A Blockchain-Enabled IoT Framework for Secure Attack Detection and Advanced Feature Selection in Smart Healthcare

Ahmed S. Alfakeeh
Department of Information Systems, Faculty of Computing and Information Technology, King Abulaziz University, Jeddah, Saudi Arabia
asalfakeeh@kau.edu.sa (corresponding author)

Received: 13 July 2025 | Revised: 26 July 2025, 18 August 2025, and 25 August 2025 | Accepted: 30 August 2025

 DOI: https://doi.org/10.48084/etasr.13349

ABSTRACT

Industrial healthcare systems aim to provide progressive real-time monitoring of patients and improve medical services through data sharing among intelligent wearable sensors and devices. However, this connectivity carries fundamental vulnerabilities associated with privacy and security because of the requirement of constant communication and monitoring over a public network. However, new technologies, namely Deep Learning (DL) and Blockchain (BC), are promising to overcome these problems and modernize healthcare systems. BC technology is receiving important attention because of its permanent and decentralized nature. Incorporating the immutable and decentralized nature of BC technology with Intrusion Detection Systems (IDS) can provide a stronger and more trustworthy security structure for IoT healthcare systems. This study presents a Secure Internet of Things Framework Using Blockchain and Advanced Feature Selection (SIoTF-BCAFS) model for smart healthcare. The aim is to improve security and reliability in IoT-enabled smart healthcare systems using advanced techniques. Initially, BC-assisted data transmission is employed to ensure secure and transparent communication between devices, especially in IoT. Then, min-max scaling is applied in the data preprocessing step to convert the input data. The ReliefF technique is used to select the best features. Additionally, the SIoTF-BCAFS technique implements an Autoencoder (AE) along with a Temporal Convolutional Network (TCN) model to effectively capture sequential patterns and temporal dependencies. The experimental analysis of the SIoTF-BCAFS technique was performed on the ToN-IoT dataset, demonstrating superior accuracy over existing approaches.

Keywords-Internet of Things (IoT); blockchain; smart healthcare diagnosis; ReliefF; temporal convolutional network; intrusion detection; autoencoder

I. INTRODUCTION

Healthcare can be described as a comprehensive system that comprises dissimilar modules, such as medical centers, health insurance, sensors, warehouses, medications, etc [1]. Modern technologies have greatly influenced healthcare methods, shifting from traditional to advanced approaches, such as tracking healthcare conditions using sensors and wearable devices [2]. This becomes a crucial aspect for many people, particularly those suffering from conditions such as diabetes or irregular blood pressure, who need immediate action and regular observation by professionals to identify possible and timely solutions [3]. The Internet of Things (IoT) links smartphones, tablets, and computer systems, connecting devices such as medical instruments, everyday appliances, and various sensors [4]. The IoT is used across different sectors, contributing to the formation of smart cities and supporting the goal of viewing the world as a single system with self-operating control [5].

There is rapid development in IoT within the healthcare field, as it has increased the adoption of emerging technologies, namely IoT and Blockchain (BC) [6]. The uses of these modern technologies in healthcare include disease detection, digital health record management, remote patient monitoring, and patient surveillance [3]. These methods can support physicians and healthcare professionals in the early identification of multiple diseases, improving accuracy [7]. BC is applied to improve the security of IoT platforms and maintain the privacy of critical data. A key characteristic of BC is decentralization, which implies that the system is operated by several units, rather than a single authority [8]. Medical sensors generate vast amounts of data that are used by Machine Learning (ML) and Deep Learning (DL) algorithms to improve disease prediction and treatment planning. Integrating ML with IoT improves health monitoring, while integrating it with BC ensures secure disease tracking and drug verification. DL also enables personalized care through continuous learning from individual routines [9].

This study presents a Secure Internet of Things Framework Using Blockchain and Advanced Feature Selection (SIoTF-BCAFS) for smart healthcare diagnosis, and analyzes it experimentally using the ToN-IoT dataset. Specifically, the SIoTF-BCAFS model:

- Applies min-max scaling to normalize input data, ensuring uniform feature ranges across all samples. This improves the learning efficiency of subsequent components and stabilizes training. This is a crucial preprocessing step that assists overall model performance.
- Employs ReliefF-based feature selection to detect the most relevant and informative features from the dataset. This improves classification accuracy by mitigating noise and dimensionality. This approach enhances model interpretability and computational efficiency.
- Utilizes an AE for effectual intrusion detection by learning compact and meaningful feature representations. This deep feature learning enables the model to detect anomalies with higher precision, strengthening the intrusion detection process by capturing intrinsic data patterns.
- Implements a TCN for effective classification by capturing long-range temporal dependencies in sequential data. This improves the ability of the technique in recognizing time-based patterns, enhancing classification accuracy.

