DL-based Wearable Scheme for Remote Monitoring of Patient Data in Healthcare 4.0

Fenil Ramoliya*, Krisha Darji†, Rajesh Gupta‡ *Member, IEEE*, Riya Kakkar§*Student Member, IEEE*, Sudeep Tanwar¶, *Senior Member, IEEE*, Aparna Kumari ‖
*†‡§¶‖Department of Computer Science and Engineering, Institute of Technology, Nirma University, Ahmedabad, India
Emails: *21bce244@nirmauni.ac.in, †21bce043@nirmauni.ac.in, ‡rajesh.gupta@nirmauni.ac.in,
§21ftphde56@nirmauni.ac.in, ¶sudeep.tanwar@nirmauni.ac.in ‖aparna.kumari@nirmauni.ac.in,

***Abstract*—The paper articulates an exploration into the integration of wearable devices for remote patient data monitoring, which marks a transformative shift in healthcare practices. This transition is underscored by user-centric interfaces and applications, enabling convenient remote monitoring. However, the escalating concern of patient data vulnerability to network breaches presents a substantial impediment. In response, we introduce the proposed scheme that harnesses Machine Learning (ML) and Deep Learning (DL) techniques. The main objective of the proposed scheme is to meet the exacting requirements of healthcare systems, aiming to fortify data integrity and confidentiality. Within this context, the proposed scheme unveils a sophisticated DL-driven detection model, adeptly tailored for discerning and countering data manipulation endeavors through a nuanced multi-label classification paradigm. Notably, the emphasis lies on safeguarding patient data privacy and security, which is paramount in today's information-rich landscape. The narrative seamlessly interweaves elements of wearable technology, sensor networks, advanced DL capabilities, and robust security measures, resulting in an innovative scheme. Finally, the proposed scheme is evaluated against various metrics such as accuracy and loss curve and F1, recall, and precision comparison.**

Index Terms*—*Healthcare 4.0, Wearable Devices, Remote Monitoring, DL, ML

I. Introduction

Digital technology has made remarkable advancements since the onset of the 21st century, and these transformations are exerting a profound impact on the global healthcare approach. Spanning from the rudimentary therapeutic practices of ancient civilizations to the intricate healthcare systems of contemporary society, the significance of healthcare has remained paramount throughout history. Initiating its journey in 1970, the healthcare sector is still in its early developmental phase, denoted as Healthcare 1.0, owing to its nascent initiatives and limited resource availability. After this, the evolution of Healthcare 2.0 was propelled by an upsurge in Information Technology (IT) advancements and medical innovations, leading to the emergence of advanced medical imaging, tracking systems, and novel healthcare paradigms [1]. The integration of computational methodologies and information processing systems catalyzed the inception of revolutionary and efficient therapeutic approaches. This transition marked the advent of Healthcare 3.0, from 2006 to 2015, gaining substantial traction. This era bore witness to the enthusiastic embrace of Electronic Health Record (EHR), empowering medical practitioners with expeditious access to pertinent clinical insights [2].

The fourth industrial revolution, denoted as healthcare 4.0, aspires to amalgamate information, processes, equipment, and operational technologies with cyber-physical systems [3]. Innovative advancements encompassing the Internet of Health Things (IoHT), medical Cyber-Physical Systems, health cloud, health fog, extensive data analytics, machine learning, blockchain, and intelligent algorithms are thoughtfully integrated and operationalized within the approach of Healthcare 4.0. The overarching goal of Healthcare 4.0 is to furnish individuals with more proficient, valuable, and accessible healthcare services, concurrently elevating the efficiency and efficacy of the healthcare domain. Healthcare 4.0 encompasses diverse capabilities, including internet-based patient monitoring, health-oriented mobile applications, and real-time telemedicine, thereby substantiating its indispensability in contemporary healthcare paradigms.

The seamless integration of patients and medical professionals within an interconnected ecosystem has ushered in a new era of patient care in the dynamic realm of Healthcare 4.0, offering remote real-time monitoring of crucial health metrics. Intuitive interfaces and applications facilitate this transformative shift, empowering healthcare providers to remotely access instantaneous sensor data from wearable devices affixed to the patient's person and environmental sensors. However, this remarkable stride is not without its challenges, chief among them being the susceptibility of patient data to malevolent network breaches. Consequently, the imperative of modern-era healthcare data security cannot be overstated. Numerous researchers employ cryptography to intertwine security measures intricately. To fortify the bedrock of security, an enhanced cryptographic methodology for safeguarding healthcare medical records suggests a refined rendition of the hill cipher, incorporating a dual-step encryption and decryption procedure, as proposed by Paragas [4]. Meanwhile, Saxena *et al.* [5] put forth a proposition for an Artificial Intelligence (AI)-based wireless network data security system for medical records, employing the tenets of cryptography. Although cryptography conventionally serves as the bulwark for securing data during transit and storage, it rarely attains full-fledged implementation of selective access control. Addressing this gap within the ambit of healthcare 4.0, while concurrently augmenting data privacy has spurred researchers and academicians to embrace solutions hinged on Machine Learning (ML).

