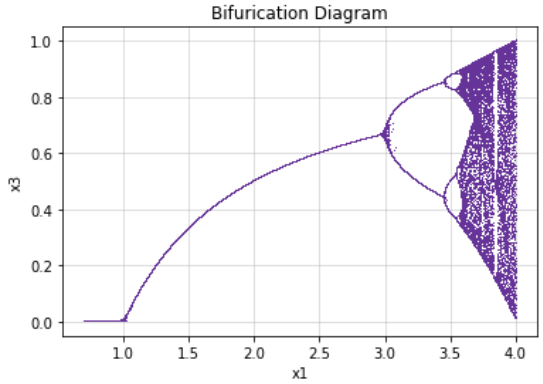
Figure 5 presents the bifurcation diagram of the multi-scroll integer-order chaotic systems being proposed.

3.4.1 Multi-Scroll Attractor – Its Advantages:

The upcoming pros of the recommended scroll attractors applied to encryption are summarized below



(a)



(b)

Figure 5: *Fractional Bifurcation Diagrams for the Recommended Multi Scroll Chaotic Systems*

1. The system requires less memory to produce an equivalent number of scrolls, as it utilizes fewer components for their generation [25].
2. Random scrolls can be created by altering any component in any direction, which sets this feature apart from other chaotic systems.
3. Scroll maps are categorized as adaptable maps, where the randomness is independent of the number of scrolls, unlike other methods where randomness is closely tied to the quantity of initial values.

3.5 Chaotic Key Generation Process:

The following steps are incorporated for the generation of the keys used for encryption and decryption

Step 1: Generation of Random Patterns Using Scroll Map Function with Different Starting Points and Specific Control Settings varies from -3.4889829 to 10.8393

Step 2: Selection of non-ordered sequence numbers (no repeating) among M data length to set the BAN Secret keys (BSK)

Step 3: Selection of random BSK for the encryption of the medical

3.6 Adaptive Feed Forward Networks Based Encryption and Decryption:

In this study, Feed Forward Neural Networks (FFNN) which relies on the principle of Extreme Learning Machines (ELM) are constructed. The working principle of ELM is detailed:

3.6.1 Extreme Learning Machines – An Overview:

The put forward model applies the principle of extreme learning machines suggested for quick and

accurate grading classification. This type of neural network consists of single hidden layers, where tuning is not a mandatory requirement.

ELM employs the kernel function to attain high accuracy, leading to better performance. Major benefits of ELM are its low training error and improved approximation. With its use of auto-tuned weight biases and non-zero activation functions, ELM finds utility in classification and value prediction.

In this kind of model, the 'L' neurons in the hidden layer must utilize an activation function that is significantly differentiable (for instance, the sigmoid function), while the output layer employs a linear activation function. In ELM, there is no requirement to tune the hidden layers. The hidden layer in ELM is not mandatory to be fine-tuned. The weights of the hidden layer are assigned arbitrarily (including bias weights). Although the hidden nodes are not insignificant, they do not require tuning, and the parameters of the hidden neurons can be randomly set before handling the training dataset.

$$f_L(x) = \sum_{i=1}^{L} B_i Q_i(x) = Q(x)B \quad (10)$$

Where x → input features from encoder-decoder

B → output weight vector and it is given as follows as

$$B = [B_1, B_2, \dots\dots\dots\dots B_L]^T \quad (11)$$

H(i)→ output hidden layer which is given by the following eqn

$$Q(x) = [Q_1(i), Q_2(i), \dots\dots\dots\dots Q_L(i) \quad (12)$$

$$H = \begin{bmatrix} Q(i_1) \\ Q(i_2) \\ \vdots \\ Q(i_N) \end{bmatrix} \quad (13)$$

The primary implementation of the ELM makes use of simple non-linear least squares approaches, illustrated in equation (14).

$$B' = H^*O = H^T(HH^T)^{-1}O \quad (14)$$

Where H∗ → inverse of H known as Moore−Penrose generalized inverse.

$$B'\, H^T(\frac{1}{C}HH^T)^{-1}O \quad (15$$

$$f_L(x) = Q(i)\beta = Q(i)\, H^T(\frac{1}{C}HH^T)^{-1}O \quad (16)$$

To design the effective encryption and decryption process, multi-layer ELM networks is designed which comprises of an input layer, concatenation layer and an output layer. Figure 6 presents the complete cycle of creation of encrypted and decrypted data. Table 2 and 3 present the number of parameters utilized for the implementing the network.

