

Original Research

Received 10 June 2026

Revised 20 July 2026

Accepted 04 August 2026

Natural Resources for Human

Health 2026, Vol. 6 (14s): 982–1002

KEYWORDS:

Medical Authentication, IoT
Healthcare, Hybrid Deep Learning,
Blockchain Security, Anomaly
Detection.

Secure Medical Authentication for IoT-Enabled Healthcare Using Hybrid Deep Learning and Blockchain-Based Audit Logging

¹*D. Soundaravalli, ²G. Bhuvaneswari

¹*Department of Artificial Intelligence and Data Science, Kings Engineering College, Irungattukottai, Chennai Tamilnadu, India-602117.

²Department of Computer Science and Engineering, Saveetha Engineering College, Thandalam, Chennai Tamilnadu, India -602105.

Corresponding Author Email: dsoundaravalli@gmail.com

ABSTRACT: As the number of Internet of Things (IoT) devices being used in healthcare grows, they provide a means for continuous monitoring of physiological measurements and network-level activities, but also introduce the requirement for reliable authentication, anomaly detection, and trustworthy event logging. This research proposes an authentication mechanism for health care systems based on the use of a secure method with Feedforward Neural Network (FNN) and Convolutional Neural Network (CNN) branches, and with an audit logging based on blockchain technology. The FNN branch aims at learning direct relationships between the heterogeneous physiological and network-related features, while the CNN branch is explored for learning on higher-order feature interactions following a structured transformation of the tabular representation. For class imbalance, Synthetic Minority Oversampling Technique (SMOTE) is not only added to the training set, but also to the training set only, thus avoiding information leakage to the validation and test sets. The prediction results are then added to a blockchain layer where the authentication-event metadata are turned into a stream of hash records and reported via smart-contract governed transactions for traceability and tamper evident auditing. The experimental protocol compares the proposed framework with individual FNN, CNN, DNN and LSTM baselines based on accuracy, precision and recall and F1 score, and area under the Receiver Operating Characteristic (ROC) curve. Other evaluations consider the cross-validation variability, confidence intervals, ablation analysis and the other performance measures related to the blockchain. The framework aims to offer a standardized solution for integrating the authentication with verifiable security logging in healthcare settings with IoT devices. The revised experimental design also reveals the restrictions of the small size of datasets, the representation of CNN in tabular form, computational complexity, and the actual deployment of blockchain systems, to serve as a more reproducible ground for the evaluation of the applicability of the proposed approach.

1. INTRODUCTION

The Internet of Things (IoT) devices have brought changes to the field of patient monitoring that can now be carried out in real-time to gather both physiological and network-related information [1]. Connected to the Internet wearable sensors, smart medical devices and equipment, used in hospitals generate masses of data that contain highly sensitive information about heart rate, blood pressure, body temperature, and access data associated with a device [2]. Even though these technologies improve the degree of patient attention and performance efficiency, they pose tremendous security and privacy risks, primarily concerning the process of patient identification and the lack of restraint of unauthorized access to the medical information [3].

Traditional authentication possibilities, such as passwords or IDs, are not necessarily applicable to the IoT-based healthcare environment, being stolen, copied, or even abused [4]. This scenario shows the necessity to introduce strong, automated and smart authentication systems that will positively identify the true users and maintain sensitive medical data [5].

IoT-enabled medical systems have several security issues when it comes to medical data. To begin with, the heterogeneous data sources such as physiological data, device metadata, and network logs provide complexity to identify meaningful patterns to be used in authentication [6]. Second, IoT data are real time, which necessitates quick and precise decisions, and does not allow time- and computer-intensive approaches [7]. Third, conventional security systems can be spoofed with identity, tamper data and unauthorized access, leading to an interference with patient safety and breach of privacy rules [8]. Also, machine learning models can be challenging when there is imbalance between normal and anomalous or suspicious events, i.e. where the normal activity is significantly larger than the rare yet critical anomalies [9]. These difficulties need a complex solution, which includes state-of-the-art pattern recognition, anomaly identification, and secure data storage. The accurate and secure authentication of patients is one of the foundations of modern healthcare [10]. The inability to properly recognize patients or medical staff might lead to medical errors, unauthorized access to data, as well as undermined patient safety. Besides, effective authentication ensures compliance with regulation, including HIPAA or local data protection laws, and builds on trust between patients and providers [11]. Machine learning and deep learning models provide superior opportunities in biometric and behavioral authentication, which can offer unique identification of users according to physiological patterns or patterns of interaction with other people, which are more secure than conventional fixed credentials [12].

Deep learning models and more specifically Feedforward Neural Networks (FNNs), Convolutional Neural Networks (CNNs) and hybrid hybrids are also effective at learning non-linear, complex patterns in vast amounts of data [13]. As a medical authentication, deep learning is able to derive feature, pattern-level representation of heterogeneous IoT data such as physiological signals and network-level activity. They are especially useful in detecting unauthorized access, abnormal behavior or compromised devices in real-time health care settings due to the ability to detect subtle anomalies and correlations that traditional approaches may not detect [14]. Blockchain technology brings about the concept of decentralization, transparency, and tamper-resistance that complements deep learning-based authentication. Blockchain makes all the activities traceable and immutable by storing authentication logs and access records and metadata in an immutable ledger, and no actions can be made retroactively. Smart contracts also act as an enforcement mechanism to access control policies which minimize human error and allow secure dissemination of sensitive medical data to authorized personnel. Such a combination of blockchain and deep learning creates a reliable, auditable, and solid medical authentication system, which would be suitable in the context of contemporary IoT-based healthcare systems [15]. Even with the development of the IoT and machine learning, the current healthcare authentication systems are challenged by restrictions in processing the real-time heterogeneous information, imbalanced distribution of events as well as security threats. Conventional methods of authentication are not flexible and robust and standalone deep learning models might fail to capture all feature level, as well as pattern level dependencies. More so, lack of tamper-proof logging system minimizes accountability and traceability in key healthcare settings. Thus, a hybrid, intelligent, and secure authentication system that incorporates deep learning to detect anomalies and blockchain to keep records that cannot be changed is required.

Authenticating data in the context of Healthcare IoT involves handling data that are diverse, dealing with minority anomalous events, and maintaining the integrity of authentication records. The scale, representation and semantic meaning of physiological measures and network metadata varies and application of a common learning architecture may be limiting. Meanwhile, anomaly-oriented authentication datasets tend to experience the problem of class imbalance in which the number of normal activities is significantly larger than the number of suspicious activities. Another drawback for prediction-only authentication systems is that there is no independently verifiable record of authentication results. Records from a conventional centralized logging can be used for operational logs, but if it is necessary to maintain high level of auditability, then it can be problematic if the record is modified or unaltered by unauthorized users. The present research study hence focuses on an integrated authentication pipeline in which the heterogeneous attributes of IoT in healthcare are preprocessed, divided into training, validation and independent test sets and then models are created. In order to prevent information leakage from the evaluation data, SMOTE is only used for the training partition data. The hybrid FNN-CNN is then compared to see if there is any measurable advantage in adopting a hybrid approach over using either direct feature learning or transformed feature-interaction learning. Once authenticated the selected event metadata is then hashed and logged via a blockchain based logging system with a smart-contract access rules system. The blockchain layer is regarded as a security and audit layer instead of an alternative to encryption or

traditional healthcare systems. The study is then geared towards assessing the ability of the combined architecture to achieve superior authentication of anomalies while retaining traceable and tamper-proof event logs. Special emphasis is placed on the reproducibility, leakage-free evaluation, contribution of each individual component and the cost of integrating blockchain. All of this would differentiate the proposed work from merely presenting each individual deep learning and blockchain techniques as standalone technologies.

1.1 Research Objectives

The study is based on the objectives of:

1. To design an authentication framework that can handle a variety of physiological and IoT network level attributes in order to differentiate normal and abnormal authentication events.
2. To explore if a hybrid FNN-CNN model has complementary feature representations to FNN, CNN, DNN and LSTM models individually.
3. To set up a leakage-free data preparation process where pre-processing parameters are only calculated with the training partition and SMOTE is only applied to the training data.
4. To link the events to the blockchain and implement smart contracts that regulate access for the purposes of creating a traceable and tamper-proof authentication record.
5. To measure the impact of each of the components of the framework using comparative and ablation experiments and analyse the overhead of the integrated architecture from a computational and blockchain perspective.

1.2 Key Contributions

The study is based on the objectives of:

1. To design an authentication framework that can handle a variety of physiological and IoT network level attributes in order to differentiate normal and abnormal authentication events.
2. To explore if a hybrid FNN-CNN model has complementary feature representations to FNN, CNN, DNN and LSTM models individually.
3. To set up a leakage-free data preparation process where pre-processing parameters are only calculated with the training partition and SMOTE is only applied to the training data.
4. To link the events to the blockchain and implement smart contracts that regulate access for the purposes of creating a traceable and tamper-proof authentication record.
5. To measure the impact of each of the components of the framework using comparative and ablation experiments and analyse the overhead of the integrated architecture from a computational and blockchain perspective.

1.3 Research Questions

The study seeks to answer the following key questions:

1. How effectively can a hybrid FNN-CNN model classifies normal and anomalous authentication activities in real-time healthcare IoT data?
2. To what extent does data preprocessing and balancing improve the detection of rare anomalous events?
3. How does blockchain integration enhance security, traceability, and auditability of medical authentication logs?
4. Can the proposed framework outperform traditional or standalone deep learning approaches in terms of accuracy and robustness?