A notable illustration is the ML-infused security approach designed for intelligent healthcare systems, featuring a quartet of distinct ML-powered detection techniques for identifying and countering malicious activities, as introduced by Newaz

et al. [6]. Similarly, Kaur *et al.* [7] contribute an expansive secure healthcare approach anchored in big data and ML. Within this context, a comprehensive survey by Qayyum *et al.* underscores the recommendation for a secure and resilient ML approach tailored to the healthcare sector, a facet accentuated by their endorsement of machine learning and big data analytics for illness diagnostics, albeit with limited emphasis on data privacy and security [8]. In this context, an innovative breakthrough is introduced as a DL-based proposed scheme designed to address a significant challenge. Within the realm of healthcare 4.0, this DL model is developed to analyze patient information remotely, ensuring the security of their data. The primary aim of this DL-based model is to harness the power of AI and ML algorithms proactively. It aims to preemptively detect and thwart any unauthorized access, manipulation, or interference with patient data during transmission. This objective is achieved by deploying advanced algorithms that consistently monitor data streams, differentiate wearable device types, detect irregular trends, and promptly alert medical experts whenever any unusual activity is detected. By employing DL methodologies, patient data is safeguarded and its integrity is maintained during the transmission process. This technological advancement ultimately enhances patient safety remotely and elevates healthcare outcomes.

A. Research Contributions

Following are the research contributions of this paper.

- The proposed scheme presents a robust DL solution that identifies source devices and ensures data integrity for the patient through the wearable devices, bolstering security in healthcare 4.0.
- We propose novel fusion techniques to integrate diverse sensor data from wearables, refining inputs for DL-driven analysis and enabling precise patient monitoring in real time.
- The proposed DL-based scheme for remote patient health monitoring is evaluated considering various parameters such as accuracy curve, loss curve, confusion matrix, F1, recall, and precision comparison.

B. Organization of the Paper

The rest of the paper is organized as follows. Section II discusses the system model and problem formulation of the proposed scheme and Section III highlights the elaborated proposed scheme. Next, Section IV presents the performance evaluation of the proposed scheme. Finally, the paper is concluded with future work in Section V.

II. System Model and Problem Formulation

This section delves into the system model and problem formulation of the suggested approach.

A. System Model

In the rapidly evolving landscape of healthcare 4.0, where innovation and patient well-being are paramount, the strategic integration of DL-driven wearable systems is a beacon of transformative potential. We present an advanced DL-driven approach tailored for remote analysis and interpretation of patient ($\mathbb{P}$) data from wearable devices. This system design ensures a seamless flow of critical information while upholding stringent security and privacy measures. Our proposed approach integrates seamlessly with healthcare practices, prioritizing innovation and patient well-being, which relies on a sophisticated DL (Λ_{DL}) solution to identify source devices and ensure data integrity accurately. This approach involves an array of wearable devices, including biosensors ($\mathbf{S}_\alpha$), environmental sensors ($\mathbf{S}_\beta$), encompassing heart rate ($\mathbf{S}_\gamma$), electrocardiogram ($\mathbf{S}_\epsilon$), respiratory rate meter ($\mathbf{S}_\vartheta$), temperature ($\mathbf{S}_\iota$), blood pressure ($\mathbf{S}_\upsilon$), forming a comprehensive sensor network $\mathbb{E}$. Data pre-processing refines raw input ($\mathbf{D}_{\text{raw}}$) by unwanted disturbances elimination, irregularities removal, and the chronological order arrangement through advanced signal processing techniques. Fusion techniques amalgamate diverse data sources into a coherent $\mathbf{X}$, serving as a basis for DL-driven analysis.