The novelty of the proposed SIoTF-BCAFS model is in its unified integration of AE and TCN within a dual-domain framework. This incorporation improves task-specific accuracy while promoting model efficiency. The proposed approach presents a novel synergy between DL and temporal modeling across distinct application areas.

II. PRIOR RESEARCH ON SMART HEALTHCARE DIAGNOSIS

In [10], a BC-based secure data-sharing tool was proposed to improve security in IoT applications, developing an effective Proof of Authentication (PoAh) validation module using BC. In [11], a BC-based tailored Federated Learning (FL) model was proposed to secure the Internet of Medical Things (IoMT), integrating edge computing and gateway tools for data collection and preprocessing. In [12], a BC-powered Secure Data Management Framework (BSDMF) was presented. In [13], a novel Golden Jackal Optimizer (GJO)-based DL method with BC was proposed to secure medical data transmission and diagnosis. This method also used homomorphic encryption.

In [14], a dual-step method merged BC with IoMT. The first step used hashing functions and a decentralized interplanetary file system. In the second step, communication costs were improved by communication ranges, power stages, and computation abilities. In [3], an IoMT BC-driven smart healthcare system used encryption alongside an optimum DL method (BSHS-EODL). In addition, image encryption used the Dingo Optimizer Algorithm (DOA). In [15], a BC-enabled IoMT Security System (BC-IoMT-SS) method was proposed. Employing a BC key, the individual's health data can securely produce alerts for authenticated healthcare professionals.

Various existing methods focus on encryption and secure data transmission, but lack real-time threat detection capabilities and adaptive security mechanisms. Some methods emphasize secure storage and access control, but fall short in addressing scalability and interoperability. Techniques comprising encryption optimizers are often limited in scope, with little attention given to their potential in anomaly detection or predictive security modeling. There is a research gap in creating lightweight, intelligent security solutions that offer context-aware protection while ensuring minimal overhead and consistent QoS across heterogeneous IoMT environments.

III. THE PROPOSED METHOD

The purpose of the proposed SIoTF-BCAFS model is to enhance security and reliability in IoT-enabled smart healthcare systems using advanced techniques. It consists of data transfer, min-max scaling, feature selection, and intrusion detection. Figure 1 illustrates the overall workflow of the proposed SIoTF-BCAFS model.

A. BC-Enabled Data Transfer

Initially, BC-assisted data transmission is employed to ensure secure and transparent communication between devices, especially medical IoT devices [16]. Multiple duplicates of data blocks are preserved and created in a distributed way. A key element in this process is solved by the contributor system, as recognition miners initiate agreement on the existing condition of a block. There are various BC model implementations that use Proof of Work (PoW) or Proof of Stake (PoS). Each block takes on a unique code-named hash, which comprises the hashing of the prior block in the chain and is utilized to connect the new block in a particular sequence. Various miners use a set of calculations to determine their integrity as leaders. Usually, a leader is selected from dual models. Hashing is fast and adds minimal overhead, and blocks are linked utilizing hashes. Hashing produces a fixed-length output regardless of input size, ensuring consistent results. In addition, it is a one-way process, making it impossible to reverse-engineer the original input from the output.

B. Feature Rescaling Using the Min-Max Method

The min-max scaling method is used in the data preprocessing phase [17]. This method is chosen for its simplicity, efficiency, and ability to preserve the original distribution of data within a fixed range, usually in [0, 1]. This method retains the associations between values without altering their interpretation and also ensures that no feature dominates others because of its magnitude. It is computationally efficient and appropriate when the input data is bounded. Data is frequently scaled employing methods such as decimal scaling, z-score normalization, and min-max scaling. Method selection frequently depends on the application. The proposed method utilizes the min-max scaling in the data preprocessing phase:

$$Min\text{-}Max\ scaling\ F\text{:}\ Form = \frac{F - F_{\min}}{F_{\max} - F_{\min}} \quad (1)$$

where the specified dataset is an input vector denoted as $(f_1, \ldots, f_n)$, with $1 < n < N$, and N signifies the overall sample counts in space.