The article is organized in such a way that it offers an in-depth discussion of safe medical authentication in the IoT-based medical systems. Section 2 includes a critical literature review that encompasses the most important topics, such as medical authentication methods, IoT security issues, the use of deep learning, and blockchain implementation. Section 3 presents the dataset, preprocesses, and data balancing procedures that were utilized in this research project, as well as the extensive coverage of the hybrid FNN-CNN model structure, including the fusion and output layers. The mechanism of the blockchain integration to provide the secure logging and access control is also described in this part. Section 4 gives the results and discussion and compares the performance of the proposed framework with other models based on quantitative measures and comparative

analyses. Section 5 is the last part of the study, summarizing the most important findings and indicating the way of future research that should improve medical authentication in IoT based healthcare setting.

2. LITERATURE REVIEW

The recent literature has recognized that blockchain technology and deep learning can be used in the healthcare system and how the two concepts can be integrated to enhance security, scales, and authentication. The other architecture proposed by Ali et al. [16] is a permission blockchain architecture with a hybrid deep learning back-end that exploited the principles of federated learning and homomorphic encryption of the IoT sensor data, which would ensure privacy and good real-time authentication; however, the complexity of computing, scalability, and compatibility with existing systems remain the impediments of this architecture. Similarly, Shafay et al. [17] give a comprehensive taxonomy and comparative overview of blockchain-deep learning architecture, such as federated learning, proof-of-learning consensus and privacy-preserving protocols, although bottlenecks in scalability is a major limitation and lack of real-life validation is a major issue. Haleem et al. [18] were concerned in blockchain networks that exchange patient data and detect anomalies with deep learning, but the problem is that it needs to be connected with numerous health IT systems in large scale and in real time. Shinde et al. [19] had a model to use smart contracts with deep-learning to achieve secure AI-oriented healthcare authentication, but the computational cost of the model is high and there are no standardized protocols that can be used to implement the model on large scale.

Mantey et al. [20] designed a combined blockchain-deep learning platform to achieve a strong level of EHR authentication, but reported the problems of heterogeneous data format, transaction costs, and scalability. Andrew et al. [21] performed a systematic review to examine blockchain-based healthcare authentication methods focusing on smart contracts and federated analysis models, but the throughput limitations, as well as the possible data leakage in models based on federation, need to be explored. According to Kasralikar et al. [22], the decentralized medical model authentication based on blockchain and federated deep learning was reviewed, but the problems with scalability, standardization, and clinical validation remain unsolved. The encrypted medical data storage with a blockchain backbone, proposed by Das et al. (2024), includes an anomaly detector based on deep learning and multifactor biometric authentication, but the transaction latency and the granularity of access control and regulatory compliance are present issues. Mamoshina et al. [23] also proposed blockchain-based AI marketplaces where authenticated medical data and shared models can be obtained through distributed medical data, but the issue of data privacy following transaction and the actual implementation of data rights remains unaddressed. Lastly, Ghadi et al. [24] investigated blockchain authentication with deep learning to validate IoMT devices with distributed networks, with limitation of real-time operation scalability, and cross-platform interoperability and security of resource-constrained sensors. Together, these papers highlight the promise of blockchain-deep learning integration of secure and scalable healthcare systems and highlight the lack of interoperability, real-time performance, regulations, and standardization. Summary of Literature Review is shown in table 1

Table 1: Summary of Literature Review

Reference	Method Brief	Key Limitation
Ali et al. (2023)	Hybrid DL + blockchain for IoT	Scalability, ethics
Shafay et al. (2022)	DL taxonomy on blockchain	Code, scalability
Haleem et al. (2021)	Blockchain for healthcare data	Integration, scale
Shinde et al. (2021)	Smart contracts + DL	Cost, standards
Mantey et al. (2022)	EHR authentication w/ DL+BC	Format, scale
Andrew et al. (2023)	Federated BC, DL frameworks	Throughput, privacy
Kasralikar et al. (2025)	FL and BC, systematic review	Validation, open code
Das et al. (2024)	Biometric BC+DL auth systems	Latency, compliance
Mamoshina et al. (2017, cited 2025)	Distributed DL market/blockchain	Data rights, privacy
Ghadi et al. (2024)	IoMT device BC+DL authentication	Scalability, sensors

2.1 Research Gap

Even though the implementation of IoT devices in healthcare, as well as the application of machine learning to authenticate a patient, gains popularity, there are still a few important gaps. Older authentication methods usually use conventional security (e.g. passwords or biometric verification) and can be easily spoofed, tampered with, or accessed unauthorised, particularly in real-time IoT applications [25]. Although standalone deep learning models (FNN, CNN, DNN or LSTM) have been utilized in both anomaly detection and authentication, they often do not provide both feature-level and complex pattern-level dependencies at the same time, restricting their classification power and recall of minority or anomalous data [26]. Furthermore, the problem of class imbalance is not properly addressed in many studies because it is a frequent problem of healthcare datasets where unusual events are uncommon but vital. Also, the majority of solutions do not provide tamper-proof and secure logging, and it is not easy to provide traceability and accountability to authentication actions. Lastly, the literature on the implementation of deep learning in conjunction with blockchain to deliver stable prediction as well as safe and auditable storage of authentication logs is extremely limited. The gap suggests that to have reliable, accurate, and secure medical authentication in the IoT-enabled healthcare systems, a sophisticated framework that integrates hybrid deep learning models with blockchain based security would be essential.

3. RESEARCH METHODOLOGY

The proposed methodology involves five sequential steps such as data preparation, leakage-controlled model training, hybrid feature learning, authentication prediction and blockchain-based audit logging for secure authentication of healthcare IoT events. The input data set includes physiological data and data from the IoT network of normal and abnormal activities. The data have numerical and categorical attributes, and both have different class frequencies and scales, therefore, the data have to be preprocessed before developing models. The data is first split into the training set, validation set and an independent test set. The parameters needed for the preprocessing are derived from training partition and then used for the validation and test partitions. SMOTE is then only applied to the training partition to boost the minority class without having to train synthetic data on evaluation samples. Oversampling does not affect the validation and test partitions. Figure 1 demonstrates the workflow of proposed Framework.

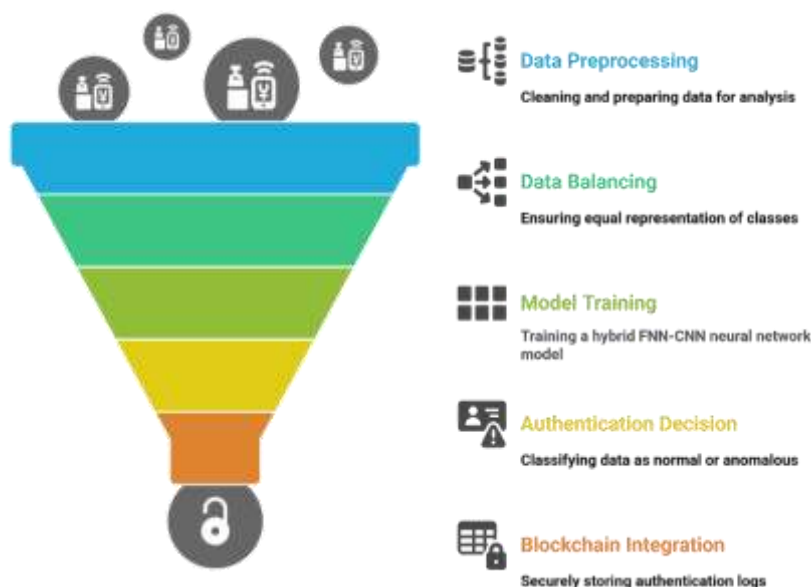


Figure 1: Workflow of the proposed Approach

Since the dataset is imbalanced in the form of class imbalance characteristic to healthcare authentication where the anomalies are minority, the SMOTE (Synthetic Minority Oversampling Technique) is employed to generate synthetic samples of the minority group forming a balanced dataset that can better identify anomalies in the model. It is the hybrid deep learning model which is a blend between Feedforward Neural Network (FNN) and Convolutional Neural Network (CNN). The FNN gets to

learn direct relationship between features at tabular data level and the CNN learns higher level relationships through processing reshapes of feature matrices. A fusion layer is then used to combine these results either through direct concatenation or weighted fusion so as to capitalize on the complementary nature of the two networks. The compounded characteristics are then passed on through an entirely interconnected sequence and an output layer having Sigmoid activation in binary classification or Softmax activation multi-class authentication. The framework has blockchain integration in an attempt to enhance security and traceability. Every authentication procedure is stored in an immutable registry whose logs are hashed down and there is an access control policy implemented by smart contracts to ensure that only sensitive information is accessible to unauthorized staff. This does not only guarantee no tampering; it also provides auditability and transparency of operations in healthcare. Such metrics as accuracy, precision, recall, F1-score, and area under the curve (AUC) are strictly measured as model performance, whereas such visual measures as confusion matrices or class-wise performance charts are. Combined, this type of methodology will ensure a holistic solution that will encompass preprocessing of data, anomaly detection, and stable logging, and can provide a feasible and stable solution to medical authentication in the context of the IoT-based healthcare environments.

3.1 Data Collection

This study utilizes an experimental dataset that includes health-care IoT-related data including attributes at the physiological and network levels [27]. The source for the dataset, access and the associated reference are clearly indicated for traceability and reproducibility. It has 2000 samples and 15 inputs, the output being a target representing normal and anomalous authentication activities. The feature set contains physiological data and network data that accompanies health care IoT events.

The updated data description includes the names of the features, the types of each feature, the distribution of each class, the percent of missing values for each feature, and the size of each partition. The significance of each feature category for the authentication in healthcare IoT is also explained. No claim with regard to the collection of real-time patient data or a specific number of patients is saved unless this information is directly supported by the verified data source.