***Table 2**: Training Parameters used for the designing the proposed network used for Encryption*

Parameters	Specifications
Hidden Layers count	10
Epochs count	50
LR	0.001
BS	05
Momentum	0.2

***Table 3** Training Parameters used for the designing the proposed network used for Input physiological datasets*

Parameters	Specifications
No of Hidden layers	20
Epochs count	100
LR	0.001
BS	10
Momentum	0.19

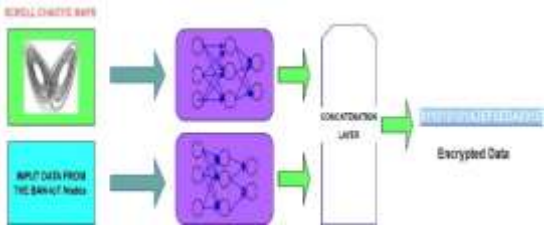


***Figure 6**: Overall Architecture for the Proposed AELM for Encryption of the Input Data*

The pattern node quantity is defined relies on the cipher key dimensions for length M. The proposed network is a non-linear regression model that maps the dynamic relationship among the BSK_1 and BSK_2 as a non-linear curve-fitting applications. Equation (17) is modified for the representation of the encryption process and decryption process

$$f_D(i) = Q(D)B(d) = Q(D)\, H^T(\frac{1}{C}Q'Q'^T)^{-1}Y \quad (17)$$

Above Equation (17) represents the training outputs from the proposed network with the physiological data signals as the output.

$$f_{BSK1}(x) = BSK(D)\beta(d) = (18)$$

Where M is the length of the input sequence. Equation (18) represents the output function from the proposed network with the scroll chaotic input

sequences used for the encryption. Finally, Equation (19) represents the output encryption function obtained after the concatenation layer of the ELM's networks

$$F(E) = Concat\left(f_D(i), f_{BSK1}(i)\right) \quad (19)$$

Similarly, output function used for the decryption is Illustrated in Equation (20) and Equation (21)

$$f_{BSK2}(x) = BSK2(D)\beta(d) \quad (20)$$

$$F(D) = Concat\left(F(E), f_{BSK2}(i)\right) \quad (21)$$

Where F(E) represents the complete encrypted data and F(D) represents the decryption key used for decrypting the data which is implemented in Fog gateways.

4. Experimental Outcomes and Analysis

Here, we execute experimentation to assess the recommended model, with metrics such as cost and time evaluated and compared against other advanced learning models. Additionally, BAN logic is formulated for the verification of the protocol.

4.1 Experimentation

The analysis is undertaken with the BAN-IoT nodes interfaced with the five physiological medical sensors. These sensors are employed to acquire the information from the subjects which are processed by the embedded processors to transmit to the fog gateways. Fog gateways are implemented using the high-end embedded processors (Cortex A-53 processors). WIFI is used as the communication medium between the BAN-IoT nodes and Fog gateways. The complete experimentation is carried out in using the Python 3.10 and Tensorflow 2.10 (Keras as frontend). The constructed algorithm is deployed in the BAN-IoT devices using the Micropython and lite version of tensorflow. Table (4) & (5) depicts the hardware deployed for the designing BAN-IoT node and fog gateways.

Table 4 *Hardware Description for experimenting the BAN-IoT Nodes*

Sl.no	BAN-IoT Devices	Specification
1	Embedded Hardware	32-bit(K20)
2	Number of Sensors	5
3	Type of Sensors	Health care
4	IoT transceivers	WIFI
5	WIFI specification	ESP8266
6	Power Supply	3.3V/batter y operated

Table 5: *Hardware Description for experimenting the Fog Gateways*

Sl.no	Fog Devices Used	Specification
1	Embedded Hardware	32-bit (CortexA-53)
2	IoT transceivers	WIFI
3	WIFI specification	ESP8266
4	Power Supply	3.3V/Stand-Alone

5. Results and Discussion:

To assess the unpredictability of the resulting bits, statistical tests from NIST were applied to the recommended encryption method. The outcomes from all tests conformed to NIST criteria and verified its randomness capabilities, providing robust defenses against network attacks. The data in the table indicates that the encrypted bits demonstrate significant randomness, which complicates any attempts by intruders to tamper with medical data during transmission.

