Computer Modeling in
Engineering & Sciences

Tech Science Press

DOI: 10.32604/cmes.2023.044169

ARTICLE

Enhancing Healthcare Data Security and Disease Detection Using Crossover-Based Multilayer Perceptron in Smart Healthcare Systems

Mustufa Haider Abidi*, **Hisham Alkhalefah and Mohamed K. Aboudaif**

Department of Industrial Engineering, College of Engineering, King Saud University, P.O. Box-800, Riyadh, 11421, Saudi Arabia

*Corresponding Author: Mustufa Haider Abidi. Email: mabidi@ksu.edu.sa

Received: 23 July 2023 Accepted: 27 October 2023 Published: 30 December 2023

ABSTRACT

The healthcare data requires accurate disease detection analysis, real-time monitoring, and advancements to ensure proper treatment for patients. Consequently, Machine Learning methods are widely utilized in Smart Healthcare Systems (SHS) to extract valuable features from heterogeneous and high-dimensional healthcare data for predicting various diseases and monitoring patient activities. These methods are employed across different domains that are susceptible to adversarial attacks, necessitating careful consideration. Hence, this paper proposes a crossover-based Multilayer Perceptron (CMLP) model. The collected samples are pre-processed and fed into the crossover-based multilayer perceptron neural network to detect adversarial attacks on the medical records of patients. Once an attack is detected, healthcare professionals are promptly alerted to prevent data leakage. The paper utilizes two datasets, namely the synthetic dataset and the University of Queensland Vital Signs (UQVS) dataset, from which numerous samples are collected. Experimental results are conducted to evaluate the performance of the proposed CMLP model, utilizing various performance measures such as Recall, Precision, Accuracy, and F1-score to predict patient activities. Comparing the proposed method with existing approaches, it achieves the highest accuracy, precision, recall, and F1-score. Specifically, the proposed method achieves a precision of 93%, an accuracy of 97%, an F1-score of 92%, and a recall of 92%.

KEYWORDS

Smart healthcare systems; multilayer perceptron; cybersecurity; adversarial attack detection; Healthcare 4.0

1 Introduction

The fundamental component of everyone's quest for a better life is health, which is categorized as a complete condition of mental, physical, and social well-being. A health system possesses every organization, action, people, attempt to affect health determinants, and effort to improve health [1]. Enhancing health, maintaining health, and restoring health is the main objective of this. The healthcare domain is currently being met with developments based on new treatment methods and technologies [2]. The smart healthcare system has greatly modified medical professionals' and patients' lives. Recently, several healthcare applications are there, those are inserted in consumer devices for gathering physiological information about a patient and giving treatments in automatic [3]. The healthcare system should have access control mechanisms and policies to assist the diversity of needed access. The healthcare data has financial, operational, and clinical value when it is explored correctly for extracting primary features [4,5]. Machine learning (ML) models are currently applied in several fields [6–8]. In the healthcare domain, ML models can be used in several ways, such as exploited for extracting valuable features from the high-dimensional data for predicting various diseases as well as the activities of the patient [9]. Adversarial machine learning encompasses strategies designed to generate incorrect predictions and deceive machine learning models, rendering them ineffective when subjected to perturbed input [10]. Adversarial attacks can influence any type of data, including images and videos; therefore, ML algorithms sometimes produce inaccurate detection. Generally, maximum attacks occur in medical imaging data to change the already detected disease [11].

Adversarial attacks, as used in the context of healthcare data security, describe apparent and frequently malicious attempts to modify, falsify, or corrupt confidential patient information. These attacks can take a number of different forms, like inserting bogus data, changing patient records, or attempting to trick machine learning models by supplying carefully constructed inputs that lead to false predictions. Adversarial attacks seriously threaten the accuracy and reliability of disease detection models and healthcare data analysis.

Several methods have analyzed the impact of the attacks and security of the healthcare system for addressing adversarial attacks [12,13]. Researchers have made advancements in the adversarial attack detection model; however, the attacks on the healthcare system used in the detection require proper assessments [14]. In the realm of healthcare data analysis and disease prediction, a persistent challenge that has garnered significant attention is the issue of 'instability in disease prediction.' This phenomenon refers to the susceptibility of machine learning models, particularly those operating on complex and high-dimensional healthcare data, to exhibit fluctuations in their predictions over different instances or input variations. The instability arises due to the intricate interplay of various factors, such as data noise, feature heterogeneity, and model complexity. In practical terms, the instability in disease prediction poses a substantial barrier to machine learning models' consistent and reliable performance in healthcare applications. It engenders uncertainty in diagnoses and prognoses, impeding the seamless integration of predictive analytics into clinical decision-making workflows. The potential consequences of this instability include misclassification of diseases, inaccurate risk assessments, and hindered patient management strategies.

These methods can have issues such as identifying patient movement and have high computational costs. Some methods also have impacts in adversarial attacks that have an effect on the smart healthcare system but cannot be detected by the system's overall security. Hence, better and optimized solutions are required. Therefore, this paper proposes the Crossover-Based-Multilayer Perceptron (CMLP) method for detecting adversarial attacks in the smart healthcare domain. The main contribution of the paper is as follows:

CMLP method: To identify the patient's activities accurately, a CMLP is developed. MLP is mainly proposed for detecting patient activities with high accuracy. The crossover optimization algorithm is primarily deployed to enhance the developed MLP model.

Validation utilizing datasets: Synthetic and UQVS datasets are exploited to validate the proposed method. The synthetic dataset possesses 17000 samples, and UQVS consists of 209,115 samples, which evaluate 26 vital signs.

Improved performances: Experimental results show that the proposed method has achieved the most remarkable performance compared to the other methods. The proposed method gets good performance using performance measures such as precision, recall, F1-score, and accuracy.

In brief, in today's data-driven healthcare landscape, where the accurate and secure analysis of patient information is paramount, ensuring data integrity is a growing concern. Adversarial attacks can undermine the trustworthiness of predictive models, impeding accurate disease prediction and patient monitoring. The use of machine learning models in healthcare is significantly affected by ethical considerations, particularly those relating to patient consent and data protection. Fundamental ethical considerations include protecting patient information and obtaining explicit agreement before using data. In order to foster confidence between patients, healthcare professionals, and these automated systems, transparent and interpretable models are becoming more and more important in the field of medicine. To maintain patient rights, data security, and the general integrity of healthcare procedures, responsible development, and deployment of these models should also be guided by strict ethical norms. Addressing these concerns forms the backdrop for this research work, motivating the development and evaluation of the proposed CMLP model. The remaining work of the paper is structured as follows: Section 2 represents the related works, and Section 3 explains the proposed methodology. Section 4 demonstrates the experimental results, and the conclusion of the work is presented in Section 5.

2 Literature Review

A plethora of research is going on in the cyber-security of healthcare. Ahmed et al. [15] illustrated a patient discomfort detection model based on deep learning-based smart healthcare systems in an IoT (Internet of Things) environment. The model utilized Mask–Region-Based Convolutional Neural Network (Mask-RCNN) for detecting key points of a patient's body by different features. The adjacent key points' distance is measured to analyze the discomfort in the patient's body parts. The model's performance was evaluated using various metrics such as recall, precision, and accuracy. As a result, this model detected each organ of the human body with high accuracy. Meanwhile, it did not correctly detect the patients' head movements and facial expressions.

Tuli et al. [10] introduced an automatic heart disease detection model Health Fog using a deep-learning-based healthcare system in an internet of things (IoT) environment. The deployment of Health Fog was used to analyze the real-time heart patient data by integrating IoT and fog computing. The model was examined by using evaluation measures such as bandwidth, accuracy, response time, and energy consumption. The result found that this model offered various configurations and attained higher accuracy based on the requirements of heart patients. However, it should be noted that Health Fog only supported file-based input data.

Raina et al. [16] developed an Intelligent and Interactive Healthcare System to focus on the comprehensive utilization of Speech Recognition. The Hidden Markov Model is used for implementation since it is more practical to use a probabilistic method to hold the active characteristics of optical features. Moreover, it maximizes efficiency but automatically reduces the requirement for any human intervention in case of any failure. Speech recognition execution is provided with various resource allocations, energy optimization, and energy efficiency methods. Sufficient data is not obtainable to train the methods for effective and trustable outcomes.

