سامانه‌های پردازشی و ارتباطی چندرسانه‌ای هوشمند
Intelligent Multimedia Processing and Communication Systems (IMPCS)

Winter 2024, 5 (4), 1-13
DOR:

Received: 5 Oct 2024
Accepted: 16 Nov 2024

مقاله پژوهشی

Intrusion Detection Using Deep Learning in Wireless Body Area Networks

Navid Asadi[1], Elham Hajian[2*]

1. MSc. Student, Department of Computer Engineering, Univeristy of Bojnord, Bojnord, Iran. navidasadi100@gmail.com
2. Assistant Professor, Department of Computer Engineering, Univeristy of Bojnord, Bojnord, Iran. **Corresponding Author*, e.hajian@ub.ac.ir

Abstract

The widespread use of information technology and computer networks has led to the emergence of numerous attacks, the main purpose of which is to compromise the security of networks and databases. Wireless body sensor networks, which are a new technology for tracking patient status, are no exception. These networks are of particular importance due to their sensitive medical applications. Any attack and intrusion into these networks will cause irreparable damage to the patient. For this purpose, intrusion detection systems can be used as a security supplement in body sensor network communications. Since common destructive techniques are increasing randomly, traditional methods are unable to respond to attacks. In addition to identifying attacks, the tasks of intrusion detection systems in body sensor networks include learning the behavioral pattern of attacks in the system. One of the challenging issues in these systems is accuracy. New methods have been developed to improve the correct detection rate and minimize the false detection rate, which increases the efficiency of the system by improving the accuracy. In this study, the accuracy increase is done using multilayer perceptron networks, which is one of the deep learning methods. By increasing the number of hidden layers, more efficient learning is done in these networks. The WBAN RSSI dataset, which is taken from Kaggle, is examined in 3 different classes: normal, type 1 attack, and type 2 attack. Then, the proposed algorithm is plotted for precision, accuracy, recall, and F1 score using the dataset alone and in 3 different classes, which shows an accuracy of 0.72.

Introduction: This paper examines intrusion detection in wireless body area networks. A wireless body area network is a network that sends a lot of clinical data remotely to a server for further processing and then to the doctor for further review. Intrusion due to data diversion in a medical system can have dangerous consequences. Therefore, a mechanism is needed to detect and prevent it.

Method: Intrusion detection in this research has been done using deep learning. By increasing the number of hidden layers in the neural network, data processing and learning are increased and they give more accurate results. Each layer has an activation function. The output layer has 3 classes, which are related to the normal class and types of attacks. The most likely class related to these classes is the prediction of this method for the input data, which attacks this data is most exposed to.

Results: Given the data set considered for testing, there are 3 different classes with different precisions. Class 0(normal data) has the highest precision. Class 0 also has the highest F1 score, indicating good performance in detecting normal data. Class 1 has lower recall, meaning it has difficulty identifying some examples of this class. Class 2 has good recall and lower precisions, indicating some false positives in this class.

Discussion: Other improvements were also made to the model in this regard. These improvements include Hyperparameter tuning: can be tested with different learning rates, batch sizes, and optimal number of epochs. Class balance: handling unbalanced datasets can improve recall of minority classes. Advanced architectures: can be tested and researched using recurrent neural networks or convolutional neural networks to improve model performance.

Keywords: Deep Learning, Intrusion Detection, Cyber Attacks, Wireless Body Area Networks, Precision, Accuracy.

سامانه‌های پردازشی و ارتباطی چندرسانه‌ای هوشمند
Intelligent Multimedia Processing and Communication Systems (IMPCS)
انجمن علمی تجارت الکترونیکی ایران
واحد نجف‌آباد

تشخیص نفوذ با استفاده از یادگیری عمیق در شبکه‌های حسگر بی‌سیم بدنی

تاریخ دریافت: ۱۴/ ۰۷/ ۱۴۰۳
تاریخ پذیرش: ۲۶/ ۰۸/ ۱۴۰۳

دورهٔ پنجم، زمستان ۱۴۰۳
شمارهٔ چهارم، صص: ۱-۱۳

نوید اسدی [۱]، الهام حاجیان [۲*]