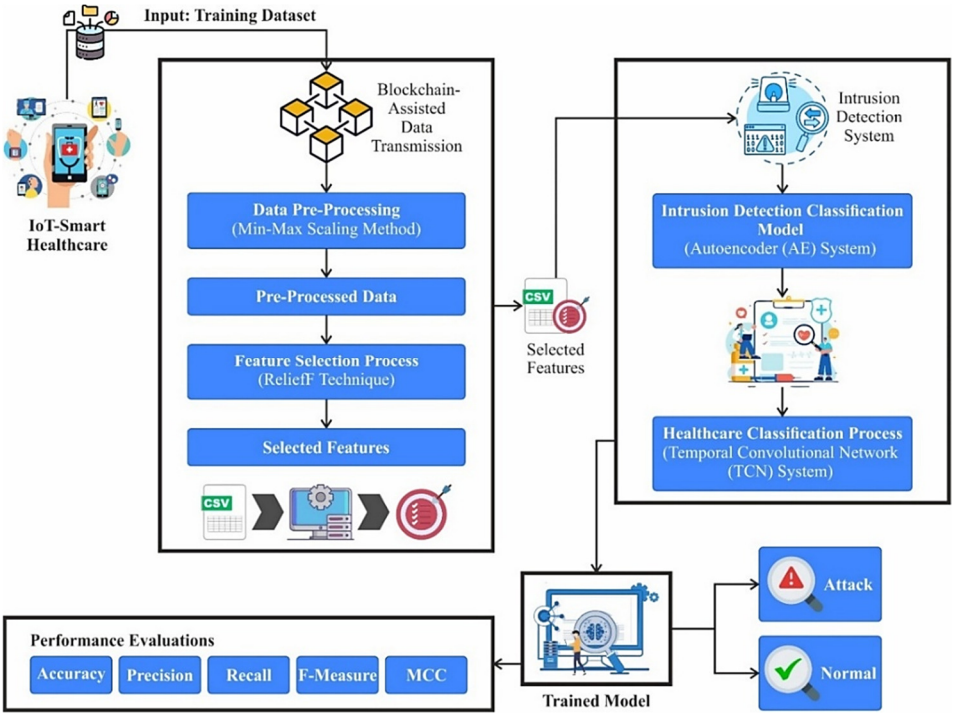

Fig. 1. Workflow of the proposed SIoTF-BCAFS technique.

C. Dimensionality Reduction

The ReliefF technique is used to choose the optimum features [18]. This method was chosen for its ability to detect and retain the most relevant features by computing their significance based on instance-based learning. ReliefF accounts for feature interactions and works well with noisy and multiclass datasets. ReliefF preserves the original feature semantics, making it appropriate and interpretable for classification tasks. The ReliefF feature selection model extends the original Relief method to handle multi-class problems by analyzing how each feature differentiates between sample classes. Within the ReliefF model, recurrent sampling was executed on arbitrarily chosen instances to gather statistical data for each feature.

Assume a training set $D = \{(x_1, y_1), (x_2, y_2), \ldots, (x_m, y_m)\}$, where x_i indicates a feature vector and y_i denotes equivalent classes. For every instance x_i, the aim is to find its out-of-class near neighbor (near misses) $M_j(C)$ and in-class nearest neighbor (near hits) H_j. For every attribute A, a weighted upgrade rule is specified:

$$W(A) = W(A) - \sum_{j=1}^{k} \frac{diff(A,R,H_j)}{mk} + \sum_{c \neq class(R)} \left[\frac{p(C)}{1-p(class(R))} \cdot \sum_{j=1}^{k} \frac{diff\left(A,R,M_j(C)\right)}{mk} \right] \quad (2)$$

where R indicates an arbitrarily chosen instance, $W(A)$ signifies the A feature's weight, $M_j(C)$ denotes the instance in class C specifically nearest to R regarding distance, m signifies the iteration counts, H_j denotes the j^{th} nearest neighbor of R in a similar class, k represents nearest neighbor counts to deliberate from every class, $p(C)$ represents the ratio of instances in category C within the training set, and $diff(A,R,S)$ refers to calculating the alteration between instances R and S in feature A. The computation of change $diff(A,R,S)$ is based on either feature A is discrete or continuous. When feature A is continuous

$$diff(A,R,S) = \frac{R(A)-S(A)}{\max(A)-\min(A)} \quad (3)$$

and when feature A is discrete or $R(A)$ is equivalent to $S(A)$, it is specified in (4) or (5), respectively.

$$diff(A,R,S) = 0 \quad (4)$$

$$diff(A,R,S) = 1 \quad (5)$$

Once every iteration is concluded, the feature weight $W(A)$ is typically standardized to be evaluated. Eventually, the features are chosen depending on their weights.