5.1 Encryption and Decryption Time Analysis:

In this assessment, the encryption and decryption times for the suggested model are evaluated and contrasted with other existing algorithms. To thoroughly assess the proposed method, diverse data sizes are applied across various sensors, and the duration required for encryption and decryption is computed for both the recommended methodologies and the alternative models listed. Figures 7-8 depicts relative analysis of processing times for various metodlogies relative to varying data sizes. The proposed model is designed and implemented to evaluate the security, integrity, non-tampering, and confidentiality of IoT data communication. This model, which leverages an adaptive chaotic cryptographic technique,

Figure 7. *Encryption Time Analysis*

Figure 8. *Decryption Time Anlaysis*

enhances internet security, as demonstrated in Figures 3-4. Keys generated through this adaptive approach are used as private keys in each smart healthcare IoT device. These private keys are utilized by hospitals and doctors to decrypt the medical data from the sender. However, if encryption is performed too quickly, there is a risk of data being compromised by intruders. To address this, experiments were conducted to gauge the encryption time of the recommended methodology. To validate the efficacy of the proposed model, comparisons were made with existing algorithms such as AES, Modified AES, S-DAC, and Lightweight AES. Figures 3-5 illustrate the performance of various algorithms in generating encrypted data. The experiments revealed that AES took longer to encrypt small-sized data, potentially increasing the risk of data tampering by intruders. In contrast, the proposed algorithm, which employs scroll maps combined with AELM, demonstrated a significant improvement over the existing methods. This shows that integrating chaos with the proposed model enhances encryption performance by adding greater randomness and computational unpredictability. The other models, while effective, consumed more time, making them less suitable for deployment in BAN-IoT nodes. Therefore, the results indicate that the proposed model offers improved randomness and a lightweight profile (by integrating scroll chaotic maps with AELM), making it more suitable for ensuring high security and integrity in smart healthcare IoT systems.

5.2. BAN Logic Analysis:

To verify the protocol, we utilized the Barrows-Abadi-Needham (BAN)-logic approach to evaluate and substantiate the security efficacy of the recommended protocol. BAN-logic provides a framework for specifying and analyzing information exchange protocols. It aids protocol designers in affirming the security of the protocol by assessing the trustworthiness of exchanged information and its protection against potential threats. BAN-logic is a prominent protocol analysis method for confirming the strength and accuracy of an authentication protocol. Additionally, it is a comprehensive validation method for establishing the mutual authentication of a protocol. The analysis in this study employs BAN-logic by defining various objectives (4 goals). We then outline the idealized form of the transmitted messages and the assumptions necessary for BAN-logic proof. Following this, we conduct a step-by-step security proof of the recommended protocol based on BAN-logic principles. The accomplishment of four goals through 8 steps demonstrates that the proposed protocol is secure and performs well. The scheme is robust, efficient, and applicable in BAN-IoT-Fog environments, and is suitable for resource-limited networks. Table 6 presents the different BAN-logic notations used in this study.

Table 6: *BAN-logic notations*

Symbols	Description
$\boldsymbol{p\vert \equiv A}$	**P is convinced that X is true.**
$W \lhd A$	P retrieves a message containing X
$W\vert\sim A$	P previously communicated X
$W \Longrightarrow A$	P oversees X
$\#(A)$	X was not transmitted in previous communications before this round
$W \overset{k}{\leftrightarrow}$ Q	P and Q can utilize shared key K for secure messaging.
$\langle A \rangle_k$	X incorporated with Y

5.2.1 BAN Logic Formulas: the BAN-logic formulas considered pursues:

$$R_1: \frac{W\vert\equiv\#(A)}{W\vert\equiv\#(A,B)} \qquad R_2: \frac{W\vert\equiv\#(A), W\vert\equiv Q\vert\sim A}{W\vert\equiv Q\vert\equiv A}$$

$$R_3: \frac{W\vert\equiv W \overset{k}{\leftrightarrow} Q, W\lhd\langle A\rangle_k}{W\vert\equiv Q\vert\sim A} \qquad R_4: \frac{W\vert\Longrightarrow A, P\vert\equiv Q\vert\equiv X}{W\vert\equiv\#(A,B)}$$

$$R_5: \frac{W\vert\equiv A, W\vert\equiv b}{W\vert\equiv A,B)} \; \frac{W\vert\equiv Q\vert\equiv(A,B)}{W\vert\equiv Q\vert\equiv A}$$

5.2.2 Security Goals:

$E_E = SAELM(B_1, B_2)$

E_E and E_d Arranged beforehand. Thus, we are committed to meeting the following security benchmarks.

$goal_1: S| \equiv S \overset{B_1,B_2}{\leftrightarrow} G$

$goal_2: S| \equiv G \equiv S \overset{B1,B2}{\leftrightarrow} G$

The Refined Version: The refined version of the message exchange is outlined below.