۱. دانشجوی کارشناسی ارشد، دانشکده فنی و مهندسی، دانشگاه بجنورد، بجنورد، ایران. navidasadi100@gmail.com
۲. استادیار گروه مهندسی کامپیوتر، دانشکده فنی و مهندسی، دانشگاه بجنورد، بجنورد، ایران. (نویسندهٔ مسئول) E.Hajian@ub.ac.ir

چکیده: فراگیری استفاده از فناوری اطلاعات و شبکه‌های کامپیوتری باعث بروز حملات متعددی شده‌است که هدف عمده این حملات، به‌خطرانداختن امنیت شبکه و پایگاه داده‌هاست. شبکه‌های حسگر بی‌سیم بدنی که نوعی از فناوری جدید برای پیگیری وضعیت بیمارند، نیز از این امر مستثنی نیستند. این شبکه‌ها به‌دلیل کاربردهای حساس پزشکی از اهمیت ویژه‌ای برخوردارند. هر گونه حمله و نفوذ به این شبکه‌ها خسارات جبران‌ناپذیری را برای بیمار به همراه دارد. به همین منظور می‌توان از سیستم‌های تشخیص نفوذ به عنوان مکمل امنیت در ارتباطات شبکه‌ای حسگر بدن، بهره‌برد. از آنجا که تکنیک‌های متداول مخرب به‌طور تصادفی در حال افزایش است، روش‌های سنتی قادر به جوابگویی در برابر حملات نیست. از وظائف سیستم‌های تشخیص نفوذ در شبکه‌های حسگر بدن، علاوه بر شناسایی حملات، یادگیری الگوی رفتاری حمله در سیستم است. یکی از موضوعات پرچالش در این سیستم‌ها، دقت می‌باشد. روش‌های جدیدی به منظور بهبود نرخ تشخیص درست و به حداقل رساندن نرخ تشخیص اشتباه ابداع‌شده‌اند که با بهبود هرچه بیشتر دقت، کارایی سیستم افزایش می‌دهند. در این پژوهش، افزایش دقت با استفاده از شبکه‌های پرسپترون چندلایه که یکی از روش‌های یادگیری عمیق می‌باشد، انجام-شده‌است. با افزایش تعداد لایه‌های پنهان، یادگیری کارآمدتر در این شبکه‌ها انجام‌می‌شود. مجموعه داده WBAN rssi که از Kaggle گرفته‌شده‌است، در ۳ کلاس مختلف نرمال، حملهٔ نوع ۱ و حملهٔ نوع ۲ بررسی‌می‌شود. سپس نمودار الگوریتم پیشنهادی برای دقت، درستی و فراخوانی و امتیاز F1 با استفاده از مجموعهٔ داده به‌تنهایی و در ۳ کلاس مختلف ترسیم‌شده‌است که نشان از دقت ۰,۷۲ دارد.

واژه‌های کلیدی: یادگیری عمیق، تشخیص نفوذ، حملات سایبری، شبکهٔ حسگر بی‌سیم بدنی، دقت، صحت.

۱. مقدمه

شبکهٔ حسگر بی‌سیم بدنی[1] یکی از تکنیک‌ها و فناوری‌های مهم در زمینهٔ پزشکی می‌باشد که به منظور حمایت از برنامه‌های کاربردی حوزهٔ سلامت برروی تلفن همراه نصب‌می‌شود. این شبکه‌ها مجموعه‌ای از تعداد معینی حسگر درون یا روی بدن انسان است که سیگنال‌های زیستی انسان مانند: درجهٔ حرارت، فشارخون، الکتروکاردیوگرافی را از طریق حسگرهای متصل به بدن انسان دریافت و به یک مرکز پزشکی برای بررسی اطلاعات ارسال‌می‌کنند. استفاده از حسگر بی سیم بدنی، موجب استفادهٔ بهینه از منابع بیمارستانی و تشخیص زودهنگام علائم پزشکی و در نهایت کاهش هزینه‌های مراقبت پزشکی شده‌است. ازآنجاکه در شبکه‌های حسگر بی‌سیم ارسال داده از طریق همه‌پخشی انجام‌می شود، هرگونه حملهٔ سایبری مانند استراق سمع، تغییر داده، جلوگیری از سرویس قابل‌انجام است و موجب تشخیص و درمان اشتباه می‌شود. تهدیدات امنیتی در شبکه‌های حسگر بدنی می‌توانند بر یکپارچگی شبکه از طریق تخریب مسیرها و ساختار گره‌ها تأثیر بگذارند، فرآیندهای مسیریابی را تغییردهند، تغییراتی غیرقانونی در شبکه انجام‌دهند یا داده‌های تحریف شده بسازند. تمامی موارد نام‌برده می‌توانند به‌راحتی از طریق پیاده‌سازی حملات روی این نوع از شبکه‌ها به تجهیزات نظارتی در بدن انسان، القاء شود و تأثیر سوء داشته‌باشد. استقرار شبکه‌های حسگر در بدن انسان، بدون هیچ مراقبتی و عدم تضمین امنیت فیزیکی گره‌های حسگر، این شرایط را تشدید می‌کند. بنابراین نیاز به استفاده از الگوریتم‌های امنیتی در این شبکه‌ها احساس می‌شود[۱].