Liu et al. [17] proposed deep learning (DL)-based channel state information to reveal the effective output of adversarial attacks on DL-based communication systems. A jamming attack is introduced in CsiNet to calculate the reaction of the adversarial attack and the outcomes of the NMSE computation. The COST 2100 channel version is deployed to simulate forms of channel state information (CSI) datasets in indoor and outdoor scenarios. The test results show analyzing the efficiency of mean square error and the disastrous effect of the adversarial attack on DL-based CSI feedback. The channel state information model is stricken by major attacks in several scenarios, which trigger our attentiveness to DL-based real-world atmospheres.

For the medical image evaluation mechanisms based on DL, Ma et al. [18] established an understanding of malicious attacks. The deep neural network (DNN) was the best medical image evaluation method for identifying lesions and detecting cancer. A finely conducted attack could able to make changes in the deep learning mechanisms for medical image analysis. This indicated the challenges in the implementation of these mechanisms in medical fields. A deeper knowledge of various examples of malicious attacks in clinical images was presented in this article. It was observed that the DNN used in the medical field gets easily affected by malicious attacks. The current attacks were 98% identified by the use of normal detectors. These findings could be used to develop safe deep-learning mechanisms for the medical field. An efficient intrusion detection for cloud computing was presented by Javadpour et al. [19]. Researchers also developed a distributed multi-agent intrusion detection system for cloud IoT environment called DMAIDPS [20]. The results reported that the developed system has improved metrics when compared against other systems available in the literature.

Moreover, Blockchain is a contemporary technology that is very efficient in data security [21]. In the Healthcare 4.0, Bhattacharya et al. [22] employed a Blockchain-based DL as-a-service. The sharing of health records by patients was made easier by the electronic health record (EHR), and it also developed risks such as security, privacy, and authenticity. To rectify these challenges created, a Blockchain-based Deep-Learning as-a-service (BinDaas) was proposed in their research work. The proposed method combines deep learning methods and blockchain to share the EHR records between various users. According to the cryptography based on lattices, the verification and signature method was developed in the first stage for resisting attacks between medical authorities. According to the present indicators and patient characteristics to forecast upcoming diseases, Deep Learning as-a-Service was applied to EHR datasets in the second stage. The proposed method outperformed the conventional methods in terms of communication/calculation cost, delay, accuracy, and time of mining. The high communication cost required was its limitation. Hady et al. [23] proposed a real-time Enhanced Healthcare Monitoring System (EHMS). It records patients biometrics and sent the metrics for further diagnostics and treatment. Several datasets were tested and the system performance showed and improvement of 7%–25% in some cases. Kumaar et al. [24] presented a hybrid system based on deep learning for detecting intrusions in healthcare environment. They named their systems as ImmuneNet. The suggested framework employs a variety of feature engineering techniques, class balance-improving oversampling techniques, and hyper-parameter optimization methods to achieve excellent accuracy and performance. Some other researchers utilized adaptive neuro-fuzzy inference system for intrusion detection in IoT based healthcare system [25]. The efficacy of the proposed method was tested with various databases. Jeyanthi et al. [26] presented a a recurrent neural network (RNN) and a bidirectional long short-term memory algorithm to detect and classify intrusion attempts. The results reported that the proposed system achieved an accuracy of 99.16%, sensitivity ratio of 99.89%, error rate of 0.008371%, and specificity ratio of 98.203% for the given dataset. Iwendi et al. [27] employed the random forest with genetic algorithm for intrusion detection in healthcare. A high detection and low alarm rate was reported.

Ahmed et al. [28] presented a comprehensive literature review for the ML based methods used in intrusion detection for healthcare data. Kilincer et al. [29] proposed an automated cyber-security system based on recursive feature elimination (RFE) and multilayer perceptron for detecting attacks in healthcare system. Savanović et al. [30] presented a ML method which was optimized by metaheuristics for intrusion detection in healthcare 4.0 system. XGBoost with modified firefly algorithm was utilized. To encrypt sensitive data and lessen privacy breaches and cyberattacks from unauthorized users and hackers, a Lionized remora optimization-based serpent (LRO-S) encryption method was proposed by Almalawi et al. [31]. It was reported that the suggested approach reduced the time required to encrypt and decrypt data while raising privacy standards.

The literature review reveals a notable research gap in the domain of healthcare data security and disease detection. Previous studies have often focused on individual aspects of data security or disease prediction, but there has been limited exploration of comprehensive approaches that integrate both aspects while addressing the challenges posed by adversarial attacks. This research work bridges this gap by proposing a novel CMLP model that not only enhances healthcare data security but also improves the stability and accuracy of disease detection within the context of smart healthcare systems. By amalgamating these critical components, we aim to provide a holistic solution that safeguards patient information and augments the reliability of predictive analytics in healthcare.

3 Proposed Methodology

In recent years, ML has been employed in various industries to fulfill needs; in the healthcare domain, one example is that it assists in developing models for effective results based on the patient's critical data. A schematic diagram of a smart healthcare system in a key configuration is delineated in Fig. 1. In this research work, initially, the data is collected from two different datasets, namely the synthetic dataset and the University of Queensland Vital Signs (UQVS) dataset. The collected samples are then pre-processed and provided to the CMLP neural network to detect whether the adversarial attack affects the patients' medical records.

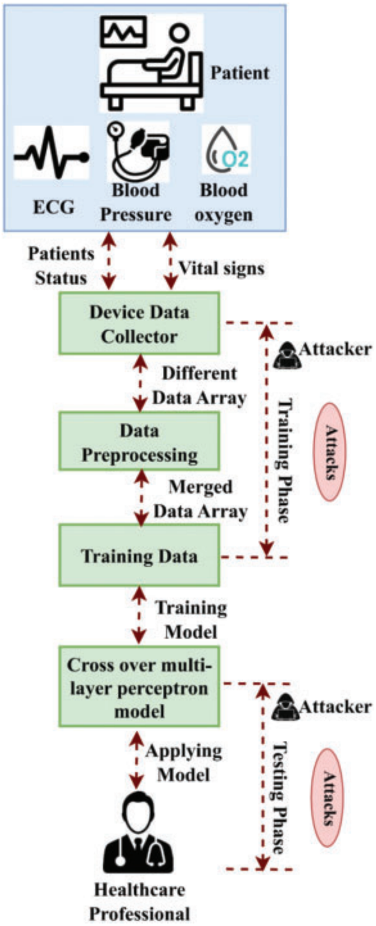


Figure 1: Architecture of the proposed model

The selection of datasets in this study was carefully considered to provide a balanced evaluation of the proposed CMLP model. The synthetic dataset was chosen due to its controllability and flexibility, enabling us to introduce and test adversarial attacks under controlled conditions systematically. The UQVS dataset, on the other hand, was selected to bring real-world relevance to our research. This dataset comprises vital signs data collected from actual healthcare scenarios, making it an ideal representative of real-world healthcare data. To ensure data quality and integrity, rigorous preprocessing steps were applied to both datasets. Data cleaning involved the identification and rectification of any missing or erroneous entries. Normalization was employed to standardize features, mitigating the influence of varying measurement units. Feature extraction was carried out with domain-specific knowledge to capture clinically relevant attributes. This combination of synthetic and real-world datasets, along with meticulous preprocessing, allowed us to evaluate the proposed CMLP model's performance across various scenarios while maintaining data quality.

The suggested CMLP model uses a novel strategy to improve transparency and comprehensibility to address concerns about machine learning model interpretability. The crossover-based process in the CMLP model lets us track information through layers, helping healthcare practitioners understand decision-making. The model emphasizes trustworthy information while minimizing noisy or unstable signals by selectively merging stable layer properties. This strengthens the model and clarifies its decision-making process. The CMLP model bridges the gap between neural network computations and healthcare professionals' demand for actionable insights they can trust by giving interpretable insights.