The fused and refined data, denoted as $\mathbf{X}$, is efficiently transmitted via robust communication protocols. The selection of networking methods, including Low Power Wide Area Networks (LPWAN) protocols like Long Range Radio (LoRaWAN) ($\boldsymbol{\kappa}$), Narrowband-Internet of Things (NB-IoT)($\boldsymbol{\eta}$), Sigfox ($\boldsymbol{\vartheta}$), and Weightless-N ($\boldsymbol{\varrho}$). These protocols exhibit an exquisite synergy between extensive range coverage, minimal energy consumption, and commendable data transmission rates to make data transmission ($\mathbf{X}_{transmission}$) robust and reliable. At the core of the proposed scheme lies a sophisticated DL model that engages in multi-label classification, adeptly identifying wearable sources and detecting unauthorized activities during data transmission. Verified patient data is seamlessly delivered to medical professionals via an intuitive real-time dashboard powered by DL. This orchestration of advanced wearables, data processing, communication protocols, and DL-driven insights promises to redefine patient monitoring within healthcare 4.0, enabling proactive interventions and elevated patient well-being.

B. Problem Formulation

The proposed scheme synergistically integrates the imperatives of patient data security and the intricate task of wearable data classification. This harmonized approach is meticulously designed to ensure data's uninterrupted, real-time, and precision-driven conveyance to attending medical practitioners. Within this system, the comprehensive aggregation of data originating from an array of real-time wearable devices collectively denoted as (D_{raw}) matrix in Eq. 1. The combined data is then subjected to a crucial signal pre-processing step to form $\mathbf{D}_{\text{pre-processed}}$. Each pre-processing operation P_i represents a tailored transformation honed to extract nuanced physiological insights as per Eq. 2 to ensure the reliability of remotely valuable data transfer.

$$\mathbf{D}_{\text{raw}} = \sum_{i=1}^{N} (\alpha \cdot \mathbf{S}_\alpha + \beta \cdot \mathbf{S}_\beta + \gamma \cdot \mathbf{S}_\gamma + \ldots) \tag{1}$$

where α, β, γ, and so on, are weights assigned to the data collected from sensors $\mathbf{S}_\alpha$, $\mathbf{S}_\beta$, $\mathbf{S}_\gamma$, and so forth. N represents the number of sensors.

$$\mathbf{D}_{\text{pre-processed}} = P_N(\ldots P_2(P_1(\mathbf{D}_{\text{raw}}))\ldots) \tag{2}$$

The refined $\mathbf{D}_{\text{pre-processed}}$ takes centre stage within a complex strategy guided by the fusion matrix $\mathbf{W}$. $\mathbf{W}$ skillfully uses

coefficients and weights to direct a multidimensional transformation. This process creates unified and comprehensive $\mathbf{X}$, as demonstrated in Eq. 3.

$$\mathbf{X} = \mathbf{D}_{\text{pre-processed}} \times \mathbf{W} \tag{3}$$

The symphony of data transmission protocols adds another layer of adaptivity to this comprehensive approach. Considering the intricacies of LPWAN protocols. Their dynamic interplay, guided by the fusion matrix $\mathbf{W}$, exemplifies a nuanced data communication pattern, ensuring that the transmitted data reaches its destination with utmost accuracy and reliability. Eq. 4 represents the selection of protocol module suitable for dynamic real-time scenarios and Φ_T signifies the optimal transmission configuration that maximizes the weighted aggregation of protocol attributes.

$$\Phi_T = \arg \max_{\mathbf{S}_\kappa, \mathbf{S}_\eta, \mathbf{S}_\vartheta, \mathbf{S}_\varrho} \{\mathbf{S}_\kappa \cdot \boldsymbol{\kappa} + \mathbf{S}_\eta \cdot \boldsymbol{\eta} + \mathbf{S}_\vartheta \cdot \boldsymbol{\vartheta} + \mathbf{S}_\varrho \cdot \boldsymbol{\varrho}\} \tag{4}$$

To counter anonymous data manipulation and ensure device-specific accuracy, we deploy Λ_{DL}, an advanced AI approach. It classifies transmitted data into multi-label categories, enhancing efficiency, security, and reliability within the remote wearable data transmission ecosystem. We introduce a complex optimization formulation with $\boldsymbol{\theta}$ as learnable parameters, aiming to minimize $\mathcal{L}$ over M instances while considering regularization $\mathcal{R}$. The loss function $\mathcal{L}(\mathbf{x}_i, \mathbf{y}_i; \boldsymbol{\theta})$ measures dissimilarity between predicted $\mathbf{y}_i$ and ground truth, with λ controlling regularization. This process mitigates overfitting and encourages parameter sparsity, ensuring robust optimization.