به‌دلیل محدودیت انرژی، حافظه و پردازش گره‌ها، امکان استفاده از روش‌های سنتی تأمین امنیت مانند رمزنگاری و پروتکل‌های امن با مشکلاتی همراه است؛ بنابراین بهتر است، از سامانه‌های تشخیص نفوذ استفاده‌کرد.

تشخیص نفوذ یک پایش هوشمندانه در شبکه بر روی تمامی سامانه‌های کامپیوتری برای یافتن هرگونه خطای امنیتی است. این تکنولوژی یکی از شیوه‌های تدافعی در برابر حملات است که در حقیقت بعد از سیستم‌های پیش‌گیری از نفوذ به عنوان دومین خط دفاعی در برابر مهاجمان بوده و وظیفه آن شنا سایی و گزارش حملات است. یکی از مزایای سیستم‌های تشخیص نفوذ در مقابل روش‌های امنیتی دیگر، پوشش طیف وسیعی از حملات در شبکه‌های حسگر و به‌تبع آن حسگر بدنی است. محققان سیستم‌های تشخیص نفوذ مختلفی را برای شبکه های حسگر ارائه‌کرده‌اند اما با توجه به محدودیت‌های موجود در شبکه‌های حسگر بی سیم، طراحی سیستم تشخیص نفوذ مؤثر و کارا که قابل‌استفاده در حسگر بدنی باشد، هنوز یک چالش بزرگ است[۲].

هدف این پژوهش بررسی دقت سیستم تشخیص نفوذ در شبکه‌های حسگر بدنی است که با استفاده از یادگیری عمیق انجام‌می شود. این سامانه پیشنهادی با هدف شنا سایی حملات و افزایش نرخ تشخیص، نخست داده های جمع آوری‌شده را تحلیل‌می‌کند و در جریان آماده‌سازی قرارمی‌دهد. با استفاده از الگوریتم یادگیری عمیق، ویژگی‌هایی از ترافیک شبکه استخراج‌می شود که موجب بالا رفتن نرخ تشخیص نفوذ می‌شوند. سپس معماری چندلایه بر اساس شبکهٔ عصبی با تعریف تعداد لایه ها، تعداد نرون ها در هر لایه و پارامترهای آن ها تنظیم می‌شود. سپس مدل بر روی داده های آموزشی، آموزش داده‌می شوند. الگوریتم Adam برای بهینه سازی وزن‌های شبکه عصبی استفاده می‌شود. در نهایت عملکرد الگوریتم بر روی داده‌های تست برای اندازه‌گیری دقت، ارزیابی‌می‌گردد. خلاصهٔ نوآوری این مقاله عبارت‌است از ارائه روشی مبتنی بر یادگیری عمیق برای انتخاب بهترین ویژگی‌ها از میان داده‌های جمع آوری‌شده به منظور بالا بردن نرخ تشخیص نفوذ در ترافیک شبکهٔ حسگر بی‌سیم بدنی.