3.1 Data Collection and Pre-Processing

A data collector phase integrates the important symptoms of sick individuals from various smart healthcare devices and sends the data to the pre-processing phase. The data is then pre-processed on the report of the sample frequencies associated with the specimen and stored in an array. For example, monitoring a heartbeat device supervises the heart rate of sick individuals, and at the same time, an Electrocardiogram (ECG) device computes a patient's cardiac status every 10 s. Diagnostics in the smart healthcare system (SHS) utilizing the MLP model and real-time supervision pattern data are applied for training. The training data are tagged with various ailments and diseases, such as high blood pressure, low sugar, ECG, etc., in order to realize the data sample. The sick person's collected physiological data is utilized in the test module to identify the various ailments detected based on the previously trained MLP sample. Here, the attack method can be described as the pre-processing of the data pipeline. An adversary carefully maintains the training data during the MLP training phase after the attack occurs in a healthcare system and comforts the entire schooling process. Safe protocols for the transfer of data: The representation of the gathered data is: $C\_encrypted = Encrypt\ (C, Key)$, where the medical data is denoted as C, the encryption process is shown as $Encrypt(\ )$, and the encryption key is indicated as key.

3.2 Development of the Model

MLP models are highly capable of forming accurate forecasts and understanding difficult patterns; they are used abundantly in medical data analysis. To improve the safety and performance of the model, it is proposed to implement dropout regularization, and the development of the deep learning model is explained in this section. The feedforward neural network contains a few hidden layers, an output layer, and an input layer, which is the MLP. A large number of neurons are joined to form every layer, and weighted links are present between these neurons. For making accurate forecasts, studying the suitable values for these weights is the objective of the MLP model. The CMLP model addresses disease prediction instability in a novel way. Its main feature is the crossover mechanism's adaptive merging of neural network layer characteristics. Unlike conventional models that predict only from the final layer output, the CMLP model uses intermediate feature representations from multiple layers. These intermediate representations undergo a crossover process, transferring information from stable and resilient layers to fluctuating ones. This technique encourages knowledge sharing and mitigates noisy or unreliable features. The crossover mechanism helps the model capture subtle data patterns while minimizing instability-causing disturbances by selectively spreading information flow. This distinguishes the CMLP model from conventional schemes, making disease prediction more resilient.

The MLP is determined from the artificial neural network (ANN) that is employed with more than one hidden layer. A huge number of hidden layers are obtained in the central portion, including input and output. The simple MLP model is employed with one hidden layer that is determined as a three-layer structure. The MLP is composed of two parts a feedforward neural network and an error-back propagation algorithm. The neuron received from the input is related to the threshold ϕ and later implemented through an activation function *a(.)* that generates output. The output of a single hidden layer neuron is formulated as:

$$x = a\left(\sum_{j=1}^{t} v_j y_j - \phi\right) \tag{1}$$

From the above equation v_j and y_j are the input function. Detecting disorders in healthcare is still considered a challenging role in medical analysis. So, to overcome this situation, the activation function makes the neural network an efficient method. The expression for the sigmoid activation function is expressed as:

$$S\left(y\right) = \frac{1}{1 + e^{-x}} \tag{2}$$

3.2.1 Multi-Layer Feedforward Neural Network

It is determined based on MLP to predict the disease accurately in health care. In this approach, each neuron is interconnected with one another but not merged with the same layer i.e., it does not provide a cross-layer connection. The input neuron gathered from g^{th} the hidden layer is formulated as:

$$\gamma_g = \sum_{j=1}^{b} u_{jg} y_j \tag{3}$$

The output of the hidden layer is determined as:

$$\alpha_i = \sum_{g=1}^{s} v_{gi} c_g \tag{4}$$

The output of g^{th} a neuron is represented as:

$$c_g = a\left(\gamma_g - \ell_g\right) = a\left(\sum_{j=1}^{b} u_{jg} y_j - \ell_g\right) \tag{5}$$

The final output layer of the perceptron is expressed as:

$$x_i = k\left(\alpha_i - \phi_i\right) = k\left(\sum_{g=1}^{s} v_{gi}c_g - \phi_i\right) = k\left[\sum_{g=1}^{s} v_{gi} \cdot a\left(\sum_{j=1}^{b} u_{jg}y_j - \ell_g\right) - \phi_i\right] \tag{6}$$

where the threshold of the hidden layer is denoted as $l_{g,}$ the output layer threshold is indicated by ϕ_i. The connection weight among the input and hidden layer is represented as u_{jg} based on j^{th} function, and for i^{th} neurons, it is indicated by v_{gi}. The output activation function is indicated by $k(.)$. The forward propagation model of a three-layer perceptron is generated in the form of a matrix.

$$X = \begin{bmatrix} x_1 \\ \vdots \\ x_i \\ \vdots \\ x_m \end{bmatrix} = \left(\begin{bmatrix} v_{11} & \cdots & v_{1g} & \cdots & v_{1s} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ v_{i1} & \cdots & v_{ig} & \cdots & v_{is} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ v_{m1} & \cdots & v_{mg} & \cdots & v_{ms} \end{bmatrix} \begin{bmatrix} c_1 \\ \vdots \\ c_g \\ \vdots \\ c_s \end{bmatrix} - \begin{bmatrix} \phi_1 \\ \vdots \\ \phi_i \\ \vdots \\ \phi_m \end{bmatrix}\right) = k\left(v\begin{bmatrix} c_1 \\ \vdots \\ c_i \\ \vdots \\ c_s \end{bmatrix} - \phi\right) \tag{7}$$

$$= \left(k\,.\,a\left(\begin{bmatrix} u_{11} & \cdots & u_{1j} & \cdots & u_{1b} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ u_{g1} & & u_{gj} & \cdots & u_{gb} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ u_{s1} & \cdots & u_{sj} & \cdots & u_{sb} \end{bmatrix} \begin{bmatrix} y_1 \\ \\ y_j \\ \\ y_b \end{bmatrix} - \begin{bmatrix} \ell_1 \\ \\ \ell_g \\ \\ \ell_s \end{bmatrix}\right) - \phi\right) = k\left(v.a\left(uy - \ell\right) - \phi\right) \tag{8}$$

3.2.2 Error Backpropagation Algorithm

In order to update the function, the backpropagation is performed in a MLP, which updates the loss function of the optimization parameter. The differences obtained between the predicted and theoretical values are estimated using the mean squared error characterization, which demonstrates the learning accuracy of the MLP. The training of the output neural network is expressed as follows:

$$\hat{x}_n = \left(\hat{x}{}_1^n, \hat{x}{}_2^n, \cdots, \hat{x}{}_m^n\right) \tag{9}$$

where

$$\hat{x}{}_i^n = a(\alpha_i - \phi_i),\ i = 1, 2, \cdots, m \tag{10}$$

The mean squared for the training set is formulated as:

$$F_n = \frac{1}{2}\sum_{i=1}^{m}\left(\hat{x}{}_i^n - x_i^n\right)^2 \tag{11}$$

Based on the gradient descent strategy, the backpropagation optimizes the negative gradient function. The learning rate $\eta \epsilon (0, 1)$ is utilized to direct the step size at each iteration. The updated value is formulated as:

$$\Delta v_{gi} = -\eta\frac{\partial F_n}{\partial v_{gi}} \tag{12}$$

From the above equation, the connection weight is denoted by v_{gi}. The activation function for the hidden and output layer based on the sigmoid function is expressed as:

$$a' (y) = a (y) \ (1 - a (x)) \tag{13}$$

Integrating Eqs. (10) and (11) the gradient strategy is obtained as:

$$k_i = -\frac{\partial F_n}{\partial \hat{x}_i^n} \cdot \frac{\partial \hat{x}_i^n}{\partial \alpha_i} = -\left(\hat{x}_i^n - x_i^n\right) a' (\alpha_i - \phi_i) = \hat{x}_i^n \left(1 - \hat{x}_i^n\right) \left(x_i^n - \hat{x}_i^n\right) \tag{14}$$

The output of MLP based on error propagation diminished the cumulative error obtained while training.

$$F = \frac{1}{r} \sum_{n=1}^{r} F_n \tag{15}$$

However, the error determined in the back-propagation is validated before updating the layer. The hidden and output layer function is processed, and the cumulative error will be determined as 10^{-3}, or the iterative process will exceed 10^5.