$$\boldsymbol{\theta}^* = \arg\min_{\boldsymbol{\theta}} \left\{ \frac{1}{M} \sum_{i=1}^{N} \mathcal{L}(\mathbf{x}_i, \mathbf{y}_i; \boldsymbol{\theta}) + \lambda \cdot \mathcal{R}(\boldsymbol{\theta}) \right\} \tag{5}$$

Upon obtaining the outcomes as $\boldsymbol{\theta}^*$, the medical professional or supervising physician will promptly receive a notification and acknowledgement from the system regarding the received data along with its corresponding sensor device details. If the received data has been subject to unauthorized manipulation or tampering during transmission, the system alerts the medical authority. The severity of this alert is contingent upon the threat posed by the detected anonymous activity.

III. The Proposed Scheme

Fig. 1 The proposed scheme encompasses of the 3-layered architecture, i.e., wearable data acquisition layer, data preprocessing layer, data transmission layer, DL layer, and medical authority layer.

A. Wearable Data Acquisition Layer

The foundation and main layer of the proposed scheme includes the crucial component of the system. As previously explained, the proposed scheme incorporates various wearable sensors capable of gathering a wide range of data points. The patient is neither restricted nor uncomfortable during this continuous data gathering because it is carried out in a non-intrusive way. The unobtrusiveness of these sensors is one of their phenomenal qualities, guaranteeing that the patient's mobility (Υ) and flexibility of movement are unaffected. This is crucial because it allows patients to continue their everyday activities and participate in physical activity, giving a more realistic picture of their overall health. This data aggregation aims to make complete and all-encompassing health monitoring possible.

$$\mathbf{D}_{\text{raw}} = \Upsilon\Bigg(\int (\mathbb{V}_T * \text{RR}, \frac{(\frac{\rho_{ADC}}{2^n} - \frac{1}{2}) * (VCC)}{\rho_G}, \ldots) \Bigg) \tag{6}$$

In Eq. 6, tidal volume (the amount of air that passes through the lungs adequately during a breath) is represented as a $\mathbb{V}_T$ and respiratory rate is represented by RR which will integrate and give real-time respiratory minute volume ($\mathbf{S}_\vartheta$). The conversion of the analog sensor signals into digital values in the range of 0 to 2^{n-1} (n=sampling resolution, typically 8-bit or 16-bit) is a crucial transition that takes place. The raw digital format in which these digitized values represent the transmitted data is designated as ρ_{ADC}. An operational voltage known as VCC is used at specific times when aiding the patient and a crucial part of patient data assessment, is calculated using the ρ_G data, which is obtained from the sensor gain. The person's mobility (Υ) is unaffected by the seamless integration of sensor outputs. This strategy ensures a smooth user experience while permitting in-depth health information and analyses.

B. Signal Data Pre-processing Layer

The signal data pre-processing layer significantly boosts the quality and dependability of the data while processing health signals from multiple sensors. In order to ensure that the data analysis and interpretation that follow are accurate and meaningful, this layer is intended to reduce noise and artifacts that can be present in the raw sensor inputs.

$$\mathbf{D}_{\text{pre-processed}} = \sum_{n=0}^{N-1} \mathbf{D}_{\text{raw}_n} * e^{\frac{-i2\pi kn}{N}} \tag{7}$$

The Fast Fourier Transform (FFT) algorithm as shown in Eq. (7) is indispensable to the preprocessing layer. It transforms the unprocessed time-domain signal into its frequency-domain equivalent. This enables us to determine which frequencies are present in the signal along with what proportions. $\mathbf{D}_{\text{pre-processed}}$ represents the complex output value at a frequency in the frequency domain with N as the total number of samples in the input signal. $\mathbf{D}_{\text{raw}_n}$ is the input sample at time index n in the time domain. i is the imaginary unit ($\sqrt{(-1)}$) and k is the frequency index.