3.2 Data Pre-processing

The unrefined information derived out of the Secure Healthcare IoT Monitoring System includes real-time physiologic indicators and network metadata. The probability of missing values, categorical variables, and normalization of numerical features necessary before the hybrid deep learning model was trained required the preprocessing of the data. These preprocessing enhances the quality of data, convergence of a model and classification.

3.2.1 Null Value Imputation

The data had missing values, which were filled in with the help of statistical imputation methods to have complete data. The mean or median value was used to impute continuous features like heart rate and body temperature depending on the distribution of the data, and the mode was used to impute categorical features like access type. This plan saved the size of the dataset and controlled information loss so that all the 2000 records of patients could be stored to be analyzed later.

3.2.2 Label Encoding

Label encoding was used to encode categorical variables, such as device ID, gender, and access type into numbers. The process will allocate a unique integer value to each category, which will not require the deep learning model to raise the dimensionality to interpret non-numeric features. An example is where access types such as Read, write and update were represented as 0, 1 and 2 respectively. This move made sure that there is no conflict of models and each category must be unique.

3.3 Normalization

Normalization was also carried out to bring all the features to the same scales to avoid the dominance of an attribute with large numeric range over those with smaller values. The normalization used was Min-Max to bring each feature to the range [0, 1]. As an example, a heart rate of 90bpm with a minimum of 60 and a maximum of 120 was scaled to 0.5. This change has guaranteed equitable contribution of all features in the training process, a higher convergence to gradient descent and a greater model stability was expressed in Eqn. (1):

$$x' = \frac{x - x_{min}}{x_{max} - x_{min}} \quad (1)$$

Preprocessing is essential in improving quality of the healthcare IoT data and guaranteeing the consistent model action. The dataset is not lost with the imputation of missing values using meaningful statistical estimates, resulting in the overall improvement of the model accuracy. Label encoding categorical attributes in numeric format renders the data in line with deep neural networks without losing category distinctiveness. Normalization also guarantees stability during training since the features are brought to an equal scale so that high-range features do not outweigh smaller ones. These preprocessing steps combined with each other do not only improve the robustness of the model but also decrease the computational complexity, which allows learning faster and more efficiently.

3.4 Data Balancing

The full data set is split into three subsets: training, validation and independent testing subset. The entire data set is divided into three subsets: training, validation and independent testing subset. The training subset is used to fit all of the preprocessing transformations and then the same transformations are applied to the validation and testing subsets. Once the data has been partitioned, SMOTE is only used for the training subset in order to balance the representation of the minority class. The validation and testing sets have no new observations and are the same as the original sets. This ensures that synthetic samples generated based on the observed evaluations are not used in training the model, and also offers a stand-alone way to evaluate the generalization performance. SMOTE is a process that is based on the artificial construction of the data points rather than merely repetition of the minorities. For each minority sample x_i , the algorithm selects one of its k nearest neighbors x_{zi} and generates a new synthetic sample by interpolation was expressed in Eqn. (2):

$$x_{new} = x_i + \delta \times (x_{zi} - x_i) \quad (2)$$

This process can be generalized across all features. If the dataset contains F features, then for feature j was expressed in Eqn. (3):

$$x'_j = x_{ij} + \delta \times (x_{zj} - x_{ij}) \quad (3)$$

After applying SMOTE, the number of anomalous records increases until it matches (or nearly matches) the number of normal records. Thus, the balanced dataset satisfies was expressed in Eqn. (4):

$$N_{normal} \approx N_{anomalous} \quad (4)$$

where N represents the number of records in each class. By balancing the data in this way, the hybrid FNN+CNN model receives an equal representation of both classes, improving sensitivity to anomalies while preventing bias toward normal events.

3.5 Hybrid FNN-CNN Model Design

In order to develop a strong authentication system of the healthcare IoT systems, this paper uses a hybrid deep learning model comprising of a Feedforward Neural Network (FNN) and a Convolutional Neural Network (CNN). The feature-learning capability of FNN and the pattern recognition power of CNN is used as a combination to create a more precise and generalized model of differentiating between normal and abnormal activities.

3.5.1 Feedforward Neural Network (FNN)

The first significant element of the hybrid authentication system is the Feedforward Neural Network (FNN) which was aimed at working with the 15 tabular characteristics of the dataset. These characteristics comprise physiological measurements, i.e. heart rate, blood pressure and body temperature, as well as network-level metadata, i.e. device ID, IP address and type of access. Because every feature is relevant in classifying whether an activity is normal or abnormal, it is the role of the FNN to learn direct feature-to-class relationship in an organized manner.

Input Layer

The input layer of the FNN contains 15 neurons, one for each feature. Each input value, denoted as x_i , is normalized during preprocessing to ensure that all features contribute fairly to the learning process, preventing attributes with larger ranges (e.g., encoded IP addresses) from dominating smaller ones (e.g., temperature values).

Hidden Layers

The hidden layers are made up of fully connected (dense) neurons that perform non-linear transformations on the input data. At each neuron, the weighted sum of inputs is calculated as in Eqn. (5):

$$z = \sum_{i=1}^n w_i x_i + b \quad (5)$$

where:

- x_i = input feature
- w_i = weight assigned to the input
- b = bias term

This linear combination is then passed through a non-linear activation function such as the Rectified Linear Unit (ReLU), defined as in Eqn. (6):

$$f(z) = \max(0, z) \quad (6)$$

The use of ReLU ensures that the network can capture complex, non-linear relationships within the dataset, enabling it to distinguish subtle differences between normal and anomalous patterns.

Dropout Regularization

In order to avert overfitting on the model, dropout layers are used in between dense layers. In training, a random fraction of neurons (e.g., 20-50% of them) is dropped, causing the network to learn more generalized and robust feature representations, as well as learn to memorize certain patterns. This renders the FNN more dependable when it comes to unobservable real-time healthcare Internet of Things data. The FNN learns both medical and network-level features by transforming both into multi-layers of dense layers, thereby learning direct feature-level relationships between the inputs and the target labels (normal = 0, anomalous = 1). An example is an abnormally high heart rate and a device access request that is not typical of the usual state of things could be an indicator of an anomalous event. Therefore, the FNN functions as a powerful baseline feature extractor, which offers meaningful features that are subsequently combined with the CNN part to further make holistic decisions.

3.5.2 Convolutional Neural Network (CNN)

The CNN is investigated as an alternative mechanism for feature learning for the tabular representation of health care IoT, instead of as a typical image-processing model. Before starting convolutional processing, the input attributes are converted to a structured feature arrangement. This transformation is designed to investigate if there is more discriminative information in the local combinations that can be extracted from neighboring feature representations besides the direct relationship between them learned by the FNN branch. This does not mean that the original health care records have any physical spatial structure, but rather it is a CNN branch which is regarded as an experimental feature-interaction learner.

The contribution of the CNN branch is assessed with ablation studies as the suitability of using CNN for tabular data cannot be taken for granted. The performance of the FNN-only, CNN-only and FNN-CNN configurations is tested in the same data partition, preprocessing, training conditions and evaluation metric. Thus, the improvements in any architecture that is proposed is backed up by empirical comparison, not by architecture assumptions.

The CNN is based on the convolution operation, in which learnable filters are moved over the input matrix to identify noteworthy patterns. Mathematically, the convolution at position (i, j) can be expressed as in Eqn.(7):

$$h_{i,j} = \sum_{m=1}^M \sum_{n=1}^N w_{m,n} \cdot X_{i+m,j+n} + b \quad (7)$$

Here, X represents the input feature grid, WWW is the kernel of size $M \times N$, b is the bias, and $h_{i,j}$ denotes the convolved feature at location (i, j) . Through this operation, the CNN is able to highlight significant combinations of features, such as the joint presence of abnormal blood pressure with unauthorized access requests.

Pooling layers are added in order to minimize the dimensions whilst maintaining the most significant information. Specifically, max pooling chooses the most optimal value in a small neighborhood, and it is denoted by the following expression as in Eqn.(8):

$$p = \max\{h_1, h_2, \dots, h_k\} \quad (8)$$

where $h_1, h_2, \dots, h_k$ are feature values within the pooling region. This process will make sure that only the strongest patterns are kept and the irrelevant variations or noise are eliminated. Instead, it is also possible to use average pooling so as to maintain smoother feature representations by calculating their mean value. The pooling, therefore, promotes computational efficiency and increases the capacity to generalize due to the absence of overfitting. Once the feature maps have been extracted, they are subjected to the convolution and pooling operations a few times after which the flattening process translates them into a one-dimensional feature vector. This is necessary because it can fill the gap between the hierarchical nature of CNN in feature extraction and the fusion mechanism that follows, in which CNN features are merged with the features learned by the Feedforward Neural Network (FNN). In general, the CNN can play an important role in medical authentication since it is able to represent complex non-linear interactions on features that cannot be reflected in simple models. The CNN uncovers complex dependencies between physiological and network-level features that are not easily captured by the FNN unlike the latter which is efficient in modeling direct feature-to-class relationships and as a result, it can reveal subtle anomalous behavior. This will make CNN a strong element in the hybrid architecture and guarantee more precise and reliable authentication in healthcare IoT systems.