In the case of training data, the MLP models are specialized; in the case of unseen data, the MLP models fail to generalize. The frequently occurring problem in the MLP models is overfitting, which will reduce safety and performance in medical data analysis. The dropout regularization is applied in the MLP model to solve this problem. At the time of training, by randomly deactivating a few of the neurons, the problem of overfitting is prevented by the dropout regularization technique. The model is forced to understand many representations, and the dropout process introduces redundancy. The model easily makes forecasts and depends less on particular links by unevenly dropping neurons. In the MLP model, the dropout normalization is usually linked after one or more hidden layers. The dropout rate is the probability of being dropped allotted to every neuron in the hidden layer while the training occurs. 0.2 to 0.5 is the rate of normal dropout; the complexity of the model and the particular dataset decides the optimal rate of dropout. The dropout is executed at the time of the MLP model's forward pass, and zero is fixed as the activations of the neurons drop. For maintaining the anticipated resulting magnitude, the scaling factor $1/(1 - dropout\_rate)$ is used for the leftover active neurons. The entire input for the upcoming layers is maintained roughly constant by this scaling, and at the time of training, it recompenses for the neurons that are deactivated. The representation of the MLP model's forward pass equation utilizing dropout normalization is given below:

$$MLP\_output = MLP\left(C\_input, W\_mlp, b\_mlp\right), \tag{16}$$

Here the input data is mentioned as C_input, the weight of the MLP is indicated as W_mlp, and the term of bias is given as b_mlp. Dropout layers are inserted between the hidden layers, deactivating a certain number of neurons based on the dropout rate. Dropout regularization is implemented in the MLP model to enhance both the safety of medical data analysis and the generalization of the model. Using dropout offers several advantages, including improved performance on unfamiliar data, reduced reliance on specific connections, and the ability to identify strong features.

3.3 Cybersecurity and Privacy Elements

3.3.1 Mechanisms for Access Control

The channel for communication present in between the storage of medical data and the end user is secured by the Elliptic Curve Integrated Encryption Scheme (ECIES) during the execution of mechanisms for access control. The system is used to safeguard the valid user's public key. The request for accessing medical data by an end user is encrypted with the receiver's public key utilizing ECIES. Data decryption can only be done with the particular key of the valid user.

3.3.2 Encryption of Data

The ECIES is used to safeguard medical data while transferring and storing. The information is encrypted with the receiver's public key utilizing ECIES before transferring or storing. From this, it is known that confidential medical information can only be decrypted and used by the receiver who has the particular private key.

1. **Key Generation:** Initially, the creation of an elliptic curve key pair is included in the key generation process. A private key (c) is produced approximately, and the congruent public key (R) is obtained, and the base point of the elliptic curve by the private key ($R = c * H$) is increased. The elliptic curve parameters and the base point (H) are preplanned and assigned to the contract parties.
2. **Encryption:** The following steps are taken using ECIES to encrypt the message (m).
   a. ***Random Secret Generation:*** For every encryption, a random secret key (l) is produced to get uniform encryption, and the secret key is employed for MAC keys.
   b. ***Key Derivation*:** The receiver's public key (Q) is increasing with the sender's private key to obtain the shared secret (T). The shared secret ($T = c * Q$) is then the uniform encryption key (KE) and the MAC key (KM) to get the random secret (k) is employed in the key derivation function (KDF).
   c. ***Symmetric Encryption:*** With the obtained encryption key the message (m) is encrypted using a uniform encryption algorithm, such as AES and it assures the surreptitiousness of the message.
   d. ***Message Authentication Code (MAC) Generation:*** HMAC and MAC are applied to produce MAC in the encrypted message along with the obtained MAC key. The MAC guarantees the encrypted message's integrity and discovers any interception efforts.
   e. ***Public Key and Encrypted Data Packaging:*** In the ciphertext, the public key is used for encryption and the encrypted data consists of the sender.
3. **Decryption:** Using ECIES the receiver executes the following steps to decrypt the ciphertext (Q, C):
   a) ***Key Derivation:*** Increasing the receiver's private key with the sender's public key is used to obtain the secret key (T). The shared secret key ($T = c * R$) is then used during encryption with the uniform and MAC keys as the random secret keys obtained in the key derivation function.
   b) ***MAC Verification:*** Using the received MAC key the MAC is computed for the derived encrypted data, and the probity of the encrypted data is cross-checked when the computed MAC suits the obtained MAC.
   c) ***Symmetric Decryption:*** The encrypted data, the received encryption key, and a similar uniform encryption algorithm are decrypted and used during encryption, and the original message (m) is shown by the decrypted data.

3.3.3 Data Access Logging and Auditing

When recording instances of data access, ECIES can be applied to keep in existence a preserved record of data acquisition activities data can be encrypted with the public key of the recording system.

The acquired records are preserved in the form of encryption, assured only decrypted by the official recording system. The surreptitiousness and integrity of the records are kept in existence, storing unofficial access by employing ECIES to access data records.

3.3.4 Security Training and Awareness

In the context of safety training and awareness programs, the use of ECIES can be implemented to promote secure communication. When distributing sensitive training materials or information among multiple contributors, the message can be encrypted using the ECIES public key of each contributor. This ensures that only authorized users with the corresponding private key can decrypt and access the training materials, thereby maintaining confidentiality and preventing unauthorized dissemination. This approach ensures the confidentiality and controlled distribution of sensitive information, reducing the risk of unofficial spreading and unauthorized access.

3.3.5 Crossover Based MLP Algorithm for Adversarial Attack Detection

The application of a crossover AOA-based MLP pattern in safeguarding healthcare data enhances the aspect of two-step authentication. Following this, the recipients are prompted to undergo authentication for the second factor, and upon successful user authentication, access is granted. A Time-based One-Time Password (TOTP) method, such as a mobile application, generates a unique one-time code to implement the two-step authentication. A shared secret key and the current-time code are generated, and the receiver's computer verifies the second component of the code. The system ensures that only authorized individuals can interact with the healthcare data by integrating two-step authentication, valid credentials, and second-factor verification.

3.4 Arithmetic Optimization Algorithm (AOA)

The Arithmetic optimization algorithm (AOA) [32] is a completely new meta-heuristic method. The important suggestion of this algorithm is to mix the four conventional arithmetic operators in mathematics, i.e., subtraction (*s*), multiplication (*m*), division (*d*), and addition (*a*). Similar to the sine-cosine algorithm (SCA), AOA additionally has a very easy shape and occasional computation complexity. The M and D operators inside the iterations can generate big steps *m* and *d*, specifically within the exploration phase where the result is carried out. The declaration is as follows:

$$Wj\left(s+1\right)=\begin{cases} Wq(s)/(MoP+EPS).\left(\left(ub-lb\right)\lambda+lb\right), & RAND<0.5 \\ Wa\left(s\right).MoP.\left(\left(ub-lb\right)\lambda+lb\right), & RAND\geq 0.5 \end{cases} \tag{17}$$

wherein EPS is the smallest positive number, and λ is a continuous coefficient that is cautiously deliberate for this set of rules. During iterations, the MoP is decreased non-linearly from 1 to 0, and the advent is as follows:

$$MoP=1-\left(\frac{s}{S}\right)^{\frac{1}{\beta}} \tag{18}$$

According to the AOA β is a continuous variable, which is set to 5 according to the AOA.