C. Data Transmission Layer

A vital tool for revolutionizing healthcare through remote monitoring, data analysis, and informed decision-making, LPWAN provides effective, low-power, and long-range communication. A private wireless sensor network built with LPWAN is used to gather and transmit health data from various sensors. Before transmission, the health information gathered from various sensors can be pre-processed. To minimize the quantity of the data and improve transmission, this preprocessing includes operations like filtering, aggregating, or

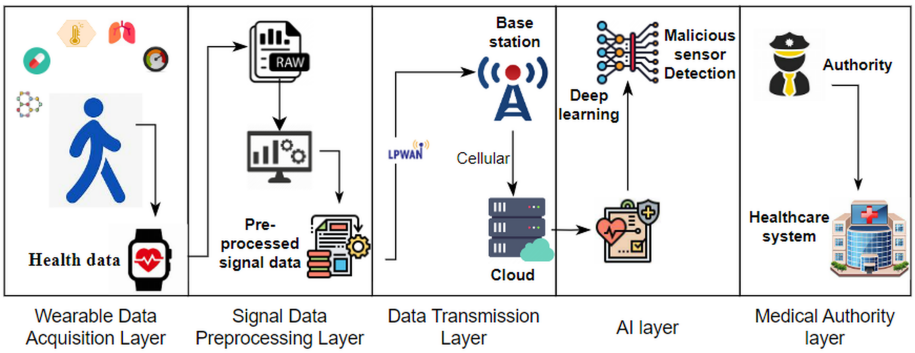


Fig. 1: The proposed scheme.

compression. This is crucial in LPWAN networks since they have less capacity than conventional wireless networks.

$$X_{\text{transmission}}(t) = \frac{1}{\sqrt{2\pi\sigma^2}} \int_{-\infty}^{\infty} e^{-\frac{(u-\mu)^2}{2\sigma^2}} \cdot X(u) \cdot P_{\text{transmit}}(u)\, du \tag{8}$$

where $X_{\text{transmission}}(t)$ represents the transmitted data matrix at time t, μ denotes the mean of the transmission probability distribution, σ^2 denotes the variance of the transmission probability distribution, $P_{\text{transmit}}(u)$ is the transmission probability function at time u, and it is a variable that ranges over time and is used as the integration variable.

D. DL layer

Functioning as the central intelligence of the private wireless sensor network, the DL layer plays a vital role in upholding the reliability of health-related data while also safeguarding against unauthorized access. The model Λ_{DL} trained on a specialized dataset focused on security within the realm of IoT healthcare [9]. In the initial stage of this architecture, comprising 22 neurons, a deliberate selection is made from a broader dataset containing 52 features, ensuring that only the most relevant 22 features are utilized. These chosen features then serve as input for the subsequent processing by the DL model. To further enhance the system's accuracy, an intricate neural network model is developed, incorporating 12 layers that strategically combine dense and dropout layers as shown in Fig. 2. This intricate structure is designed to effectively harness the power of these layers, facilitating proficient feature learning. Throughout the dense layers, Rectified Linear Unit (ReLU) activation functions are frequently applied, contributing to the model's capability to derive valuable insights from the data. In the final layer of the architecture, an outer layer, a sigmoid activation function is employed. This choice is made to optimise the model's overall performance and ensure precise predictions of results, which is especially crucial in the context of accurate outcome forecasting. Algorithm 1 shows the algorithmic flow defined for explaining the DL-based multi-label classification applied for predicting manipulated patient data through wearable devices.

$$\mathbf{Prc}^{\text{micro}} = \frac{\sum_{c_i \in \mathbf{C}} \text{TPs}_{c_i}}{\sum_{c_i \in \mathbf{C}} (\text{TPs}_{c_i} + \text{FPs}_{c_i})} \tag{9}$$

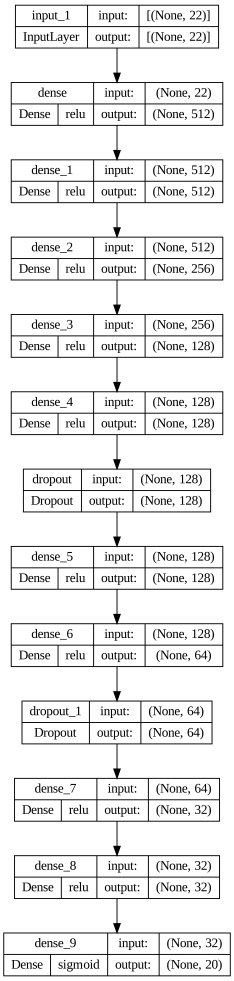
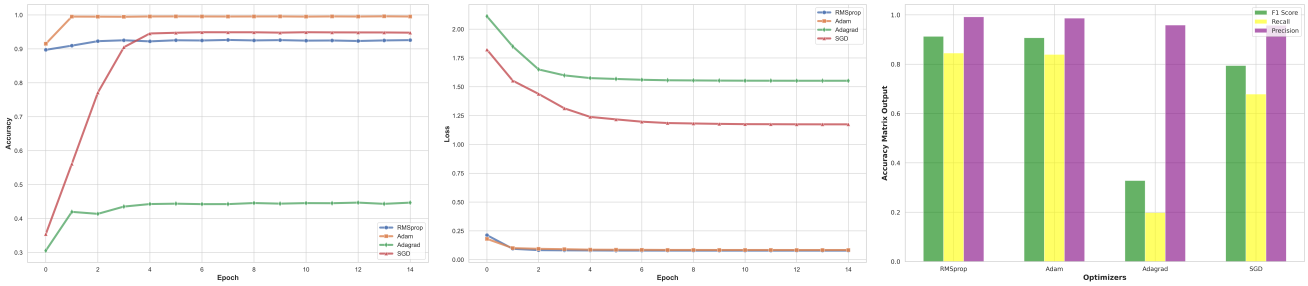