3.5.3 Fusion Layer

The fusion layer is important in integrating the advantages of the Feedforward Neural Network (FNN) and Convolutional Neural Network (CNN) to create a single representation that can be used to perform classification. Once the FNN has consumed the 15 tabular features and trained feature-level dependencies, and the CNN has obtained high-order spatial associations between reshaped feature grids, the output of both is sent through the fusion mechanism. The simplest one is concatenation fusion in which the resulting vectors of both networks are simply concatenated into one, more complex feature representation. This technique maintains all the acquired knowledge, and the classifier will synergistically contemplate abstract feature-based linkages of FNN with intricate pattern-based associations of CNN. Weighted fusion has a more adaptive form in which weighted fusion is used to combine each output vector using learnable weights. Here, the dynamically changing relative weight of both FNN and CNN contribution is used during training based on the branch that gives a higher level of discriminative ability on a particular sample. This flexibility comes in handy especially in non-homogenous healthcare IoT data whereby in certain instances physiological data can prevail and in other instances, network meta data can give more robust evidence about abnormal authentication requests. The fusion layer assures that the hybrid framework combines the two perspectives harmoniously and thus results in stronger and more precise classification results in real-time medical authentication application.

3.5.4 Output Layer

The output layer is the ultimate stage of decision making level of the hybrid FNN-CNN design and here the unified feature manifestations of the fusion layer are allocated to forecasting space. After the fully connected layers, the network sums up the learned features, each with a weight of the learned features and afterward, run through an activation function to generate class probabilities. In the case of binary classification, which is used to distinguish between a normal (0) and anomalous (1) authentication event, the Sigmoid activation function is used. Mathematically this can be formulated as in Eqn. (9).

$$y = \frac{1}{1+e^{-z}} \quad (9)$$

where z is the weighted sum of the inputs to the output neuron. The sigmoid function is useful in reducing the output to a range of probability values, between 0 and 1, and thus would be applicable to binary decision-making in medical authentication applications. A probability with a value nearer to 1 shows an increased tendency of abnormal behavior whereas a value near 0 indicates normal behavior. The Softmax activation function is used in instances in which the framework is expanded to multi-class authentication (such as differentiating between various types of anomalies or access privileges). The Softmax function gives a probability distribution over the possible classes and is given by Eqn. (10):

$$P(y_i) = \frac{e^{z_i}}{\sum_{j=1}^k e^{z_j}} \quad (10)$$

Here, $P(y_i)$ denotes the probability of class i , z_i is the weighted sum for class i , and k represents the total number of classes. The Softmax normalizes the exponentials of the output scores to make sure all probabilities of the classes are summed up to 1 so that the model can be certain about the likelihood of the input belonging to the most probable class.

The output layer, therefore, converts the rich representations taught through the hybrid model to explicit and understandable predictions, which allow safe and trustworthy classification of the medical authentication tasks in the IoT-based healthcare systems.

3.6 Blockchain Integration

The blockchain is used merely as an audit and integrity layer, placed after the authentication decision, not as a way of conducting the deep learning computation. The predictive module will classify incoming events from the healthcare IoT system as normal or anomalous and the blockchain layer will store an authenticated representation of the resulting events. These metadata, which include a subset of the device identifier, the time of the event, whether or not they were authenticated and a user identifier, are mapped to a cryptographic hash prior to sending them to the blockchain network.

Smart contracts are used to program the access-control rules for retrieval of authentication logs. The architecture thus enables two functions to be separated: deep learning for data-driven authentication; and blockchain for a tamper evident log, traceability and access to audit control. The design isn't an alternative to existing encryption, or secure communications or hospital data-management systems. That is not the case with blockchain, though, as it's seen as an extra layer of integrity and accountability.

The following properties of the blockchain are used to assess the usefulness of this layer: transaction latency, throughput, storage requirements, computational requirements and scalability. These measures should be taken to check the increase in the infrastructure cost against the security and auditability gains in the healthcare IoT environments. Figure 2 illustrates the blockchain working process.

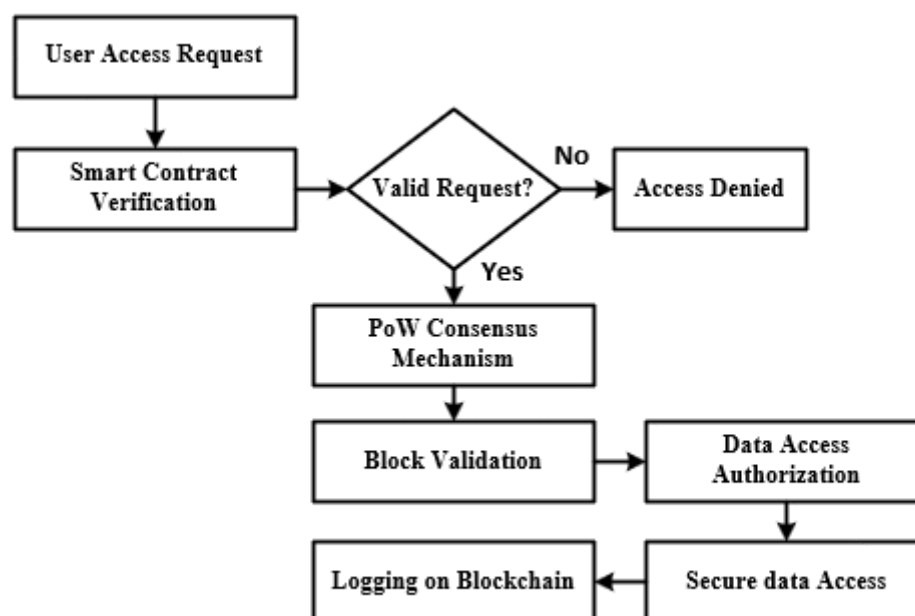


Figure 2: Blockchain Process

The integration of blockchain also offers some important advantages to the authentication system. First, it provides tamper-proof storage since every block within the chain is cryptographically bound to the last block, and it is not computationally feasible to make changes retroactively. Second, it allows traceability, which means that the administrators can trace the history of all authentication events in real-time. Third, it improves auditability which offers a verifiable record of all activities to comply with the healthcare regulations and healthcare security standards. With authentication through deep learning and the immutable

ledger by blockchain, The framework provides a powerful, safe, and open system. This hybrid solution does not only make medical authentication decisions more reliable but also improves general data management and trust in the IoT-based healthcare settings.

3.7 Integration of Proposed FNN+CNN with Blockchain

The model suggested incorporates a hybrid FNN+CNN model in combination with blockchain to deliver safe, resistant to tampering, and auditable medical authentication. IoT devices initially provide real-time physiological data (heart rate, blood pressure, and body temperature), metadata related to the network (ID of the device, IP address, and access type). The data are preprocessed, with the null values being imputed, the labels being transformed into codified values, and then normalized, and finally, by the means of balancing with SMOTE that anomalous events are represented fairly. This preprocessed data is then made to go through the hybrid model where it is classified as either normal (authenticated) or anomalous (unauthenticated). After a prediction has been produced, a hash of the record, and other pertinent metadata (including device ID, timestamp, predicted class, and user ID) is uploaded into the blockchain ledger as a transaction. Smart contracts secure access, which means that the logs can only be queried or accessed by the authorized personnel in the healthcare. Figure 3 demonstrates the Proposed Secure Health Care IoT Authentication Framework.

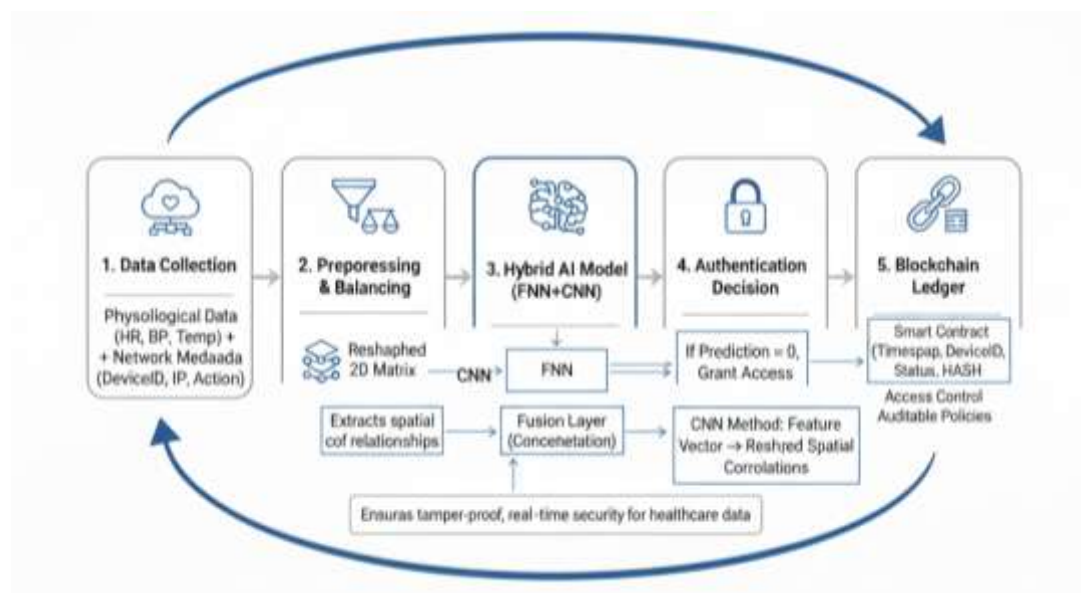


Figure 3: Proposed Secure Health Care IoT Authentication Framework

The system offers complete traceability and accountability as every transaction can be verified as being immutable and time-stamped, with blockchain technology essentially being the predictive power of deep learning with the security and disclosure of blockchain technology.

Algorithm 1: Leakage-Controlled FNN-CNN Authentication with Blockchain Logging

Input: Physiological measurements and IoT network metadata
Output: Authentication prediction and hashed blockchain audit record

Step 1: Data Acquisition and Preprocessing
Collect the healthcare IoT authentication dataset.
Identify numerical, categorical, and target attributes.
Divide the complete dataset into training, validation, and independent test sets.
Fit preprocessing transformations using the training set.
Apply the learned transformations to the training, validation, and test sets.