From the above equation, M and D operators each have very consistent postures at the concept of what the hunt agent can produce. Instead, s and a operators had been used to prominence neighborhood exploitation, which creates small steps within the search location. The numerical notation is represented as:

$$Wj\,(s+1) = \begin{cases} Wa\,(s) - MoP\ .\,((ub-lb)\,\lambda + lb)\,, & RAND < 0.5 \\ Wa\,(s)\ .\ MoP\,.\,((ub-lb)\,\lambda + lb)\,, & RAND \geq 0.5 \end{cases} \tag{19}$$

For an optimization algorithm to explore and exploit, there may be no ambiguity approximately the consequences of equilibrium. In AOA, the MOA parameter is used for the duration of iterations to change exploration and exploitation, which is represented as:

$$MoA\,(s) = MINI + s\left(\frac{MAXI - MINI}{S}\right) \tag{20}$$

where $MINI$ and $MAXI$ are constant values. According to Eq. (20), MOA increases from Min to Max. Therefore, in the preliminary stage, the search agent operates in the seek area and has a greater opportunity to explore even as the search agent is much more likely to act the search close by the optimal position. In order to enhance the exploration and exploitation capability, a crossover strategy is established. In the crossover operation, a hybrid offspring is created by combining two parent solutions using the crossover operator, preserving the characteristics of both parent solutions in the offspring [33]. The equation presented below describes the crossover utilized in the current work.

$$f_r = \begin{cases} e_r^q & if\ i_q \leq XV \\ a_r^q & otherwise \end{cases} \tag{21}$$

Here the rate of crossover is XV. The evenly issued random number in the range [0,1] is denoted as i_q. The parent solutions used for crossing are e_r and a_r. The value of 0.3 is fixed as the crossover probability XV of the current work. By comparing the robustness of the present solution vector and the updated solution vector, the selection of greedy determines whether the vector f_r which is updated, exists or not in the upcoming generation. The following equation defines the selection operator:

$$a_{r,g+1} = \begin{cases} f_{r,g} & if\,k\left(f_{r,g}\right) \leq k\left(a_{r,g}\right) \\ a_{r,g} & if\,k\left(f_{r,g}\right) > k\left(a_{r,g}\right) \end{cases} \tag{22}$$

Here the objective function is denoted as k. For the challenge of minimization, this selection process can be used. The solution's populations in the flat search locations are steered by the inequality $\leq$ implemented, and it prevents solutions from immobility. Thus, by employing crossover based MLP algorithm, the medical data of various patients are protected from adversarial attack. Fig. 2 below describes the developed hybrid algorithm.

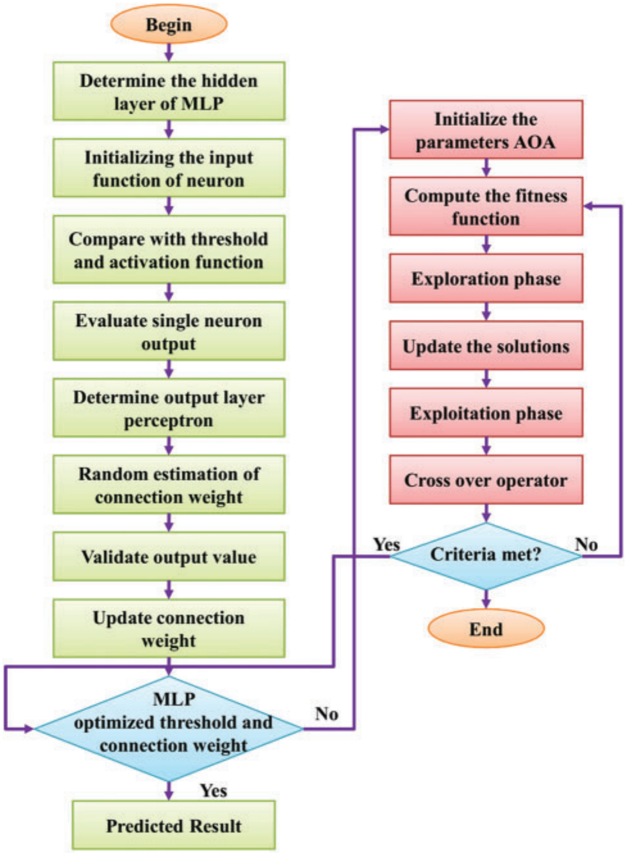

Begin
Determine the hidden layer of MLP
Initializing the input function of neuron
Compare with threshold and activation function
Evaluate single neuron output
Determine output layer perceptron
Random estimation of connection weight
Validate output value
Update connection weight
MLP optimized threshold and connection weight
No
Yes
Predicted Result
Initialize the parameters AOA
Compute the fitness function
Exploration phase
Update the solutions
Exploitation phase
Cross over operator
Criteria met?
Yes
No
End

Figure 2: MLP based crossover AOA algorithm

4 Results and Discussions

This paper presents the proposed CMLP method for accurately identifying the patient's activities. The method simulates various attacks in MATLAB using Python library and implements Keras and Scikit-Learn library on the Google Collab platform to test the dataset. The algorithm and computation was peformed on i7 processor with 16 Gb RAM, and 4 GB graphics card. Hyperparameter tuning was conducted to optimize the CMLP model's performance. This process involved systematic adjustments to parameters such as learning rates, batch sizes, and the number of hidden layers to achieve the best results. For the training-validation split, an 80–20 ratio was adopted, where 80% of the dataset was used for training, and the remaining 20% was designated for validation. To further assess the model's robustness, a cross-validation procedure using k-fold cross-validation (with k = 5) on both the synthetic and UQVS datasets was conducted. This approach involved splitting the data into k subsets (folds), training the model on k-1 folds, and validating it on the remaining fold. This process was repeated k times, rotating the validation fold each time. The results from each iteration were then averaged to provide a more robust estimate of the model's performance. This method is assessed with various metrics such as precision, accuracy, recall, and F1-score, and these results are compared with existing methods such as DL-based CSI [17], Blockchain-based DL [22], and Mask-RCNN [15].

4.1 Data Collection

This work collects data from the UQVS dataset, which consists of almost 16,000 data samples [34]. The samples in the dataset are divided into training and testing in the ratio of 80:20. In data analysis, this research utilized the MLP model to learn complex patterns and provide accurate predictions. When implementing access control mechanisms, ECIES can be used to secure the communication channel between the user and the healthcare data repository. ECIES is used to protect the communication channel between the healthcare data repository and the user. This ensures that only authenticated users with the corresponding private key can decrypt and access the data. This research implements a two-factor authentication phase, which increases healthcare data security by MLP model. For identifying the various activities of the patient, the proposed CMLP utilizes correlation among several medical devices. Here, that correlation is utilized to execute the crafting decision tree untargeted attacks for finding more important devices. The untargeted attack assumes and utilizes the total training sample to generate adversarial examples. To change the state of the disease from a stroke to an abnormal oxygen level, hemoglobin devices were established for observing the untargeted attack. Likewise, the glucose device is influenced when modifying the disease state, as mentioned from high cholesterol to stroke. An oxygen saturation device, heart rate, and glucose are more influenced devices, and these devices perform the untargeted attack. Table 1 depicts the parameters involved, its final state, affected device as well as device count.

Table 1: Status of every affected device and device count

Current state	Final state	Affected device	Device count
High blood pressure	Stroke	Glucose	One
Stress	Heart attack	Blood oxygen	One
Abnormal oxygen level	Stroke	Heart rate, glucose	Two
High cholesterol	Stroke	Glucose	One
Sleeping	Drunk	Alcohol	One
Stroke	Abnormal oxygen level	Glucose, hemoglobin	Two

4.2 Evaluation Measures

The evaluation in terms of precision, accuracy, recall, and F1-score is conducted to validate the performance of the proposed CMLP model.