$msg_1: S \leftrightarrow G: (S_{id}, S \overset{B_1}{\leftrightarrow} G)_{S \overset{E_E}{\leftrightarrow} G}$

$msg_2: G \leftrightarrow S: (G_{id}, S \overset{B_1}{\leftrightarrow} G, S \overset{B_2}{\leftrightarrow} G)_{S \overset{E_{E,}}{\leftrightarrow} G}$

The Presumptions: We assume the initialization as follows.

$P_1: S| \equiv \#(B_1)$

$P_2: G| \equiv \#(B2\ )$

$P_3: S| \equiv S \overset{Ee,E_d}{\leftrightarrow} G$

$P_4: G| \equiv S \overset{Ee,E_d}{\leftrightarrow} G$

$P_5: S| \equiv G \Rightarrow S \overset{B1}{\leftrightarrow} G$

$P_6: G| \equiv S \Rightarrow S \overset{B1}{\leftrightarrow} G$

$P_7: S| \equiv S \overset{B_1}{\leftrightarrow} G$

$P_8: G| \equiv S \overset{B_2}{\leftrightarrow} G$

5.2.3 The BANLogic Proving Process:

The BANlogic process is detailed.

Step 1: Originating in P_1 gets $S| \equiv \#(S \overset{B_1}{\leftrightarrow} G, S \overset{B_2}{\leftrightarrow} G, G_{id})$

Step 2: Originating inmsg_2 we get: $S \lhd (S \overset{B1}{\leftrightarrow} G, S \overset{B}{\leftrightarrow} G, G_{id})_{S \overset{E_E,E_d}{\leftrightarrow} G}$

Step 3: Originating in step 2, P_3, R_3 we can get $S| \equiv G \sim (S \overset{B_1}{\leftrightarrow} G, S \overset{B_2}{\leftrightarrow} G, G_{id})$

Step 4: Originating in step 1, step 3, R_2 we can get $S| \equiv G \equiv (S \overset{B1}{\leftrightarrow} G, S \overset{B2}{\leftrightarrow} G, G_{id})$

Step 5: Originating in step 4, R_5 we can get: $S| \equiv G \equiv S \overset{B1\ ,B_2}{\leftrightarrow} G$ (we get $goal_2$)

Step 6: Originating in step 5, R_5 we can get: $S| \equiv G \equiv S \overset{B_2}{\leftrightarrow} G$

Step 7: Originating in step 6, P_5, R_4 we can get: $S| \equiv S \overset{B_2}{\leftrightarrow} G$

Step 8: Originating in step 7, P_1, R_5 we can get: $S| \equiv S \overset{C1\ ,C_2}{\leftrightarrow} G$ (we get$Goal_1$)

6. Conclusion and Suggestions

In this research article, AELM based encryption and decryption were recommended for providing the physiological data security in the Fog-BAN environment. BAN-IoT devices are assembled on the human body and different body parameters are collected. Subsequently, two identical AELM architectures were trained based on the body parameters collected and chaotic scroll maps to get the encrypted data. The AELM is customized in accordance to the BAN-IoT devices that can be used for the encryption whereas the same algorithm is also installed in the Fog devices for decrypting the input signals from the BAN-IoT nodes. The scroll chaotic maps and input data signals are encrypted and decrypted by the proposed adaptive feed forward networks based on the principle of extreme learning machines. The extensive experimentations are carried out to evaluate the recommended algorithm and assesed with various resin ding methodologies. Results demonstrates that the proposed algorithm has shown less computational overhead (40% reduced) and consumes only little time for encryption and decryption process. Moreover, NIST standard test and BAN logic analysis has been conducted in which it is observed that the suggested model depicts more randomness and fulfils the security goals for BAN-IoT networks. In light of future trends, the recommended model should be tested with the greater number of users mounted with BAN-IoT nodes interfaced with multiple sensor that leads for improving the algorithm to with stand the multiple attacks under unique persons. A Hybrid Symmetric Cryptography with Multi-layer Feed Forward Networks model used in literature for different fields [32-39].

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] S. M. R. Islam, D. Kwak, M. D. H. Kabir, M. Hossain, and K.-S. Kwak, (2015). The internet of things for

health care: a comprehensive survey, *IEEE access*, 3;678–708. doi: 10.1109/ACCESS.2015.2437951

[2] A. M. Rahmani et al., (2018). Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach, *Futur. Gener. Comput. Syst.*, 78;641–658, 2018.