۲. تاریخچه

محمد عثمان و همکاران[۳] شبکه‌های حسگر بی سیم بدنی را از زاویهٔ انتقال داده بررسی‌کرده‌اند. ایشان انتقال داده را در این شبکه به چهاربخش (۱) جمع‌آوری داده توسط حسگر (۲) انتقال به گره چاهک (۳) انتقال به دروازهٔ اینترنت و (۴) انتقال به پزشک، تقسیم‌کرده‌اند و سپس به بررسی تهدیدهای امنیّتی هر بخش پرداخته‌اند. ازآنجاکه حسگرهای قرارگرفته بر روی بدن بیمارممکن است از دقّت کافی در اندازه‌گیری برخوردار نبا شند، ضروری است تا مقادیر اندازه‌گیری شده توسط حسگرها بررسی شوند. هرگونه مقدار اندازه‌گیری شدهٔ اشتباه می‌تواند منجر به ایجاد یک هشدار اشتباه برای بیمار و پزشک شود.

عثمان سالم و همکاران[4] به منظور جداسازی بین مقادیر اندازه‌گیری شده درست و اشتباه ازفیلتر کالمن استفاده‌کرده‌اند. ایشان از فیلتر کالمن برای پیش‌بینی مقدار اندازه‌گیری‌شده توسط حسگر استفاده‌می‌کنند. با محاسبهٔ مقدار همگرایی بین این دو مقدار و پایش دیگر جنبه‌های سلامتی بیمار، می‌توانند مقادیر اندازه‌گیری شدهٔ اشتباه را شناسایی‌کنند.

جی ها[5] با افزودن یک دستگاه خارجی به شبکهٔ حسگر بی سیم بدن، به نامMEDMON امنیّت آن را تأمین‌کرده‌است. این دستگاه برای هردو مرحلهٔ دادهٔ آزمایشی و دادهٔ واقعی در نزدیک محل شبکهٔ حسگر بی‌سیم قرارگرفته و برای بیمارهای مختلف آموزش می‌بینند. بدین ترتیب می‌تواند میان ویژگی‌های رفتاری شبکه‌های حسگر بی‌سیم بدن اولویت‌بندی‌کرده و رفتارعادی و ناهنجار را طبقه‌بندی کند.MEDMON برای تشخیص ناهنجاری، سیگنال‌های موجود در شبکهٔ حسگر بی سیم، بدن را نظارت‌کرده و بعد ازتحلیل آن‌ها تشخیص‌می‌دهد که ترافیک موجود، مربوط به یک ترافیک عادی است یا به یک ترافیک ناهنجار تعلق دارد.

در [۶] سیستم مراقبت بهداشتی مبتنی بر ابر توسط رانی و همکاران پیشنهادشده‌است که در آن داده‌ها فقط توسط کاربران مجاز قابل‌دسترس است. این سیستم از روش ماشین بردار پشتیبان[2] برای پیش‌بینی شرایط بیماران و بیماری های مورد انتظار و همچنین از

داده‌کاوی برای یادگیری ماشین استفاده‌می‌کند. یادگیری ماشین در کشف حملات به داده‌ها نقشی ندارد.

علابدلطیف و همکاران سیستمی را پیاده سازی‌کرده‌اند که تغییرات زمان را تشخیص‌داده و ناهنجاری را در چند علائم حیاتی بدن بیمار پیش‌بینی‌می‌کند[۷]. سیستم از سه بلوک تشکیل‌شده‌است، جمع‌آوری و تجمیع داده‌ها، ارسال به ابر و ذخیره‌سازی داده به فرمت رمزگذاری شده. آخرین بلاک از مدل‌های ریاضی بدون رمزگشایی استفاده‌می‌کند که تغییرات ناهنجاری و در نتیجه حملات را تشخیص‌می‌دهد.

در [8] کارتا و همکاران، یک تکنیک مهندسی ویژگی برای تشخیص کارآمد ناهنجاری‌ها و بهبود عملکرد سیستم‌های تشخیص نفوذ سنتی معرفی‌کرده‌است.

الزهرانی و همکاران در [۹] اگرچه ناشناس بودن، غیرقابل‌ردیابی و محافظت در برابر حملهٔ داخلی ممتاز را انجام‌داده‌اند ولی به‌دلیل محاسبات و پارامترهای سنگین از گره سطح اول که باعث‌می‌شود مهاجم مقادیر پارامترهای جعلی را در طول ارتباط ارسال‌کند، در برابر حمله انکار سرویس[۳] آسیب‌پذیر است.