Accuracy: Accuracy is the most basic measurement used to evaluate the effectiveness of the model. It is defined as the number of correct predictions to the total number of predictions. Accuracy measures the overall correctness of the model's predictions, providing a global assessment of its performance. In healthcare data security and disease detection, high Accuracy indicates the model's capability to make correct predictions across various scenarios, contributing to reliable decision support.

$$A_{ccuracy} = \frac{True_{Positive} + True_{Negative}}{True_{Positive} + True_{Negative} + False_{Positive} + False_{Negative}} \tag{23}$$

Precision: Precision is the measurement used to analyze positive predictions. Precision quantifies the model's ability to correctly identify relevant instances among all instances it classifies as positive. In healthcare data security, a high Precision signifies that the model's positive predictions are highly accurate, reducing the chances of false alarms and unnecessary alerts. It is defined as the ratio of true positives to the summation of true positives and false positives.

$$P_{recision} = \frac{True_{Positive}}{True_{Positive} + False_{Positive}} \tag{24}$$

Recall: Recall is the measurement used to analyze the number of true positive samples. Recall, also known as Sensitivity or True Positive Rate, measures the model's ability to correctly identify relevant instances among all actual positive instances. In the context of healthcare data security, a high Recall ensures that the model effectively detects adverse events, minimizing the risk of data breaches and unauthorized access. It is defined as the ratio of true positives to the sum of false negatives and true positives.

$$R_{ecall} = \frac{True_{Positive}}{True_{Positive} + False_{Negative}} \tag{25}$$

F1-score: F1-score is the harmonic mean of precision and recall, and during the precision-recall tradeoff, if the precision increase, recall decrease and vice versa. The F1-score strikes a balance between Precision and Recall, offering a single metric that considers both false positives and false negatives. In the healthcare domain, a high F1-score signifies a model's proficiency in achieving accurate, reliable, and balanced predictions, which is crucial for data security and disease detection scenarios.

$$F1_{score} = 2 \times \frac{(P_{recision} \times R_{ecall})}{P_{recision} + R_{ecall}} \tag{26}$$

4.3 Performance Analysis

The performance of the developed algorithm is evaluated based on the above-mentioned measures. Fig. 3a demonstrates the effects of device reduction in terms of the effectiveness of untargeted attacks. The success rate of the proposed attack is dropped when the number of devices is decreased. To remove 2 devices (glucose, blood oxygen) and 1 device, the proposed attains the greatest success rate of 14.60% than the existing methods. The proposed method attains the greatest success rate of 16.45% in removing three devices: oxygen, glucose, and heart rate. To eliminate one, two, and three devices, as can be seen in Fig. 3b. By decreasing the devices at SHE, the effectiveness of adversarial attacks decreased in short.

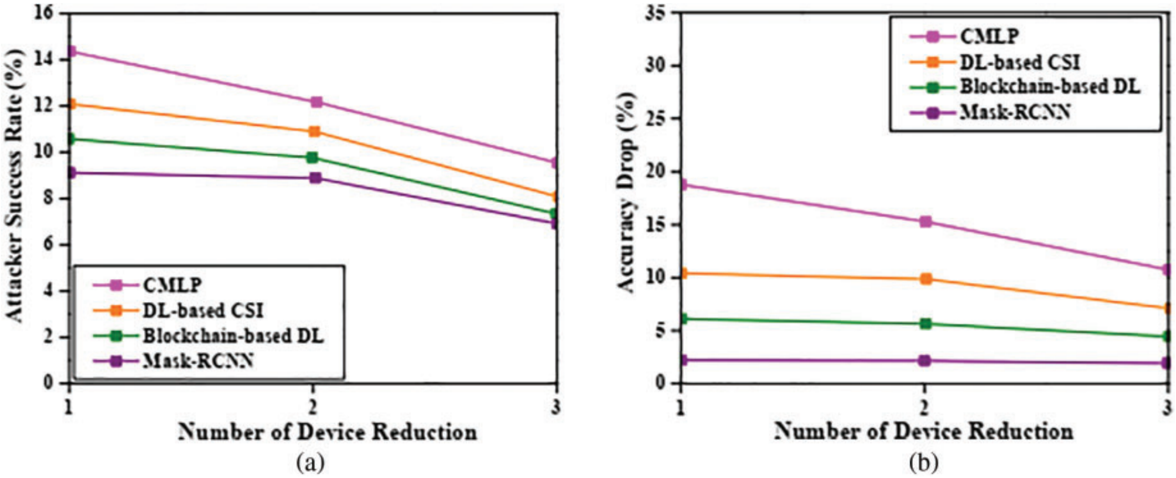


Figure 3: Analysis based on (a) attacker success rate (b) accuracy drop rate

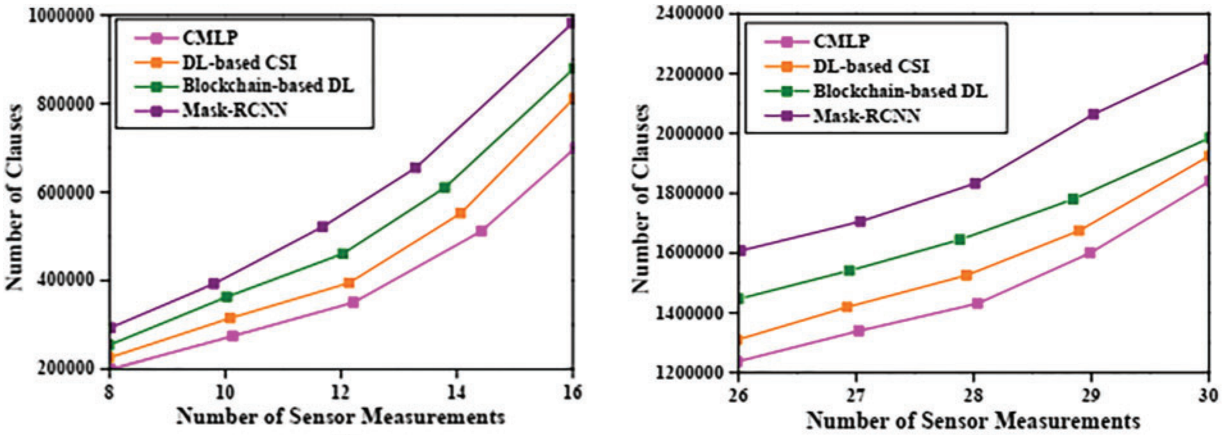
4.3.1 Assessment with Various Attack Algorithms

Here, in CMLP, two attacks are executed such as a black box and white box attack, to assess the proposed model's effectiveness by several algorithms. Table 2 shows the effectiveness of the various methods with the proposed method. In Table 2, the proposed method has a 32.30% for success rate and a 15.70% for accuracy drop in both targeted attack and targeted attack. The existing Mask-RCNN method attained an 8.32 accuracy drop lower than the proposed method as well as it attained a success rate of 9.26. The proposed method achieved a success rate of 8.22 and a 12.29 accuracy drop in the black box.

Table 2: Performance analysis

Methods	Accuracy drop	Success rate	Actual accuracy
Proposed	32.66	8.5	97.56
DL-based CSI	20.44	7.77	88.66
Blockchain-based DL	24.18	8.65	89.21
Mask-RCNN	8.32	7.99	87.32

The time complexity of the proposed method is analyzed with the existing methods. Fig. 4a demonstrates the complexity analysis of the proposed method. The proposed method obtains low complexity in the synthetic data. It has low complexity in 10 sensors with 1600000 clauses. The proposed method achieves low complexity in the clauses. Fig. 4b shows the complexity of using UQVS data. In the UQVS data, when compared to existing techniques, the proposed method has low complexity in 10 sensors with 200000 clauses. Hence, these methods are utilized across various domains which will be affected by adversarial attacks.



(a) (b)

Figure 4: Complexity analysis for (a) synthetic data (b) UQVS data

The performance is evaluated by comparing the proposed CMLP method with the existing DL-based CSI, Blockchain-based DL, and Mask-RCNN. Fig. 5a shows the accuracy analysis of the proposed method. The proposed method and existing methods are compared in terms of detecting activities. The proposed method achieves a higher accuracy of 97% than the other methods. The DL-based CSI attains an accuracy of 94%, 85% for the Blockchain-based DL method, and Mask RCNN reaches an accuracy of 91%. The graphical representation of the precision analysis is illustrated in Fig. 5b. From the figure, it can be see seen the proposed method attains a precision of 93% higher than the existing methods.