[3] S. Tuli, N. Basumatary, and R. Buyya, (2019). Edgelens: Deep learning-based object detection in integrated iot, fog and cloud computing environments," *4th International Conference on Information Systems and Computer Networks (ISCON)*, 2019, pp. 496–502.

[4] S. S. Gill, R. C. Arya, G. S. Wander, and R. Buyya, (2018). Fog-based smart healthcare as a big data and cloud service for heart patients using IoT, *International Conference on Intelligent Data Communication Technologies and Internet of Things*, pp. 1376–1383.

[5] S. He, B. Cheng, H. Wang, Y. Huang, and J. Chen, (2017). Proactive personalized services through fog-cloud computing in largescale IoT-based healthcare application," *China Commun.*, 14(11); 1–16, 2017.

[6] I. Abdullahi, S. Arif, and S. Hassan, (2015) "Ubiquitous shift with information centric network caching using fog computing," *Computational intelligence in information systems, Springer*, pp. 327–335.

[7] M. Satyanarayanan, (2017). The emergence of edge computing," Computer (Long. Beach. Calif)., 50(1); 30–39.

[8] A. Goyal et al., (2019). Seasonal variation in 24 h blood pressure profile in healthy adults-A prospective observational study, *J. Hum. Hypertens.*, 33(8); 626–633 DOI: 10.1038/s41371-019-0173-3

[9] A. A. Omala, A. S. Mbandu, K. D. Mutiria, C. Jin, and F. Li, (2018). Provably secure heterogeneous access control scheme for wireless body area network, *Journal of Medical Systems*, 42(6);108. DOI: 10.1007/s10916-018-0964-z

[10] G. Gao, X. Peng, and L. Jin, (2019). Efficient access control scheme with certificateless signcryption for wireless body area networks, *International Journal of Network Security*, 21;428–437.

[11] I. Ullah, A. Alomari, N. Ul Amin, M. A. Khan, and H. Khattak, (2019). An energy efficient and formally secured certificate-based signcryption for wireless body area networks with the internet of things, *Electronics*, 8(10);1171, 2019.

[12] J. Iqbal, A. I. Umar, N. Amin, and A. Waheed, (2019). Efficient and secure attribute-based heterogeneous online/offline signcryption for body sensor networks based on blockchain, *International Journal of Distributed Sensor Networks*, 15(9).

[13] H. Xiong, Y. Hou, X. Huang, Y. Zhao, and C. -M. Chen, (2021). Heterogeneous signcryption scheme from IBC to PKI with equality test for WBANs," *IEEE Systems Journal*, pp. 1–10.

[14] I. Ullah, N. U. Amin, J. Khan et al., (2019). A novel provable secured signcryption scheme: a hyper-elliptic curve-based approach," *Mathematics*, 7(8); 686.

[15] M. Asghar Khan, I. Ullah, A. Alkhalifah et al., (2021). A provable and privacy-preserving authentication scheme for UAV-enabled intelligent transportation systems, *IEEE Transactions on Industrial Informatics*, p. 1, 2021.

[16] M. Khan, I. Ullah, N. Kumar et al., (2021). An efficient and secure certificate-based access control and key agreement scheme for flying ad-hoc networks, *IEEE Transactions on Vehicular Technology*, 70(5);4839–4851.

[17] M. A. Khan, I. Ullah, S. Nisar et al., (2020). Multiaccess edge computing empowered flying ad hoc networks with secure deployment using identity-based generalized signcryption, *Mobile Information Systems*, 2020;8861947

[18] M. A. Khan, H. Shah, S. U. Rehman et al., (2021). Securing internet of drones with identity-based proxy signcryption, *IEEE Access*, 9;89133–89142.

[19] N. U. Amin, J. Iqbal, and A. R. Abbasi,(2014). Secure key establishment and cluster head selection for body area networks based on signcryption, *Journal of Applied Environmental and Biological Sciences*, 4;210–216

[20] Y. Lu, X. Wang, C. Hu, H. Li, and Y. Huo, (2018). A traceable threshold attribute-based signcryption for mHealthcare social network, *International Journal of Sensor Networks*, 26(1);43–53.

[21] A. Arul Jothi and B. Srinivasan, (2016). Security analysis in body area networks using attribute-based ring signcryption scheme, *Research Journal of Applied Sciences, Engineering and Technology*, 13(1);48–56.