Step 2: Training Data Balancing
Apply SMOTE only to the training partition.
Keep validation and test partitions unchanged.

Step 3: Hybrid Model Training

Provide the processed training data to the FNN branch.

Transform the feature representation for the CNN branch.

Extract FNN and CNN representations.

Fuse the learned representations.

Generate the binary authentication prediction.

Step 4: Model Evaluation

Evaluate the trained model using the untouched validation and test sets.

Calculate accuracy, precision, recall, F1-score, and AUC.

Repeat the training procedure according to the defined cross-validation protocol.

Step 5: Blockchain Logging

Construct an authentication-event record containing selected metadata.

Generate a cryptographic hash of the record.

Submit the hash and permitted metadata through the blockchain transaction.

Apply smart-contract access rules to authentication-log queries.

Step 6: Audit

Maintain the blockchain transaction as a time-stamped, tamper-evident audit record.

4. RESULTS AND DISCUSSION

In this section, the analysis of the performance of the proposed hybrid FNN-CNN model with the integration of blockchain-based medical authentication is provided on a large scale. The analyzed results are discussed through a complex measurement of such measures as accuracy, precision, recall, F1-score, and area under the curve (AUC), which help to gain a comprehensive insight into the effectiveness of the model to distinguish between normal and anomalous activities. Quantitative and qualitative analyses are conducted in order to evaluate the effectiveness of the model in dealing with real-time healthcare IoT data, both with and without preprocessing, data balancing, and feature extraction. Moreover, the paper examines the comparative advantages of hybrid model to standalone models with reference to the fusion of FNN and CNN outputs to improve the classification performance. It also explores the role of blockchain integration in the delivery of secure, tamper-proof, and auditable authentication logs which show that the framework can be realistically applied in healthcare settings. Taken altogether, this discussion is supposed to offer an integrated understanding of the experimental results, connecting the model performance to the suggested methodology and elucidating the information on the future enhancements.

All experiments are repeated with the new leakage-controlled data preparation procedure. The data set is split into training and test set prior to SMOTE. Before SMOTE, the data set is divided into training set and test set, and only synthetic minority set is generated from the training set. The validation and test sets are not over-sampled. All the same partitioning strategy, preprocessing procedure, model architecture, training configuration and evaluation criteria are applied to the proposed framework and baseline models. Random initialisation and experimental parameters are reported to ensure reproducibility. The final performance values given in the manuscript are only from the revised experimental protocol.

Experimental Outcome

Figure 4 demonstrates a web-based interface that is used to predict patient health incidents and, safely and securely, record the findings with the help of blockchain technology. The system also connects with Ganache which is a personal blockchain of Ethereum to maintain tamper-proof records. Patient-specific information (ID, IV insert rate, temperature, blood pressure, device ID, IP address, and access type) are entered by the user into the structured fields. When one clicks on the Predict button, the system takes the data through a processing system and goes ahead to give the Authenticated status, which indicates that the prediction has been verified. The result will then be recorded on the blockchain and a noticeable transaction hash will mark the recording of the result. A connection confirmation to Ganache and a balance of 100 ETH are also indicated on the interface and develops confidence in the system as being ready to conduct secure transactions. It is a good example of how blockchain can be utilized in healthcare to make data integrity, traceability, and trust in predictive analytics more productive.



Figure 4: Snippet of Event Prediction

The histogram of a binary target variable in a data set is presented graphically in Figure 5(a), and it reveals that there is a large imbalance between classes. The target values are put in categories 0 and 1 in the x-axis and their corresponding counts in the y-axis. The chart shows that the majority class (target = 0) represents the most frequent in the dataset having about 1350 cases, and the minority class (target = 1) has only about 200 cases. This is a typical problem in machine learning because when a model is trained on biased data, the model will be biased towards the majority class, and therefore not predict well on the minority class. This illustration explains why data balancing methods, e.g., resampling, or synthetic data generation, are required to enable models to be trained fairly and effectively.

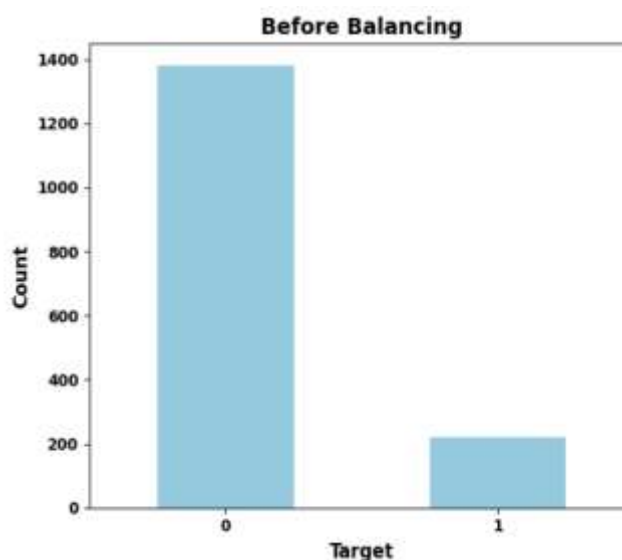


Figure 5(a): Distribution of Target Classes Before Balancing

Figure 5(b) shows how the binary target variable is distributed after preprocessing to deal with the imbalance between classes. Both of the classes, 0 (normal) and 1 (anomalous) appear in the x-axis, and the y-axis indicates the number of instances under each of the classes. As compared to the Before Balancing chart where, in contrast to the previous chart, one of the classes prevailed, the current chart indicates that the two classes are almost equal in terms of their representation in the dataset with each bar having approximately 1,400 instances. This means that methods like SMOTE (Synthetic Minority Oversampling Technique) ran successfully to create more samples in the minority group to obtain a balanced dataset. The model can be trained in a more equitable manner and does not achieve bias towards the majority class but can better predict both normal and

anomalous events. In general, this figure is clear evidence of the balancing process effectiveness and the significance of the balancing process to the reliable model performance.

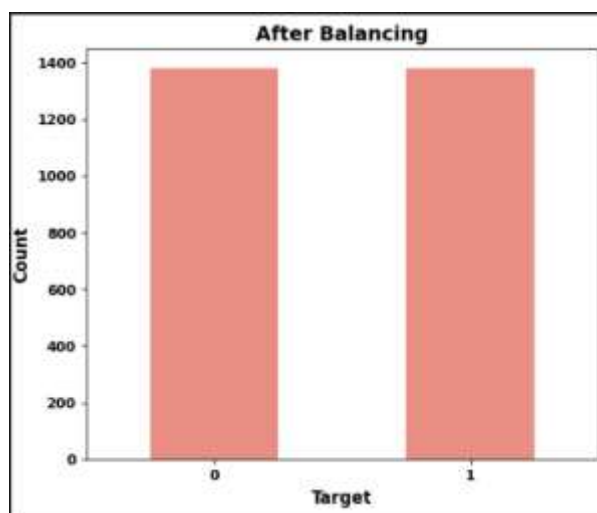


Figure 5(b): Distribution of Target Classes After Balancing

This two-panel figure 6 shows the training performance of the machine learning model with eight epochs, on which it reduces its errors and increases its performance. The training, validation and testing results are computed from the same experiment of building the final model. The validation set is only used for model selection and monitoring while training, while the independent test set is only used for model performance evaluation. During the model optimization, neither any test observations nor any synthetic samples based on test observations are used. This means that the training curves, validation curves, confusion matrix, ROC curve and reported performance metrics are related to the same experimental set-up controlled by leakage.

The entire dataset is divided into training, validation and testing sets prior to developing the model. The training subset is used for parameter optimization and it is the only subset that is applied with SMOTE. The validation subset is kept in its original class distribution and used to monitor the performance of the model and to choose the final configuration of the model. The independent test subset is not used in the training of the model, hyperparameter selection, the estimation of the preprocessing parameters, or in the SMOTE generation. Final performance metrics are computed once training and model selection is done.

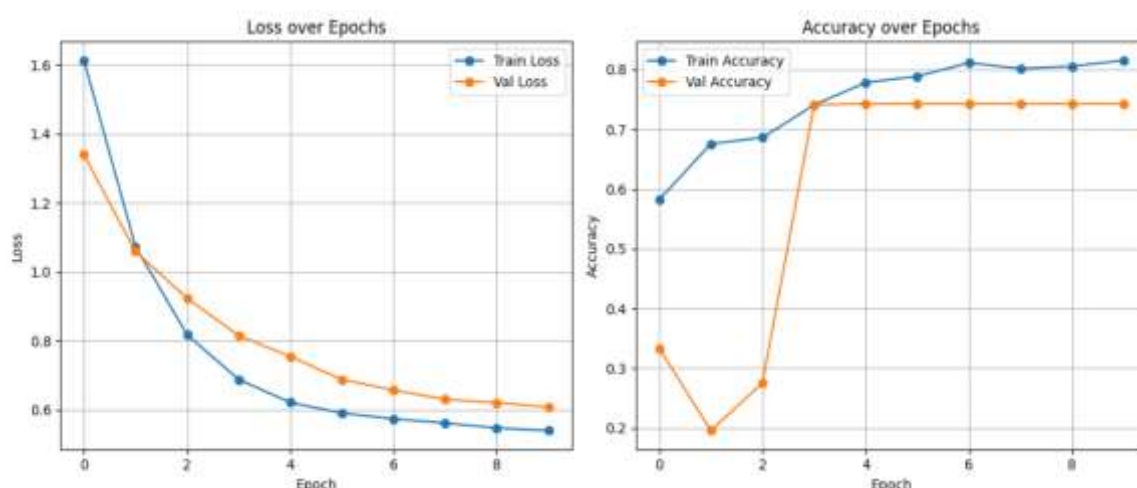


Figure 6: Training Loss and Accuracy Across Epochs

This confusion matrix is used to see the overall performance of the binary classification model using the comparisons between the predicted and the actual labels. In the form of a 2x2 grid, it depicts 345 true negatives (correctly identified class 0), 48 true positives (correctly identified class 1), 7 false negatives (actual class 1 misclassified as 0) and 0 false positives (no instances of 0

misclassified as 1). The lack of false positives implies that the model is highly accurate in predicting anomalous events (class 1) whereas the small number of false negatives implies that there is a small difference between recall or sensitivity. High overall accuracy and reliability is evidenced by the high intensity of the diagonal dominance such that most of the counts appear in the true prediction axis. The distribution is emphasized by color shading where darker color is used to show more counts and thus make it easier to evaluate the performance visually. This is an important diagnostic device that can not only tell about the accuracy but also the trade-off between the precision and recall that is especially important in sensitive tasks like healthcare where misclassifications may be devastating. Figure 7 illustrated the Confusion matrix.