Fig. 2: DL working model.

$$\mathbf{Rcl}^{\text{micro}} = \frac{\sum_{c_i \in \mathbf{C}} \text{TPs}_{c_i}}{\sum_{c_i \in \mathbf{C}} (\text{TPs}_{c_i} + \text{FNs}_{c_i})} \tag{10}$$

In micro-averaging all True Positives (TPs), True Negatives (TNs), False Positives (FPs), and False Negatives (FNs) for each class ($\mathbf{C}$) are summed up and then the average is taken. Here precision is denoted as $\mathbf{Prc}^{\text{micro}}$ and recall is expressed as $\mathbf{Rcl}^{\text{micro}}$.



(a) Accuracy curve. (b) Loss curve. (c) F1, recall, and precision comparison.

Fig. 3: (a) Accuracy curve for DL model using different optimizers during the training, (b) Loss curve for DL model using different optimizers during the training, (c) F1, recall, and precision score comparison across different optimizers for testing set.

Algorithm 1 DL-based Multilabel Classification Algorithmic Flow.

Input: $\mathbf{D}_{\text{raw}}, \mathbf{D}_{\text{pre-processed}}, \mathbf{X}, X_{\text{transmission}}$

Output: $\Phi_T, \boldsymbol{\theta}^*, \Psi, \mathbf{Prc}^{\text{micro}}, \mathbf{Rcl}^{\text{micro}}$
Initialization: $\Delta_j = 0.05$,p$= 3, LR_0 = 0.001, f = 0.02$, epochs=15

procedure DL_PRED($\mathcal{S}, F$)
  if $\mathbf{D}_{\text{raw}} \in (\mathbb{P}, \mathbb{E})$ **then**
    $\mathbf{D}_{\text{raw}} = \sum_{i=1}^{N} (\alpha \cdot \mathbf{S}_\alpha + \beta \cdot \mathbf{S}_\beta + \gamma \cdot \mathbf{S}_\gamma + \ldots)$
    $\mathbf{D}_{\text{pre-processed}} = P_N(\ldots P_2(P_1(\mathbf{D}_{\text{raw}}))\ldots)$
    $\mathbf{X} = \mathbf{D}_{\text{pre-processed}} \times \mathbf{W}$
    $\boldsymbol{\theta}^* = \arg\min_{\boldsymbol{\theta}} \left\{ \frac{1}{M} \sum_{i=1}^{N} \mathcal{L}(\mathbf{x}_i, \mathbf{y}_i; \boldsymbol{\theta}) + \lambda \cdot \mathcal{R}(\boldsymbol{\theta}) \right\}$
    $\mathbf{Prc}^{\text{micro}} = \frac{\sum_{c_i \in \mathbf{C}} \text{TPs}_{c_i}}{\sum_{c_i \in \mathbf{C}} (\text{TPs}_{c_i} + \text{FPs}_{c_i})}$
    $\mathbf{Rcl}^{\text{micro}} = \frac{\sum_{c_i \in \mathbf{C}} \text{TPs}_{c_i}}{\sum_{c_i \in \mathbf{C}} (\text{TPs}_{c_i} + \text{FNs}_{c_i})}$
    $M = \frac{1}{1+e^{-\omega}}$
  end if
end procedure

The "ReduceLROnDrop" Keras callback dynamically modulates the learning rate based on shifts in validation accuracy. If validation accuracy (Δ_j) substantially drops below the threshold (δ, set to 0.05), the learning rate diminishes by a factor (f, set to 0.2), enhancing the model's adaptability to accuracy fluctuations. Additionally, when validation accuracy remains static for p epochs (patience=3), the learning rate sequentially decreases, promoting convergence. By adeptly adapting the learning rate, this approach optimizes model training based on real-time accuracy dynamics.

$$LR_{j+1} = LR_j \times f \tag{11}$$

Or, for persistent accuracy stability over p epochs:

$$LR_{j+p+1} = LR_j \times f^p \tag{12}$$

where j denotes the epoch index, LR_j stands for the learning rate at epoch t, and Δ_j signifies the accuracy change at epoch j.