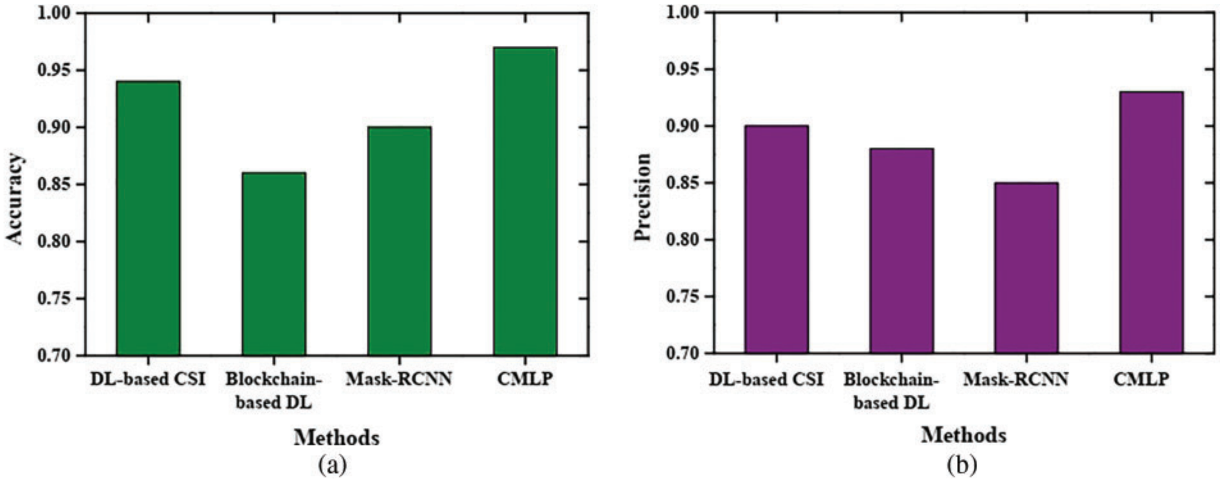


Figure 5: Comparative analysis for (a) accuracy and (b) precision

Fig. 6a demonstrates the recall analysis with the comparison of the proposed method and other methods. When comparing the existing methods with the proposed method, the proposed method outperformed the existing methods. It achieves a recall of 92% more than the other methods. The DL-based CSI method attains a recall of 90%, the Blockchain-based DL method achieves a recall of 86%, and the mask RCNN method has 85%. Fig. 6b illustrates the F1-score analysis for the proposed method. The proposed method attains an F1-score of 92% in the comparison of existing methods. The methods get an F1-score of 90% for DL-based CSI, .80% for Blockchain-based DL, and 85% for mask-RCNN.

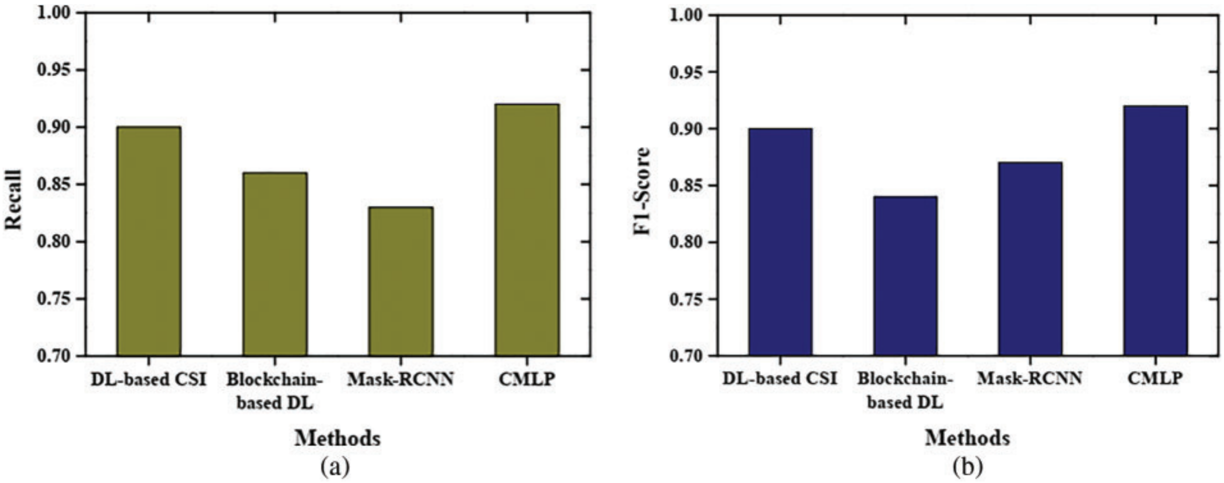


Figure 6: Comparative results based on (a) recall and (b) F1-score

The achieved accuracy, precision, recall, and F1-score bear significant practical implications in the realm of healthcare data security and disease detection. The high precision indicates a low rate of false alarms, ensuring that healthcare professionals can confidently act on model alerts without being inundated with erroneous notifications. The equally high recall signifies the model's ability to effectively detect potential issues, minimizing the risk of missed critical events. The impressive F1-score balances precision and recall and demonstrates the model's proficiency in maintaining accuracy while providing comprehensive coverage.

In practical terms, this translates to a more secure environment for healthcare data, where there is a substantially lower risk of data breaches and illegal access. It simultaneously improves disease detection accuracy, enabling prompt intervention and accurate patient management. These metrics demonstrate the value and relevance of this study in enhancing the dependability and security of smart healthcare systems.

To provide a more comprehensive comparison, a thorough assessment of the proposed CMLP model was made against three existing methods: DL based CSI, Blockchain-based DL, and Mask-RCNN. This detailed evaluation sheds light on the CMLP model's unique advantages in healthcare data security and disease detection. While DL-based CSI exhibits competence in certain predictive tasks, it may be vulnerable to adversarial attacks and often lacks transparency. The CMLP model excels by integrating a crossover-based mechanism that enhances both security and interpretability. Blockchain-based DL offers data security but can introduce computational inefficiencies and scalability challenges. The CMLP model, through its feature fusion approach, manages to provide robustness against adversarial attacks without compromising computational efficiency. Mask-RCNN, designed for image segmentation, may not seamlessly translate to healthcare data security and disease detection, particularly with non-image data. The CMLP model's adaptability to diverse data types and its ability to effectively handle adversarial attacks position it as a more versatile solution in the healthcare domain.

CMLP model addresses adversarial attacks by selectively fusing features from different layers, prioritizing reliable information while attenuating noisy or adversarial signals. Its adaptability to diverse healthcare data types and its capability to maintain robustness without sacrificing computational efficiency sets it apart from other approaches.

5 Conclusions

Machine learning methods are used to analyze large amounts of patient data in the healthcare industry. However, these models face several challenges due to their instability in disease prediction. To address this drawback, this research proposed a novel adversarial CMLP-based attack. This method used the UQVS dataset and some performance evaluation measures such as accuracy, precision, recall, and F1-score. The performance of the proposed CMLP model is validated by comparing it with existing methods such as DL-based CSI, Blockchain-based DL, and Mask-RCNN. The model achieved an accuracy of 97%, a precision of 93%, a recall of 92%, and an F1 score of 92%, respectively. The experimental result revealed that the proposed CMLP model performs better than the existing methods.

While the proposed CMLP model presents several advantages, it is essential to acknowledge its limitations and identify avenues for future research. One potential limitation lies in its susceptibility to highly sophisticated adversarial attacks that may exploit intricate data correlations. Further research into advanced adversarial defense mechanisms could enhance the model's resilience. Additionally, while our model demonstrates robustness in offline experiments, deploying it in real-time automated disease detection systems poses practical challenges. Considerations such as data privacy, real-time processing constraints, and scalability need to be carefully addressed. Strategies for secure and efficient data transmission and processing warrant exploration, especially in cloud-based healthcare systems. Its effective application in real-world healthcare settings will depend on recognizing its limitations and resolving deployment issues that arise in the real world, paving the way for a safer and more dependable healthcare ecosystem.

In the future, this proposed CMLP model will be applied in a real-time automated disease detection system. Future research could also focus on enhancing the model's interpretability further, making it more accessible to healthcare professionals. Incorporating domain-specific knowledge or designing user-friendly interfaces could facilitate seamless integration into clinical workflows.

Acknowledgement: The authors extend their appreciation to King Saud University for funding this work through Researchers Supporting Project Number (RSP2024R499), King Saud University, Riyadh, Saudi Arabia.

Funding Statement: This research was funded by King Saud University through Researchers Supporting Program Number (RSP2024R499).