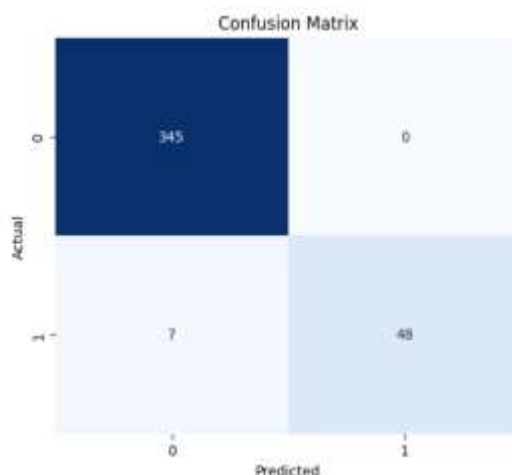


Figure 7: Confusion Matrix

Figure 8 shows a breakdown of the performance of the model with respect to four major evaluation metrics, such as accuracy, precision, recall, and F1-score represented in terms of class. In Class 0, the model performs very well, with the accuracy and precision of 0.98, and recall and F1- score of 0.99. This shows that the model is able to identify and correctly to a great extent classify instances of Class 0 with minimal error. In Class 1, model accuracy (0.98) and precision (0.99) are also high indicating its low false positive. Nonetheless, Class 1 drops to 0.87, which implies the fact that certain real cases of this class are overlooked. As a result, the F1-score that balances precision and recall is a little bit less at 0.93. The chart demonstrates the strengths of the model in terms of the overall accuracy and precision as well as shows one of the possible areas of improvement in terms of sensitivity to the minor class. These insights can be vital in improving the performance of the models, especially when the model is used in critical scenarios whereby a proper identification of the minority group is of great value.

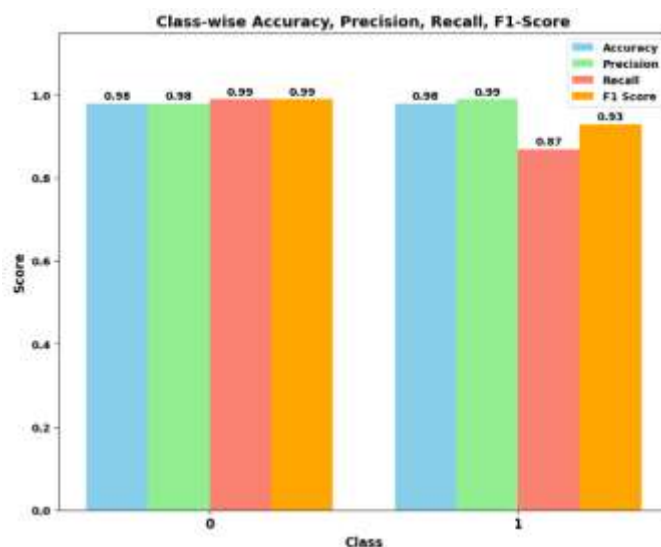


Figure 8: Class-wise Accuracy, Precision, Recall, and F1-Score

Figure 9 illustrates the Comparison of Precision Across Models, provides a clear and powerful visualization of the various machine learning architectures in terms of precision, which is defined as the ratio of true positive predictions to the total positive predictions. There are five models to be compared in the chart, namely FNN, CNN, DNN, LSTM and a hybrid Proposed model that integrates FNN with CNN. Surprisingly, the four models, FNN, CNN, DNN, and the Proposed FNN+CNN, have a precision score of 0.99, which means that these models have a high probability of positive predictions and a low number of false positives. Contrastingly, the LSTM model achieves considerably lower accuracy rating at a mere 0.22 indicating that it is not very effective in detecting positive cases and can also generate a large false alarm. This difference provides evidence of the high performance and reliability of the other models, especially the hybrid approach, and points out at the restrictions of LSTM in this particular situation. This kind of comparative analysis is necessary to pick the most appropriate model architecture, particularly in the field of application where precision counts, e.g. in medical diagnostics or fraud detection.

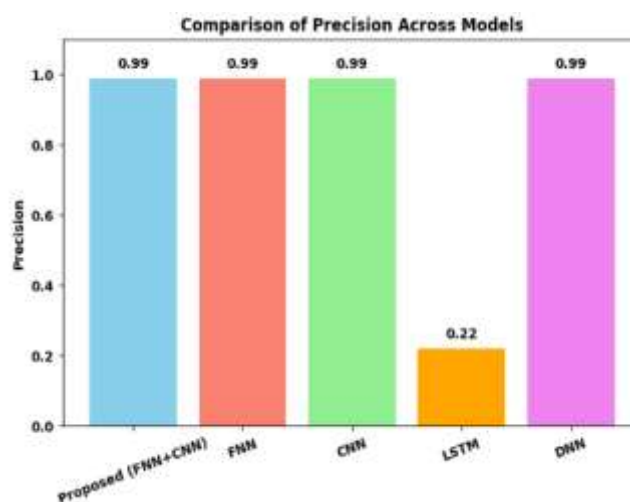


Figure 9: Comparison of Precision Across Models

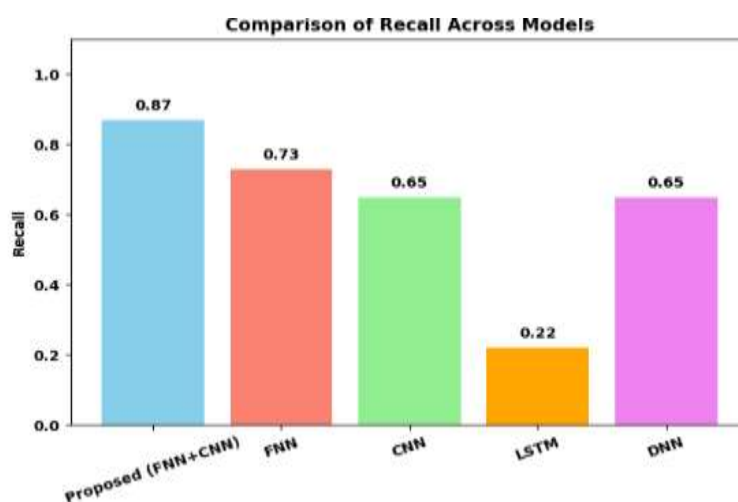


Figure 10: Comparison of Recall Across Models

Figure 10 shows a comparative analysis of five machine learning architectures in terms of their recall scores, which is one of the important measures that determine how a model can correctly identify all the relevant positive examples. The high performance and sensitivity is evidenced by the high recall of the proposed hybrid model with a high recall of 0.87 when compared to the other models, a combination of FNN and CNN. The standalone FNN and CNN models, in their turn, record moderate recall scores of 0.73 and 0.65, respectively. The DNN model recalls a 0.65, and the LSTM model has a much lower recall of 0.22 which means that it is not able to identify much of the existing positive cases. The chart displays different colored-coded bars, which clearly indicate differences between the models and one can easily view the strengths and weaknesses of the

models, as compared to the others. In general, this visualization highlights how the hybrid proposed model is better at recall performance, which is especially important in the context of medical diagnosis or detection of anomalies, when false negativity can be severely detrimental. The analysis gives great ground to choosing the hybrid architecture in case of high sensitivity.

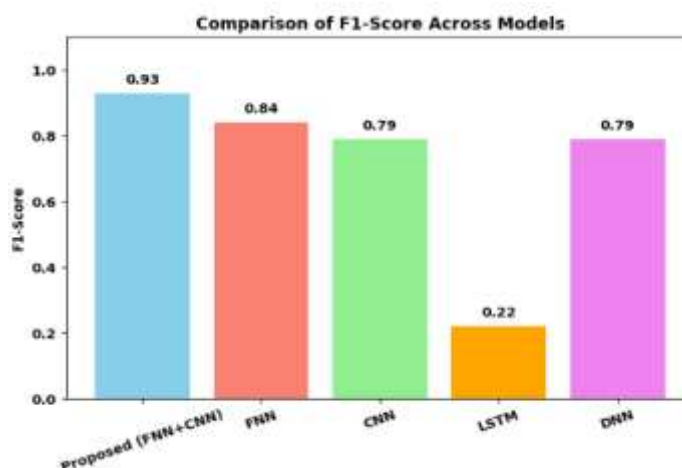


Figure 11: Comparison of F1-Score Across Models

Figure 11 is a comparative analysis of 5 machine learning architectures through their F1-scores which is a metric that balances precision and recall to identify the overall classification performance. In situations where both false positives and false negatives are of great importance, the F1-score is especially significant, e.g., in medical diagnosis, fraud detection, or anomaly detection. The F1-score of the proposed hybrid model (FNN + CNN) reaches the highest value of 0.93, which confirms that this model has high precision and can be used to recognize positive cases with good recall and reduce cases of misclassification. Comparatively, the FNN model achieves a score of 0.84, which is good but with a minor difference in overall balance between precision and recall. Both CNN and DNN models perform with F1-scores of 0.79, demonstrating moderate performance which is probably because the two models appear to be trade-offs between precision and recall. LSTM model performs dismally with the F1-score of 0.22 showing that it has much to be desired when it comes to capturing the right set of patterns in this dataset-possibly due to its inability to capture the temporal dependency of tabular and network level healthcare data. It is apparent in this visualization that the proposed hybrid model performs well and it is necessary to select an architecture that suits the property of the dataset and the intended classification task. The focus on F1-score allows the chart to present a balanced view on the reliability of the model and offer more than just the raw accuracy and informs the model choice in practice.