E. Medical Authority layer

This layer assumes a pivotal role as the ultimate sentinel within the DL-driven wearable scheme's architecture for remote patient data monitoring. Its mandate encompasses the meticulous validation of the veracity of received data, engendering an environment of unwavering trust and data fidelity. By judiciously scrutinizing the outcomes of the DL classification stratum, the medical authority layer orchestrates a nuanced comparison against the anticipated comportment and attributes associated with the ascribed wearable device. This culminates in a comprehensive assessment, quantified by a sophisticated metric of similarity, which acts as a discerning arbiter of data integrity.

$$M = \frac{1}{1 + e^{-\omega}} \tag{13}$$

$$\Psi = \begin{cases} \text{Alert or Strategic Intervention,} & \text{if } M < T \\ \text{Deferred Alert or Proximate Action,} & \text{if } M \geq T \end{cases} \tag{14}$$

where M is the Quantitative Integrity Metric (QIM), serving as an indicator of the degree of congruence and ω represents multidimensional dissimilarity measure, intricately derived from a fusion of diverse feature-level divergences, including statistical moments, spectral variances, and correlation coefficients. The epochal deliberations of the medical authority layer are epitomized by an intricate dichotomy threshold T.

IV. Performance Evaluation

This section undertakes an in-depth evaluation of the proposed multi-label classification scheme, which is aimed at ensuring the integrity of wearable device identity and the security of remotely transmitted patient data using a DL approach. To refine our model's training process, a comprehensive analysis and comparison of advanced optimization algorithms were conducted. These optimizers were chosen due to their proven effectiveness across diverse DL applications. The experimental setup is meticulously designed to maintain consistent conditions, including dynamic learning rate configurations, which are uniformly applied over 15 epochs, batch size of 64, and a fixed kernel regularizer of 0.001 to promote model generalization and mitigate overfitting concerns.

The visualization of accuracy curves is a pivotal juncture in the performance evaluation. As showcased in Fig. 3a, each optimizer's accuracy trajectory unfolds distinctly. Adam's exceptional prowess is particularly striking, boasting

a training accuracy pinnacle of 0.9971—an unequivocal testament to its adeptness in steering the model toward precision. Concurrently, Stochastic Gradient Descent (SGD) garners commendable achievement, securing a noteworthy accuracy of 0.9882. The Root Mean Square Propagation (RMSprop) optimizer solidifies its standing with an appreciable accuracy of 0.9582, thus establishing its reliability. It is imperative, however, to acknowledge the Adaptive Gradient (Adagrad) comparatively subdued performance, recording the lowest accuracy at 0.5572. This outcome accentuates the potential limitations of Adagrad within our specific context. These findings inherently underscore the paramount importance of strategic optimizer selection, unravelling nuanced implications for optimizing multi-label classification performance.

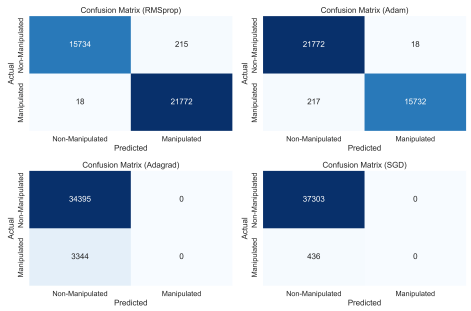


Fig. 4: Confusion matrix for different optimizers.

The scrutiny of loss curves, presented in Fig. 3b, yields profound insights into the optimization dynamics. Strikingly, both Adam and RMSprop consistently demonstrate the most favourable convergence outcomes, yielding notably minimal binary cross-entropy losses of 0.0761 and 0.0774 on the testing dataset. These compelling values stand as a testament to the inherent efficacy of these optimizers in steering our model toward convergence. In contrast, SGD surfaces with a slightly heightened loss metric yet maintains competitive performance with a minimum recorded loss of 1.5407. Noteworthy, however, is Adagrad's persistent emergence with the highest loss magnitudes within the cadre of evaluated optimizers, reaching a minimal value of 1.1605. These empirical findings hold valuable implications for the discerning choice of optimizers in the context of multi-label classification tasks, thereby augmenting the overarching efficacy of our proposed methodology.