D. Autoencoder-Driven Threat Identification

The SIoTF-BCAFS technique implements an AE model for intrusion detection [19]. This model is chosen for its ability to effectively learn compact meaningful representations of high-dimensional data in an unsupervised manner. AEs can capture complex non-linear patterns and subtle discrepancies in network traffic, making them highly effective. Their reconstruction-based approach allows them to detect deviations by measuring reconstruction errors. AEs also present greater flexibility and adaptability, enhancing detection accuracy and mitigating false positives. This makes them a robust choice for dynamic and complex security environments.

Considering that the novel time-series data might have higher dimensionality, an AE is applied to produce a latent lower-dimensional model. This not only decreases

computational efficiency but removes unnecessary information and noise. Assume $X = [X_1, X_2, \dots, X_n]$ is the collection of every time series non-linear initial encoding over the linear mapping and non-linear activation functions:

$$H_i = g(WX_i + b_m) \quad (6)$$

whereas $X_i \in X$, W denotes a weighted matrix amongst the input and the encoder layers, b_m refers to the bias of either the encoder layer nodes, and $g(\cdot)$ denotes node activation functions.

Decoding reconstructs the encoded features, obtaining $\hat{X}$. The decoder procedure is equivalent to the encoder method:

$$\hat{X}_i = g(W^T H_i + b_d) \quad (7)$$

where b_d stands for the biased vector of the decoder layer.

The squared error is used as the loss function. Consider the input instance $X = [X_1, X_2, \dots, X_n]$ and the reconstruction $\hat{X} = [\widehat{X_1}, \widehat{X_2}, \dots, \widehat{X_n}]$:

$$\mathcal{L}_R = \frac{1}{2}\sum_{i=1}^{n} \| \hat{X}_i - X_i \|_2^2 \quad (8)$$

The AE is trained to reduce the loss function as:

$$\arg\min_{W,b} \mathcal{L}\,(W, b) \quad (9)$$

The encoder output gained after the last iteration $H = [H_1, H_2, \dots, H_n]$ is a novel time series.

E. Classification Using the TCN Model

The final classification process is performed using a TCN model [20], chosen for its robust pability to model long-range temporal dependencies in sequential data, which are common in medical time series. Unlike conventional recurrent networks, TCNs present parallel processing, stable gradients, and flexible receptive fields, resulting in faster and more reliable training. Their convolutional architecture captures temporal patterns effectively without suffering from vanishing gradient issues, improving prediction accuracy. Compared to other sequence models such as LSTMs, TCNs provide better scalability and robustness, making them suitable for complex healthcare datasets where timely and accurate diagnosis is critical.

TCNs use causal convolutions to maintain temporal order, dilated convolutions to capture long-term dependencies efficiently, and residual connections to enable deeper networks to prevent gradient vanishing and improve convergence speed. TCNs present adaptable receptive fields and excel at handling long sequences, making them suitable for applications such as time series forecasting, natural language processing, audio, and video analysis. A typical residual block in the TCN includes two dilated causal convolutional layers with 64 filters each, followed by batch normalization layers using the Exponential Linear Unit (ELU) activation function. The block also features three max-pooling (2×2×1), a dropout, a 3×3×2 convolutional layer, and a summation operator. The dilation and kernel size parameters are dynamically fine-tuned based on feature map weights. This presents smooth handling of sequence dependencies, easy integration with other CNNs, flexibility as a core module, and simple parameter adjustment. Key merits include causal convolutions that ensure that outputs rely only on past inputs, dilated convolutions that capture long-range dependencies, and parallel processing that accelerates training and inference compared to sequential RNNs.

IV. EXPERIMENTAL ANALYSIS

The SIOTF-BCAFS model was simulated using the ToN-IoT [21, 22] dataset. The model was run on Python 3.6.5 with an i5-8600K CPU, 4GB GPU, 16GB RAM, 250GB SSD, and 1TB HDD, using a 0.01 learning rate, ReLU, 50 epochs, 0.5 dropout, and a batch size of 5. The dataset comprises 119,957 samples with 9 attack types, as shown in Table I. The total features are 63, but only 22 features were selected. The sensor types are ECG sensor (Electrocardiogram), PPG sensor (Photoplethysmography), Blood Pressure sensor, Pulse Oximeter sensor, Accelerometer, Temperature sensor, Bioimpedance sensor, and Heart Sound sensor (Phonocardiogram).