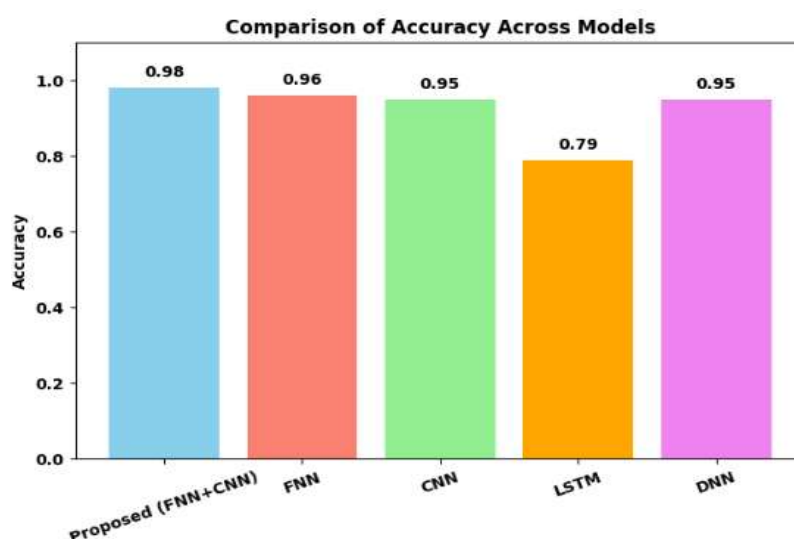


Figure 12: Comparison of Accuracy Across Models

A comparative evaluation of five machine learning architecture in terms of the overall accuracy, the proportion of the correctly classified instances of all predictions is presented in Figure 12. The best accuracy of 0.98 of the suggested hybrid models (FNN + CNN) also reflects an almost flawless classification accuracy and demonstrates the ability to combine the spatial and abstract representation of features of the dataset. The FNN model is the second with an accuracy of 0.96 and the CNN and DNN models 0.95 which is high but slightly lower. On the other hand, the LSTM model exhibits much less accuracy at 0.79 and that represents the potential limitations of handling the structure and arrangement of data. The chart has color-coded bars that enable one to know the performance difference visually and make it comprehensible. Such visualization will be of great use when it comes to selecting a model and ultimately it is the hybrid model proposed that will be more reliable in giving the best possible predictions at all times. Durable performance is important in high-stakes tasks, such as healthcare diagnostics, anomaly detection, or compliance monitoring, where mistakes can be severe.

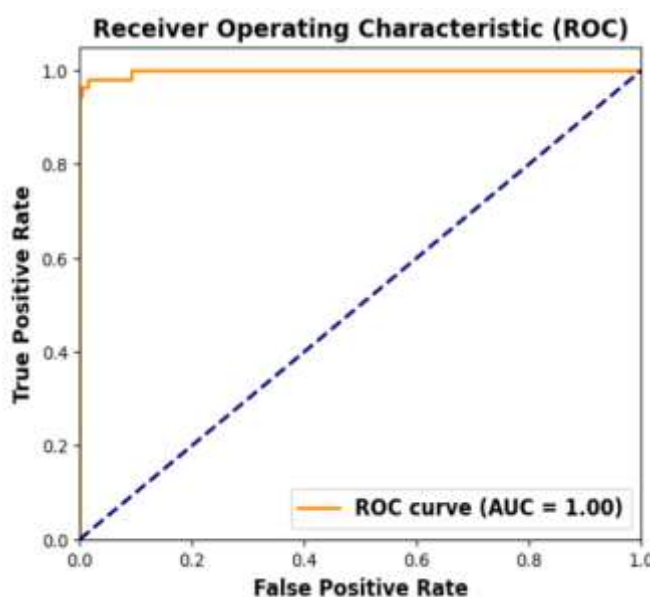


Figure 13: ROC Curve

Figure 13 graph which entails a potent visual overview of how a classification model differentiates two classes. The curve is used to plot TPR (sensitivity) versus FPR at different threshold levels. The orange ROC curve in this graph is very close to the upper-left corner, which means that it has almost perfect classification performance. The blue line is a diagonal dashed line that is used to define a random classifier and use it as a standard of comparison. The Area Under the Curve (AUC) of the model is 0.9980 which is very high and it indicates that the model is capable of nearly perfectly separating positive and negative cases. The score of this type indicates the excellent discriminative power i.e. the model is very effective in distinguishing the actual positives and reducing the false positives. This has been found to be highly beneficial in high performance applications such as medical diagnostics or fraud detection where classification accuracy is vital.

DISCUSSION

The objective of the experimental analysis is to find out if the integrated FNN-CNN architecture offers any measurable benefits when it comes to authentication in the context of IoT devices in healthcare and to gain an understanding of how the blockchain-based event logging can be practically applied in this context. It is possible to interpret model performance by means of the overall accuracy as well as the precision, recall, F1 score, AUC, class-wise behavior, and variability of repeated evaluation procedures. This is done with emphasis on recall for anomalous events as missed anomalous authentication attempts could pose a more serious security threat than the ability to classify majority class events. The hybrid architecture is presented as a hybrid of two different representation strategies. The FNN branch directly processes the tabular features and learns the non-linear feature-to-output relationship while the CNN branch explores interactions with the transformed feature representation. But if there are only two branches, then it's not necessarily a good sign that both are there. Thus, the ablation analysis of FNN-only, CNN-only and FNN-CNN needs to be performed to find out whether the joint representation consistently improves

performance. Such impact of SMOTE should be similarly assessed by comparing the models trained with and without training-set oversampling in the same experimental conditions. The reported predictive performance should also be interpreted in the context of the size of the data set and distribution of the classes. The number of records available in the dataset is about 2,000, which does not allow the results to be widely generalized to more demanding and broader healthcare settings with respect to predictive performance. Therefore, a one-time train-test should not be viewed as evidence of generalization. The results from cross-validation, repeated runs, standard deviation, confidence intervals, and statistical comparisons give greater confidence in the consistency of the differences between models, compared to one data partition or some random model initialization. This CNN representation adds on another calculation to a typical tabular FNN. Thus, depending on the degree of usefulness of the additional architectural complexity, it is useful to see if measurable predictive improvement can offset it. The model parameters, training time, inference time, and computational requirements (if available) should be reported in the proposed evaluation. These are especially significant when the IoT edge devices or gateway systems are constrained in resources or have limited resources, such as in healthcare IoT environments. The blockchain layer serves a different purpose as compared to the deep learning part. However, blockchain's utility cannot be shown by predictive performance as it does not directly increase the accuracy of the classifier. It should rather be evaluated on its contribution in terms of integrity, traceability, access control, and operational aspects such as transaction latency, throughput, storage overhead, computational overhead and cost of transaction. These measurements will give an idea of the cost benefit and help you to know if blockchain integration is feasible as the number of authentication events goes up.

The main differences with the traditional centralized logging also lie in how the audit records are dealt with. It is possible to efficiently store authentication events in a centralized server and it can be used alongside encrypted communication channels. The blockchain layer offers yet another persistence of tamper-evident transactions and an access control mechanism that can be programmed. The proposed architecture should not be understood as an attempt to replace the existing security infrastructure in the hospital or end-to-end encryption. Instead, the blockchain part augments current protection measures, enhancing the auditability and maintenance of the integrity of data records. When comparing with baseline models, it is necessary to use a consistent preprocessing, the same data partitions, same training conditions and a set of models that are correctly designed. Especially a poor baseline like LSTM should not be interpreted as a weakness in the model without considering the representation of the available data and the architecture and training process of the model. If the data structure allows it, there may be some other contemporary sequence or attention-based models to consider as well. Several limitations remain. Generalisability is limited by the size and source of the dataset and data includes only a range of devices and network conditions, and specific combinations of patient populations and healthcare institutions. The CNN transformed tabular representation needs to be further tested on independent datasets. The current set of data does not establish adversarial robustness, distribution shifts, real world data theft scenarios, or large-scale deployment. Such constraints must be addressed via external validation, controlled security experiments, increased data sets and deployment-based evaluation. From a general perspective, the main interest of the framework is the assessment of the complementary characteristic of predictive authentication and of trustworthy audit logging.