Within the context of Fig. 3c, a comprehensive analysis unfolds, presenting a side-by-side comparison of F1, recall, and precision scores across various optimizers using a multi-bar graph format. The F1 scores achieved by Adam and RMSprop optimizers are of particular significance, reaching 0.9068 and 0.9025, respectively. These are complemented by recall values of 0.8391 and 0.8449, along with precision values of 0.9863 and 0.9818. In contrast, Adagrad registers an F1 score of 0.3280, while SGD achieves 0.7941, shedding light on their distinct performances. These metrics collectively emphasize the nuanced interrelation between precision and recall, elucidating the optimizers' prowess in navigating the intricate landscape of label associations inherent in multi-label classification scenarios.

The confusion matrix is a vital analytical tool in multi-label classification, crucial in our research with four distinct optimization algorithms. It comprehensively breaks down outcomes—true positive, true negative, false positive, and false negative. For the proposed scheme, the matrix serves a dual role: precisely identifying data origin among 18 devices, detecting data manipulation, and securing remote patient data. Fig. 4 shows the confusion matrix visually represents our classification efforts, enriched by four optimization algorithms. It captures multifaceted outcomes in DL exploration in classifying whether provided input is manipulated or not. In this, Adam performed quite well as compared to other optimizers.

V. Conclusion

In this paper, we harnessed the capabilities of AI to address the crucial challenge of ensuring the integrity and security of patient health data processed through wearable devices in healthcare 4.0. By employing an advanced DL model, the proposed has the capacity to meticulously analyze and scrutinize incoming data streams, identifying subtle and complex patterns that may indicate malicious content by bifurcating it from the non-malicious data of patients by performing the multi-label classification. In instances where the data is deemed malicious, the proposed DL-powered scheme further distinguishes itself by performing a granular analysis to pinpoint the sensor source of the threat to avail the secure data to the healthcare system remotely. Additionally, we have extensively evaluated the proposed scheme, comparing accuracy and loss curves using different optimizers and a confusion matrix. In the future, we aim to further enhance the accuracy of the proposed scheme by integrating advanced AI optimization algorithms, reinforcing the model's effectiveness in safeguarding against data threats.

References

[1] S. Subramoniam and M. Saifullah, "Healthcare 2.0," *IT Professional*, vol. 12, pp. 46 – 51, 01 2011.

[2] "Healthcare 3.0." https://www.forbes.com/sites/forbestechcouncil/2022/06/01/a-vision-of-healthcare-30/?sh=78c7dbeb1015. Accessed: 25 July, 2023.

[3] J. Li and P. Carayon, "Health care 4.0: A vision for smart and connected health care," *IISE Transactions on Healthcare Systems Engineering*, vol. 11, pp. 1–14, 02 2021.

[4] J. R. Paragas, "An enhanced cryptographic algorithm in securing healthcare medical records," in *2020 Third International Conference on Vocational Education and Electrical Engineering (ICVEE)*, pp. 1–6, 2020.

[5] A. Saxena, D. MISRA, R. Ganesamoorthy, J. L. Arias Gonzales, H. A. Almashaqbeh, and V. Tripathi, "Artificial intelligence wireless network data security system for medical records using cryptography management," in *2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, pp. 2555–2559, 2022.

[6] A. I. Newaz, A. K. Sikder, M. A. Rahman, and A. S. Uluagac, "Healthguard: A machine learning-based security framework for smart healthcare systems," in *2019 Sixth International Conference on Social Networks Analysis, Management and Security (SNAMS)*, pp. 389–396, 2019.

[7] P. Kaur, M. Sharma, and M. Mittal, "Big data and machine learning based secure healthcare framework," *Procedia Computer Science*, vol. 132, pp. 1049–1059, 2018. International Conference on Computational Intelligence and Data Science.

[8] A. Qayyum, J. Qadir, M. Bilal, and A. Al-Fuqaha, "Secure and robust machine learning for healthcare: A survey," *IEEE Reviews in Biomedical Engineering*, vol. 14, pp. 156–180, 2021.

[9] F. Hussain, S. G. Abbas, G. A. Shah, I. M. Pires, U. U. Fayyaz, F. Shahzad, N. M. Garcia, and E. Zdravevski, "Iot healthcare security dataset," 2021.