همچنین اودلو و همکاران[10] یک پروتکل احراز هویت سبک‌وزن برای شبکه‌های حسگر بی‌سیم بدنی براساس جفت‌شدن دوخطی برای غلبه بر مشکلات حریم خصوصی و مدیریت تعداد زیاد کلید عمومی پیشنهاد کرده‌است. طرح آن‌ها دارای دو مشتری ارتباطی با حسگر و مدیر شبکه است که آن را در برابر حمله انکار سرویس ایمن‌می‌کند اما زمان محاسبات و پیچیدگی بالایی دارد.

در [۱۱] توسط تانگاراسو سیستم جلوگیری از نفوذ ارائه‌شده‌است که منجر به کاهش معنادار تعداد حملات سیستم شبکهٔ بدنی بی‌سیم می‌شود. در این پژوهش از شبکهٔ عصبی متراکم استفاده شده که داده یادگیری‌اش را از چندین مجموعهٔ داده به‌دست‌می‌آورد. در این پژوهش از طریق استفاده از پایگاه داده انکار سرویس توزیع‌شده به عنوان تست مدل آموزش دیده می‌تواند حملات را شناسایی‌کند. استفاده از شبکهٔ عصبی متراکم در این پژوهش، بهبود قابل‌توجه نرخ تشخیص و پیشگیری را در مقایسه با مدل‌های دیگر یادگیری عمیق در شبیه‌سازی نشان‌می‌دهد.

شاکر در [۱۲] با استفاده از یادگیری عمیق، طبقه‌بندی قابل‌اعتماد و غیرقابل‌اعتماد انجام‌می‌دهد. سپس برای حذف درایه‌های تکراری از دادهٔ ورودی از Z-SCORE استفاده و در ادامه برای گرفتن ویژگی‌های داده نرمال از آنالیز تشخیص خطی استفاده می‌کند. در ادامه عملکرد روش پیشنهادی با رویکردهای فعلی دیگر مقایسه‌شده‌است که نشان از برتری این روش در دقت و تأخیر می‌باشد.

در [13] توسط لیا برای انجام مسیریابی درست و انتخاب بهینهٔ سرخوشه از الگوریتم ازدحام مرغ ماهی‌خوار و پیرانای قرمز[۴] استفاده‌می شود. زمانی‌که سرخوشه به صورت بهینه انتخاب‌می‌گردد، مسیریابی بهینه با الگوریتم RPESA اجرامی‌شود. سپس داده‌های ارسالی با استفاده از این طرح برای تشخیص بیماری به یک شبکهٔ عصبی بازگشتی آبشاری گشاده‌شده[۵] فرستاده‌می شود. پارامترها با استفاده از RPESA به‌صورت بهینه در الگوریتم شبکه عصبی بازگشتی آبشاری بهینه انتخاب‌می‌شوند و خروجی بیماری طبقه‌بندی‌شده از الگوریتم به‌دست‌می‌آید. رویکرد مسیریابی انرژی کارآمد مبتنی بر رویکرد تعاملی پیاده‌سازی‌می‌شود.

آرتی در [۱۴] از شبکه نرم‌افزار محور برای داشتن چارچوبی امن در اکوسیستم بهداشتی اینترنت اشیاء و ترکیب یادگیری عمیق و یادگیری ماشین برای شناسایی حملات شبکه در داده حسگرهای بهداشتی استفاده‌کرده‌است. همچنین به‌صورت کارا بر وسایل متصل‌شده و رفتارهای ناخواسته نظارت‌می‌کنند.