TABLE I. TON-IOT [23] DATASET DETAILS

Attack Type	Cardinality
Normal	78369
MiTM	336
DoS	5440
DDoS	5987
Password	6016
Injection	5867
XSS	5951
Ransomware	5976
Backdoor	6015
Total	**119957**

Table II shows the results of a comparison study of the SIOTF-BCAFS approach with [23]. The results show that the SIoTF-BCAFS approach achieved maximum $accu_y$, $prec_n$, $reca_l$, and $F_{Measure}$ of 99.48%, 92.25%, 87.60%, and 88.70% in intrusion detection, respectively, outperforming the XGBoost+AFSO model in [23].

TABLE II. COMPARATIVE ANALYSIS OF SIOTF-BCAFS

Methods	$Accu_y$	$Prec_n$	$Reca_l$	F_{score}
XGBoost+AFSO [23]	97.43	81.47	85.46	88.33
SIoTF-BCAFS	99.48	92.25	87.60	88.70

V. CONCLUSION

This study presented the SIoTF-BCAFS model to support smart healthcare diagnosis. Initially, BC-assisted data transmission is employed. Then, min-max scaling is applied in the data preprocessing step. The ReliefF technique is used to select features. An AE model is used for intrusion detection, along with a TCN model. The SIoTF-BCAFS technique was evaluated using the ToN-IoT dataset and achieved an accuracy of 99.48%. Although the proposed SIoTF-BCAFS technique confirms secure communication and efficient data processing, it faces difficulty with managing complex data in time-sensitive conditions. However, the feature selection approach may not effectively adapt to shifting data patterns or threats, leaving a research gap in enhancing adaptability, precision, and speed across varying IoT scenarios without increasing computational overhead.

REFERENCES

[1] R. F. Mansour, A. E. Amraoui, I. Nouaouri, V. G. Díaz, D. Gupta, and S. Kumar, "Artificial Intelligence and Internet of Things Enabled Disease Diagnosis Model for Smart Healthcare Systems," *IEEE Access*, vol. 9, pp. 45137–45146, 2021, https://doi.org/10.1109/ACCESS.2021.3066365.

[2] A. Alabdulatif, I. Khalil, and M. S. Rahman, "Security of Blockchain and AI-Empowered Smart Healthcare: Application-Based Analysis," *Applied Sciences*, vol. 12, no. 21, Jan. 2022, Art. no. 11039, https://doi.org/10.3390/app122111039.

[3] A. Albakri and Y. M. Alqahtani, "Internet of Medical Things with a Blockchain-Assisted Smart Healthcare System Using Metaheuristics with a Deep Learning Model," *Applied Sciences*, vol. 13, no. 10, Jan. 2023, Art. no. 6108, https://doi.org/10.3390/app13106108.

[4] A. Samad, "Internet of Things Integrated with Blockchain and Artificial Intelligence in Healthcare System," *Research Journal of Computer Systems and Engineering*, vol. 3, no. 1, pp. 01–06, Oct. 2022, https://doi.org/10.52710/rjcse.34.

[5] K. Aldriwish, "A Deep Learning Approach for Malware and Software Piracy Threat Detection," *Engineering, Technology & Applied Science Research*, vol. 11, no. 6, pp. 7757–7762, Dec. 2021, https://doi.org/10.48084/etasr.4412.

[6] M. A. Rahman, M. S. Hossain, M. S. Islam, N. A. Alrajeh, and G. Muhammad, "Secure and Provenance Enhanced Internet of Health Things Framework: A Blockchain Managed Federated Learning Approach," *IEEE Access*, vol. 8, pp. 205071–205087, 2020, https://doi.org/10.1109/ACCESS.2020.3037474.

[7] R. H. Altaie and H. K. Hoomod, "An Intrusion Detection System using a Hybrid Lightweight Deep Learning Algorithm," *Engineering, Technology & Applied Science Research*, vol. 14, no. 5, pp. 16740–16743, Oct. 2024, https://doi.org/10.48084/etasr.7657.

[8] M. H. Alanazi and B. Soh, "Behavioral Intention to Use IoT Technology in Healthcare Settings," *Engineering, Technology & Applied Science Research*, vol. 9, no. 5, pp. 4769–4774, Oct. 2019, https://doi.org/10.48084/etasr.3063.