[22] S. Prameela, (2018). Enhanced certificateless security improved anonymous access control with obfuscated quality-aware confidential data discovery and dissemination protocol in WBAN, *International Journal of Pure and Applied Mathematics*, 118;2627–2635.

[23] M. A. Khan, I. Ullah, S. Nisar et al., (2020). Multiaccess edge computing empowered flying ad hoc networks with secure deployment using identity-based generalized signcryption," *Mobile Information Systems*, 2020;8861947.

[24] S. Amudha; M. Murali,(2022). F-CHILS maps - a novel encryption scheme for secured medical data transmission using FoG-ban environment, *International Journal of Ad Hoc and Ubiquitous Computing*, 40(1,2,3);67–79, DOI: 10.1504/IJAHUC.2022.10048192

[25] L. A. Demidova and A. V. Gorchakov, (2020). A study of chaotic maps producing symmetric distributions in the fish school search optimization algorithm with exponential step decay, *Symmetry* 12(5);784

[26] Wang B, Huang S, Qiu J, et al. (2015). Parallel online sequential extreme learning machine based on Map Reduce. *Neurocomputing* 149: 224-32.

[27] https://www.celerium.com/nist-800171

[28] Cryptographic Technology Guideline (Lightweight Cryptography). [Online]. Available: https://www.cryptrec.go.jp/report/cryptrecgl-2003-2016en.pd.

[29] Maheshwari, R.U., Kumarganesh, S., K V M, S. *et al.* (2020). Advanced Plasmonic Resonance-enhanced Biosensor for Comprehensive Real-time

Detection and Analysis of Deepfake Content. *Plasmonics*. https://doi.org/10.1007/s11468-024-02407-0

[30] Maheshwari, R. U., Paulchamy, B., Arun, M., Selvaraj, V., & Saranya, N. N. (2024). Deepfake Detection using Integrate-backward-integrate Logic Optimization Algorithm with CNN. *International Journal of Electrical and Electronics Research*, *12*(2), 696-710. https://doi.org/10.37391/IJEER.120248

[31] Maheshwari, R. U., & Paulchamy, B. (2024). Securing online integrity: a hybrid approach to deepfake detection and removal using Explainable AI and Adversarial Robustness Training. *Automatika*, *65*(4), 1517-1532.

[32]M, P., B, J., B, B., G, S., & S, P. (2024). Energy-efficient and location-aware IoT and WSN-based precision agricultural frameworks. *International Journal of Computational and Experimental Science and Engineering*, 10(4);585-591. https://doi.org/10.22399/ijcesen.480

[33]Guven, M. (2024). A Comprehensive Review of Large Language Models in Cyber Security. *International Journal of Computational and Experimental Science and Engineering*, 10(3);507-516. https://doi.org/10.22399/ijcesen.469

[34]Agnihotri, A., & Kohli, N. (2024). A novel lightweight deep learning model based on SqueezeNet architecture for viral lung disease classification in X-ray and CT images. *International Journal of Computational and Experimental Science and Engineering*, 10(4);592-613. https://doi.org/10.22399/ijcesen.425

[35]ÇOŞGUN, A. (2024). Estimation Of Turkey's Carbon Dioxide Emission with Machine Learning. *International Journal of Computational and Experimental Science and Engineering*, 10(1);95-101. https://doi.org/10.22399/ijcesen.302

[36]Türkmen, G., Sezen, A., & Şengül, G. (2024). Comparative Analysis of Programming Languages Utilized in Artificial Intelligence Applications: Features, Performance, and Suitability. *International Journal of Computational and Experimental Science and Engineering*, 10(3);461-469. https://doi.org/10.22399/ijcesen.342

[37]guven, mesut. (2024). Dynamic Malware Analysis Using a Sandbox Environment, Network Traffic Logs, and Artificial Intelligence. *International Journal of Computational and Experimental Science and Engineering*, 10(3);480-490. https://doi.org/10.22399/ijcesen.460

[38]S, P. S., N. R., W. B., R, R. K., & S, K. (2024). Performance Evaluation of Predicting IoT Malicious Nodes Using Machine Learning Classification Algorithms. *International Journal of Computational and Experimental Science and Engineering*, 10(3);341-349. https://doi.org/10.22399/ijcesen.395

[39]Polatoglu, A. (2024). Observation of the Long-Term Relationship Between Cosmic Rays and Solar Activity Parameters and Analysis of Cosmic Ray Data with Machine Learning. *International Journal of Computational and Experimental Science and Engineering*, 10(2);189-199. https://doi.org/10.22399/ijcesen.324