در [۱۵] توسط آیوندی سیستم تشخیص نفوذ جدید برای رویارویی با افزایش حملات امنیتی وب در سیستم مراقبتی و بهداشتی پیاده‌سازی شده‌است. این پژوهش برای جلوگیری از محدودیت‌های این سیستم در پاسخ به حملات و چالش‌های آن، یادگیری ماشین را با جنگل تصادفی و الگوریتم ژنتیک ترکیب‌کرده و توسط آن‌ها یک روش بهینه‌سازی برای سیستم تشخیص نفوذ ارائه‌شده‌است که نرخ تشخیص بالا و اطلاعات درست می‌دهد. برای بهینه‌سازی دید، الگوریتم ژنتیک وزن‌دار و جنگل تصادفی ترکیب‌شده استفاده‌می‌شود که بهترین زیرمجموعه را برای رسیدن به نرخ کشف بالا تولیدمی‌کند. برای این هدف از طبقه بندی رگرسیون لجستیک برای یادگیری ماشین استفاده‌می‌نماید. نتایج حاکی از آن است که در پارامترهای دقت و نرخ تشخیص و F1 ، تابع بهینه سازی به‌خوبی عمل‌کرده‌است. ترکیب الگوریتم ژنتیک و جنگل تصادفی به نرخ تشخیص ۹۸,۸ ٪ و نرخ پیش‌بینی غلط ۰,۸ ٪ می‌رسد.

آشیش در [۱۶] سیستم فیزیکی سایبری[۶] پزشکی ارائه کرده که از حسگرهایی با هزینه کم برای تشخیص زمان واقعی، نظارت و تصمیم‌گیری تشکیل‌شده‌است. داده‌های حساس MCPS توسط شخص سوم قابل‌اعتماد پردازش می‌شوند. بنابراین انتقال داده از مالک به شخص سوم در معرض آسیب‌پذیری از فعالیت‌های مخرب قرارمی‌گیرد. همچنین می‌توان حملات از درون شبکه را به‌راحتی انجام‌داد و اطلاعات محرمانه بیمار را به بیرون منتقل‌کرد. برای غلبه بر چنین مشکلاتی، MCPS سیستم تشخیص نفوذ برای شناسایی فعالیت‌های مخرب و نظارت بر ترافیک شبکه در زمان واقعی نیاز دارد. این پژوهش سیستم تشخیص نفوذ را بر اساس اعتماد رفتاری دستگاه پزشکی هوشمند[۷]، مانند تلفن هوشمند پزشکی[۸]، پیشنهادمی‌کند. میزان اعتماد SMD/MSP را می‌توان با استفاده از پارامترهای رفتاری مختلف با مدل شهرت بتا ارزیابی‌کرد. مجموعه‌ای از قوانین تصمیم‌گیری براساس درجهٔ اعتماد محاسبه‌شده به صورت پویا برای بررسی سطح نفوذ گره و فرآیند تولید هشدار پیشنهاد شده‌است. عملکرد مدل پیشنهادی دقت ۹۳,۹ ٪ را نشان‌می‌دهد.

نوروزی در [۱۷] برای افزایش کارایی سیستم تشخیص نفوذ در شبکه‌هایی کامپیوتری از روش ترکیبی شبکه‌های عصبی عمیق استفاده

کرده اســت. با اســتفاده از روش‌های ترکیبی، شــامل ترکیب معماری شــبکه‌های عصــبی، ویژگی‌ها، خروجی‌ها و ترکیب نتایج از شــبکه‌های عصبی مختلف، تنوع و قدرت تشخیص مدل افزایش‌می‌یابد و درستی و عملکرد آن بهبودمی‌یابد.

در [۱۸] توســط کامل، به‌دلیل باز بودن محیط اینترنت اشــیا و آسیب‌پذیر بودن وسایل، روشی برای تشخیص نفوذ ارائه‌کرده‌است. ارائه سیستم تشخیص نفود دو لایهٔ مبتنی بر طبقه‌بند KNN برای جداسازی ترافیک عادی از حمله و شــبکه مصــنوعی پرســپترون چند لایه برای تشخیص نوع حمله استفاده شده‌است. سپس دقت، صحت و فراخوانی بررسی شده‌است. جدول ۱ خلاصه‌ای از مطالعات پیشین را براساس نحوه تشخیص نفود نشان‌می‌دهد.