[9] B. E. Sabir, M. Youssfi, O. Bouattane, and H. Allali, "Towards a New Model to Secure IoT-based Smart Home Mobile Agents using Blockchain Technology," *Engineering, Technology & Applied Science Research*, vol. 10, no. 2, pp. 5441–5447, Apr. 2020, https://doi.org/10.48084/etasr.3394.

[10] S. Asaithambi, S. Nallusamy, J. Yang, S. Prajapat, G. Kumar, and P. S. Rathore, "A secure and trustworthy blockchain-assisted edge computing architecture for industrial internet of things," *Scientific Reports*, vol. 15, no. 1, May 2025, Art. no. 15410, https://doi.org/10.1038/s41598-025-00337-3.

[11] A. Mazid, S. Kirmani, M. Abid, and V. Pawar, "A secure and efficient framework for internet of medical things through blockchain driven customized federated learning," *Cluster Computing*, vol. 28, no. 4, Feb. 2025, Art. no. 225, https://doi.org/10.1007/s10586-024-04896-4.

[12] A. Abbas, R. Alroobaea, M. Krichen, S. Rubaiee, S. Vimal, and F. M. Almansour, "Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things," *Personal and Ubiquitous Computing*, vol. 28, no. 1, pp. 59–72, Feb. 2024, https://doi.org/10.1007/s00779-021-01583-8.

[13] K. Kulandaivelu, S. Rajappan, and V. Murugasamy, "Blockchain Enabled Secure Medical Data Transmission and Diagnosis Using Golden Jackal Optimization Algorithm with Deep Learning," *Brazilian Archives of Biology and Technology*, vol. 67, 2024, Art. no. e24240214, https://doi.org/10.1590/1678-4324-2024240214.

[14] K. Fiaz *et al.*, "A Two-Phase Blockchain-Enabled Framework for Securing Internet of Medical Things Systems," *Internet of Things*, vol. 28, Dec. 2024, Art. no. 101335, https://doi.org/10.1016/j.iot.2024.101335.

[15] L. Lodha, V. S. Baghela, J. Bhuvana, and R. Bhatt, "A blockchain-based secured system using the Internet of Medical Things (IOMT) network for e-healthcare monitoring," *Measurement: Sensors*, vol. 30, Dec. 2023, Art. no. 100904, https://doi.org/10.1016/j.measen.2023.100904.

[16] H. Alamro *et al.*, "Modeling of Blockchain Assisted Intrusion Detection on IoT Healthcare System Using Ant Lion Optimizer With Hybrid Deep Learning," *IEEE Access*, vol. 11, pp. 82199–82207, 2023, https://doi.org/10.1109/ACCESS.2023.3299589.

[17] S. M. Kasongo and Y. Sun, "Performance Analysis of Intrusion Detection Systems Using a Feature Selection Method on the UNSW-NB15 Dataset," *Journal of Big Data*, vol. 7, no. 1, Nov. 2020, Art. no. 105, https://doi.org/10.1186/s40537-020-00379-6.

[18] Y. W. Song *et al.*, "PF-PSS: a double-layer parallel embedded feature selection method for cancer gene expression data," *Journal of Big Data*, vol. 12, no. 1, May 2025, Art. no. 136, https://doi.org/10.1186/s40537-025-01144-3.

[19] C. Liu, D. Guan, W. Yuan, and Ç. K. Koç, "ITS2Graph: Graph-based generative adversarial learning for imbalanced time series classification," *Neural Networks*, vol. 191, Nov. 2025, Art. no. 107770, https://doi.org/10.1016/j.neunet.2025.107770.

[20] T. Shawly *et al.*, "LHAENA: Lightweight Hybrid Attention Ensemble Network Architecture for Epileptic Seizure Detection," *Journal of Disability Research*, vol. 4, Jul. 2025, Art. no. 20250581, https://doi.org/10.57197/JDR-2025-0581.

[21] "Edge-IIoTset Cyber Security Dataset of IoT & IIoT." Kaggle, [Online]. Available: https://www.kaggle.com/datasets/mohamedamineferrag/edgeiiotset-cyber-security-dataset-of-iot-iiot.

[22] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, "Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications for Centralized and Federated Learning." Jan. 27, 2022, https://doi.org/10.36227/techrxiv.18857336.v1.

[23] W. Song, X. Zhu, S. Ren, W. Tan, and Y. Peng, "A hybrid blockchain and machine learning approach for intrusion detection system in Industrial Internet of Things," *Alexandria Engineering Journal*, vol. 127, pp. 619–627, Aug. 2025, https://doi.org/10.1016/j.aej.2025.05.030.