Author Contributions: The authors confirm contribution to the paper as follows: study conception and design: M.H.A., H.A., M.K.A.; methodology: M.H.A., H.A.; data collection: M.H.A., M.K.A.; analysis and interpretation of results: M.H.A., H.A.; draft manuscript preparation: M.H.A., H.A., M.K.A. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: All the databases and their reference source are mentioned in the paper.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

1. Islam, M. M., Rahaman, A., Islam, M. R. (2020). Development of smart healthcare monitoring system in IoT environment. *SN Computer Science, 1(3),* 185.
2. Yahya, Z., Hassan, M., Younis, S., Shafique, M. (2020). Probabilistic analysis of targeted attacks using transform-domain adversarial examples. *IEEE Access, 8,* 33855–33869.
3. Selvakkumar, A., Pal, S., Jadidi, Z. (2022). *Addressing adversarial machine learning attacks in smart healthcare perspectives*, pp. 269–282. Cham: Sensing Technology.
4. Maqsood, M., Yasmin, S., Gillani, S., Aadil, F., Mehmood, I. et al. (2023). An autonomous decision-making framework for gait recognition systems against adversarial attack using reinforcement learning. *ISA Transactions, 132,* 80–93.
5. Anthi, E., Williams, L., Javed, A., Burnap, P. (2021). Hardening machine learning denial of service (DoS) defences against adversarial attacks in IoT smart home networks. *Computers & Security, 108,* 102352.
6. Abidi, M. H., Alkhalefah, H., Mohammed, M. K. (2022). Mutated leader sine-cosine algorithm for secure smart IoT-blockchain of Industry 4.0. *Computers, Materials & Continua, 73(3),* 5367–5383. https://doi.org/10.32604/cmc.2022.030018
7. Abidi, M. H., Mohammed, M. K., Alkhalefah, H. (2022). Predictive maintenance planning for Industry 4.0 using machine learning for sustainable manufacturing. *Sustainability, 14*. https://doi.org/10.3390/su14063387

8. Alkahtani, M., Abidi, M. H., Obaid, H. S. B., Alotaik, O. (2023). Modified gannet optimization algorithm for reducing system operation cost in engine parts industry with pooling management and transport optimization. *Sustainability, 15(18),* 13815.
9. Ali, F., El-Sappagh, S., Islam, S. M. R., Kwak, D., Ali, A. et al. (2020). A smart healthcare monitoring system for heart disease prediction based on ensemble deep learning and feature fusion. *Information Fusion, 63,* 208–222.
10. Tuli, S., Basumatary, N., Gill, S. S., Kahani, M., Arya, R. C. et al. (2020). HealthFog: An ensemble deep learning based smart healthcare system for automatic diagnosis of heart diseases in integrated IoT and fog computing environments. *Future Generation Computer Systems, 104,* 187–200.
11. Finlayson, S. G., Bowers, J. D., Ito, J., Zittrain, J. L., Beam, A. L. et al. (2019). Adversarial attacks on medical machine learning. *Science, 363(6433),* 1287–1289.
12. Kebande, V. R., Alawadi, S., Awaysheh, F. M., Persson, J. A. (2021). Active machine learning adversarial attack detection in the user feedback process. *IEEE Access, 9,* 36908–36923.
13. Hao, J., Tao, Y. (2022). Adversarial attacks on deep learning models in smart grids. *Energy Reports, 8,* 123–129.
14. Newaz, A. I., Haque, N. I., Sikder, A. K., Rahman, M. A., Uluagac, A. S. (2020). Adversarial attacks to machine learning-based smart healthcare systems. *GLOBECOM 2020—2020 IEEE Global Communications Conference*, pp. 1–6. Taipei, Taiwan.
15. Ahmed, I., Jeon, G., Piccialli, F. (2021). A deep-learning-based smart healthcare system for patient's discomfort detection at the edge of internet of things. *IEEE Internet of Things Journal, 8(13),* 10318–10326.
16. Raina, R., Jha, R. K. (2022). Intelligent and interactive healthcare system (I2HS) using machine learning. *IEEE Access, 10,* 116402–116424.
17. Liu, Q., Guo, J., Wen, C. K., Jin, S. (2020). Adversarial attack on DL-based massive MIMO CSI feedback. *Journal of Communications and Networks, 22(3),* 230–235.
18. Ma, X., Niu, Y., Gu, L., Wang, Y., Zhao, Y. et al. (2021). Understanding adversarial attacks on deep learning based medical image analysis systems. *Pattern Recognition, 110,* 107332.
19. Javadpour, A., Abharian, S. K., Wang, G. (2017). Feature selection and intrusion detection in cloud environment based on machine learning algorithms. *2017 IEEE International Symposium on Parallel and Distributed Processing with Applications and 2017 IEEE International Conference on Ubiquitous Computing and Communications (ISPA/IUCC)*, pp. 1417–1421. Guangzhou, China.
20. Javadpour, A., Pinto, P., Ja'fari, F., Zhang, W. (2023). DMAIDPS: A distributed multi-agent intrusion detection and prevention system for cloud IoT environments. *Cluster Computing, 26(1),* 367–384.
21. Abidi, M. H., Alkhalefah, H., Umer, U., Mohammed, M. K. (2021). Blockchain-based secure information sharing for supply chain management: Optimization assisted data sanitization process. *International Journal of Intelligent Systems, 36(1),* 260–290.
22. Bhattacharya, P., Tanwar, S., Bodkhe, U., Tyagi, S., Kumar, N. (2021). BinDaaS: Blockchain-based deep-learning as-a-service in Healthcare 4.0 applications. *IEEE Transactions on Network Science and Engineering, 8(2),* 1242–1255.
23. Hady, A. A., Ghubaish, A., Salman, T., Unal, D., Jain, R. (2020). Intrusion detection system for healthcare systems using medical and network data: A comparison study. *IEEE Access, 8,* 106576–106584.
24. Akshay Kumaar, M., Samiayya, D., Vincent, P. M. D. R., Srinivasan, K., Chang, C. Y. et al. (2022). A hybrid framework for intrusion detection in healthcare systems using deep learning. *Frontiers in Public Health, 9.*
25. Akram, F., Liu, D., Zhao, P., Kryvinska, N., Abbas, S. et al. (2021). Trustworthy intrusion detection in E-healthcare systems. *Front Public Health, 9,* 1–10.
26. Jeyanthi, D. V., Indrani, B. (2023). IoT-based intrusion detection system for healthcare using RNNBiLSTM deep learning strategy with custom features. *Soft Computing, 27(16),* 11915–11930.

27. Iwendi, C., Anajemba, J. H., Biamba, C., Ngabo, D. (2021). Security of Things intrusion detection system for smart healthcare. *Electronics, 10*. https://doi.org/10.3390/electronics10121375
28. Si-Ahmed, A., Al-Garadi, M. A., Boustia, N. (2023). Survey of machine learning based intrusion detection methods for Internet of Medical Things. *Applied Soft Computing, 140,* 110227.
29. Firat Kilincer, I., Ertam, F., Sengur, A., Tan, R. S., Rajendra Acharya, U. (2023). Automated detection of cybersecurity attacks in healthcare systems with recursive feature elimination and multilayer perceptron optimization. *Biocybernetics and Biomedical Engineering, 43(1),* 30–41.
30. Savanović, N., Toskovic, A., Petrovic, A., Zivkovic, M., Damaševičius, R. et al. (2023). Intrusion detection in Healthcare 4.0 Internet of Things systems via metaheuristics optimized machine learning. *Sustainability, 15(16),* 12563.
31. Almalawi, A., Khan, A. I., Alsolami, F., Abushark, Y. B., Alfakeeh, A. S. (2023). Managing security of healthcare data for a modern healthcare system. *Sensors, 23(7),* 3612.
32. Zheng, R., Jia, H., Abualigah, L., Liu, Q., Wang, S. (2021). Deep ensemble of slime mold algorithm and arithmetic optimization algorithm for global optimization. *Processes, 9*. https://doi.org/10.3390/pr9101774
33. Gupta, S., Deep, K. (2019). Improved sine cosine algorithm with crossover scheme for global optimization. *Knowledge-Based Systems, 165,* 374–406.
34. Imtiazul Haque, N., Ashiqur Rahman, M., Hasan Shahriar, M., Ataur Khalil, A., Uluagac, S. (2021). A novel framework for threat analysis of machine learning-based smart healthcare systems. https://doi.org/10.48550/arXiv.2103.03472