5. CONCLUSION AND FUTURE WORK

In this study, an integrated framework for healthcare IoT authentication is proposed, which integrates the hybrid FNN-CNN learning with the blockchain-based audit logging concept. The framework was created to handle heterogeneous physiological attributes or network-level characteristics, to generate decisions for authentication using a training-set-only SMOTE, and finally to ensure tamper-evident record keeping due to blockchain transactions being hashed and access control being governed by smart contracts. The new methodology better distinguishes between the nature of training and evaluation data, thus preventing data leakage and ensuring a more accurate evaluation of model generalization. The impact of the hybrid architecture is assessed by comparing it with individual learning models and by performing component-wise ablation and not by solely attributing the performance gains to the combination of multiple established architectures. Likewise, blockchain integration is considered an audit and integrity mechanism that needs to be evaluated by security and operational aspects, not by prediction. While the available data offers a valuable set of experiments to explore the proposed pipeline, the relatively small data volume limits the ability of generalizing this approach to larger and more diverse healthcare settings. The latter is also a tabular representation that has been transformed by the CNN, and therefore needs to be further validated since the original attributes lack inherent image-like spatial structure. There are also other restrictions such as large-scale blockchain evaluation, computational profiling, comprehensive adversarial-security testing, and the necessity of independent datasets. Future studies may involve testing the

framework with various external datasets from other healthcare environments, as well as testing the framework with distribution shifts and realistic unauthorized-access scenarios. In an IoT device with limited resources, lightweight architectures can be considered; where enough sequential or contextual information is available, attention based or transformer-based models can be explored. Besides, further work should be dedicated to measuring the latency, throughput, storage needs, transaction cost and scalability of blockchain with escalating authentication tasks. Federated learning is an approach that could be explored to minimize the exposure to sensitive healthcare information from a centralized source. These extensions can help establish greater confidence in the security and reliability of AI-powered authentication in healthcare, as well as scalability and real-world deployment compatibility. These extensions can offer better insights into the assurance, scalability, and feasibility of secure AI-powered healthcare authentication.

DECLARATIONS

Declaration of Competing 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.

Funding Statement

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Conflict of Interest

The authors of this manuscript declare no relationships with any companies, whose products or services may be related to the subject matter of the article.

REFERENCES

- [1] S. Abdulmalek *et al.*, "IoT-Based Healthcare-Monitoring System towards Improving Quality of Life: A Review," *Healthcare (Basel)*, vol. 10, no. 10, p. 1993, Oct. 2022, doi: 10.3390/healthcare10101993.
- [2] Q. Tao *et al.*, "Clinical applications of smart wearable sensors," *iScience*, vol. 26, no. 9, p. 107485, Jul. 2023, doi: 10.1016/j.isci.2023.107485.
- [3] L. A. Jawad, "Security and Privacy in Digital Healthcare Systems: Challenges and Mitigation Strategies," *Abhigyan*, vol. 42, no. 1, pp. 23–31, Mar. 2024, doi: 10.1177/09702385241233073.
- [4] A. Alotaibi, H. Aldawghan, and A. Aljughaiman, "A Review of the Authentication Techniques for Internet of Things Devices in Smart Cities: Opportunities, Challenges, and Future Directions," *Sensors*, vol. 25, no. 6, p. 1649, Jan. 2025, doi: 10.3390/s25061649.
- [5] C.-W. Lien and S. Vhaduri, "Challenges and Opportunities of Biometric User Authentication in the Age of IoT: A Survey," *ACM Comput. Surv.*, vol. 56, no. 1, pp. 1–37, Jan. 2024, doi: 10.1145/3603705.
- [6] C. Li, J. Wang, S. Wang, and Y. Zhang, "A review of IoT applications in healthcare," *Neurocomputing*, vol. 565, p. 127017, Jan. 2024, doi: 10.1016/j.neucom.2023.127017.
- [7] S. Abolhassani Khajeh, M. Saberikamarposhti, and A. M. Rahmani, "Real-Time Scheduling in IoT Applications: A Systematic Review," *Sensors*, vol. 23, no. 1, p. 232, Jan. 2023, doi: 10.3390/s23010232.
- [8] B. Aldosari, "Cybersecurity in Healthcare: New Threat to Patient Safety," *Cureus*, vol. 17, no. 5, p. e83614, doi: 10.7759/cureus.83614.
- [9] K. Fujiwara, "Knowledge distillation with resampling for imbalanced data classification: Enhancing predictive performance and explainability stability," *Results in Engineering*, vol. 24, p. 103406, Dec. 2024, doi: 10.1016/j.rineng.2024.103406.
- [10] M. Tabassum, S. Mahmood, A. Bukhari, B. Alshemaimri, A. Daud, and F. Khalique, "Anomaly-based threat detection in smart health using machine learning," *BMC Med Inform Decis Mak*, vol. 24, p. 347, Nov. 2024, doi: 10.1186/s12911-024-02760-4.
- [11] R. A. Tariq and P. B. Hackert, "Patient Confidentiality," in *StatPearls*, Treasure Island (FL): StatPearls Publishing, 2025. Accessed: Sep. 20, 2025. [Online]. Available: <http://www.ncbi.nlm.nih.gov/books/NBK519540/>

- [12] "(PDF) Behavioral Biometrics and AI for Cloud User Authentication," ResearchGate. Accessed: Sep. 20, 2025. [Online]. Available: https://www.researchgate.net/publication/389717394_Behavioral_Biometrics_and_AI_for_Cloud_User_Authentication
- [13] M. M. Taye, "Understanding of Machine Learning with Deep Learning: Architectures, Workflow, Applications and Future Directions," *Computers*, vol. 12, no. 5, p. 91, May 2023, doi: 10.3390/computers12050091.
- [14] M. Li, Y. Jiang, Y. Zhang, and H. Zhu, "Medical image analysis using deep learning algorithms," *Front Public Health*, vol. 11, p. 1273253, Nov. 2023, doi: 10.3389/fpubh.2023.1273253.
- [15] A. M. Tawfik, A. Al-Ahwal, A. S. T. Eldien, and H. H. Zayed, "Blockchain-based access control and privacy preservation in healthcare: a comprehensive survey," *Cluster Comput*, vol. 28, no. 8, p. 529, Aug. 2025, doi: 10.1007/s10586-025-05308-x.
- [16] O. Cheikhrouhou, K. Merzhad, M. Laurent, and A. Koubaa, "Blockchain and Emerging Technologies for Next Generation Secure Healthcare: A Comprehensive Survey of Applications, Challenges, and Future Directions," *Blockchain: Research and Applications*, p. 100305, May 2025, doi: 10.1016/j.bcr.2025.100305.
- [17] M. Shafay, R. W. Ahmad, K. Salah, I. Yaqoob, R. Jayaraman, and M. Omar, "Blockchain for deep learning: review and open challenges," *Cluster Comput*, vol. 26, no. 1, pp. 197–221, 2023, doi: 10.1007/s10586-022-03582-7.
- [18] A. Haleem, M. Javaid, R. P. Singh, R. Suman, and S. Rab, "Blockchain technology applications in healthcare: An overview," *International Journal of Intelligent Networks*, vol. 2, pp. 130–139, Jan. 2021, doi: 10.1016/j.ijin.2021.09.005.
- [19] R. Shinde, S. Patil, K. Kotecha, V. Potdar, G. Selvachandran, and A. Abraham, "Securing AI -based healthcare systems using blockchain technology: A state-of-the-art systematic literature review and future research directions," *Trans Emerging Tel Tech*, vol. 35, no. 1, p. e4884, Jan. 2024, doi: 10.1002/ett.4884.
- [20] E. A. Mantey, C. Zhou, S. R. Srividhya, S. K. Jain, and B. Sundaravadivazhagan, "Integrated Blockchain-Deep Learning Approach for Analyzing the Electronic Health Records Recommender System," *Front. Public Health*, vol. 10, May 2022, doi: 10.3389/fpubh.2022.905265.
- [21] A. J. D. P. Isravel, K. M. Sagayam, B. Bhushan, Y. Sei, and J. Eunice, "Blockchain for healthcare systems: Architecture, security challenges, trends and future directions," *Journal of Network and Computer Applications*, vol. 215, p. 103633, Jun. 2023, doi: 10.1016/j.jnca.2023.103633.
- [22] P. Kasralikar, O. R. Polu, B. Chamarthi, R. Veer Samara Sihman Bharatje Rupavath, S. Patel, and R. Tumati, "Blockchain for Securing AI-Driven Healthcare Systems: A Systematic Review and Future Research Perspectives," *Cureus*, Apr. 2025, doi: 10.7759/cureus.83136.
- [23] P. Das, M. Singh, and K. K. Verma, "Blockchain-Enabled Deep Learning Approach to Improve Healthcare System," *Journal of Multimedia Information System*, vol. 11, no. 1, pp. 9–16, 2024, doi: 10.33851/JMIS.2024.11.1.9.
- [24] Y. Y. Ghadi *et al.*, "The role of blockchain to secure internet of medical things," *Sci Rep*, vol. 14, no. 1, p. 18422, Aug. 2024, doi: 10.1038/s41598-024-68529-x.
- [25] M. Mamdouh, A. I. Awad, A. A. M. Khalaf, and H. F. A. Hamed, "Authentication and Identity Management of IoHT Devices: Achievements, Challenges, and Future Directions," *Computers & Security*, vol. 111, p. 102491, Dec. 2021, doi: 10.1016/j.cose.2021.102491.
- [26] E. Edozie, A. N. Shuaibu, B. O. Sadiq, and U. K. John, "Artificial intelligence advances in anomaly detection for telecom networks," *Artif Intell Rev*, vol. 58, no. 4, p. 100, Jan. 2025, doi: 10.1007/s10462-025-11108-x.
- [27] "Secure Healthcare IoT Monitoring Dataset." Accessed: Sep. 20, 2025. [Online]. Available: <https://www.kaggle.com/datasets/programmer3/secure-healthcare-iot-monitoring-dataset?resource=download>