جدول ۱: خلاصه‌ای از مطالعات پیشین

مراجع	نحوه تشخیص نفوذ				مزایا	معایب
	داده	انتقال داده		احراز هویت		
		ترافیک	مسیریابی			
[۳]		*			امنیت	ارتباطات زیاد
[۴]	*				تشخیص ناهنجاری	محاسبات زیاد
[۵]		*			امنیت ارتباطات	سخت‌افزار اضافه
[۶]				*	معماری جدید	سخت‌افزار اضافه
[۷]		*			رمزنگاری	سرباراضافه
[۸]		*			کاهش الگوها	افزایش تأخیر
[۹]	*				زمان محاسبات کم	مقایسه با یک روش
[۱۰]				*	کاهش تعداد کلیدهای عمومی	فقط احراز هویت
[۱۱]		*			کاهش تعداد حملات	نداشتن راه‌حل برای حملات
[۱۲]	*				تشخیص گره‌های تحت حمله	نداشتن راه‌حل حمله
[۱۳]			*		مسیریابی بهینه	نداشتن راه‌حل برای حمله
[۱۴]		*			تشخیص رفتار نادرست گره	جدا نکردن حسگرهای مخرب
[۱۵]		*			کاهش نرخ داده-های غلط	تشخیص ندادن حمله
[۱۶]			*		تشخیص ناهنجاری	نداشتن راه‌حل برای ناهنجاری
[۱۷]	*				تشخیص الگوهای ناهنجار	عدم جلوگیری از حمله
[۱۸]		*			تشخیص حمله	عدم جلوگیری از حمله

۳. مقدمات الگوریتم پیشنهادی

در زیر الگوریتم پیشنهادی با جزئیات شرح‌داده‌می‌شود.

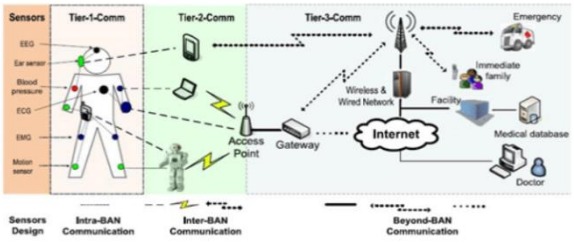
۱،۳ معماری الگوریتم پیشنهادی

با توجه به عملکرد متفاوت شــبکه‌های حســگر بی‌ســیم بدنی، هر گره می‌تواند نسبت به وظایفش از اجزای متنوعی تشکیل شده‌باشد ولی در حالت کلی هر گره متشکل است از: واحد پردازش مرکزی، فرستنده – گیرنده رادیویی، منبع تغذیه که می‌تواند از طریق باطری یا ســلول‌های خورشیدی یا ترکیب هر دو، انرژی موردنیاز سیستم را فراهم‌کند، یک یا تعدادی حســگر که داده‌های موردنظر را جمع‌آوری‌می‌کنند، انواع حافظه‌های جانبی در صــورت نیاز، ســیســتم موقعیت‌یاب جهانی[۹] در صورت نیاز و سایر اجزایی که بسته به کاربردهای متفاوت می‌تواند در هر گره گنجانده‌شود[۱۹].

عواملی چون اقتصادی‌بودن سیستم، قابلیت مورد انتظار، تعداد انبوه گره‌هــا و نهــایتــاً عملی‌شــــدن ایــده‌هــا در محیط واقعی، موجــب محدودیت‌های سخت افزاری در هر گره می‌شود. یک WBAN متشکل از تعدادی گره حســگر و یک هماهنگ‌کننده اســت، هر گره از باتری، حســگر، عملگر، پردازشــگر، حــافظــه و فرســتنــده گیرنــده تشکیل‌شده‌است[۲۰].

معماری شــبکه، ســازمان‌دهی منطقی دســتگاه‌های ارتباطی در یک ســیســتم اســت. در این بخش ســیســتم نظارت بر ســلامتی بیمار که متشکل از سه لایه است، بررسی‌می‌شود.

۱. ارتباطات درون BAN لایهٔ شبکه حسگر
۲. ارتباطات بین‌BAN لایهٔ شبکه محاسبات
۳. ارتباطات فراتر از BAN لایهٔ شبکه نظارت از راه دور



شکل ۱: معماری عمومی سیستم نظارت بر سلامتی

شکل ۱ معماری عمومی از یک سیستم نظارت بر سلامتی مبتنی بر BAN را نشان‌می‌دهد. ECG ، EEG، EMG، حسگرهای حرکتی و حسگرهای فشارخون که داده‌های خود را به دستگاه سرور شخصی[۱۰] ارسال‌می‌کنند. سپس این داده‌ها در شبکه‌های حسگر بی سیم بدنی برای تشخیص بیماری از طریق ارتباط بلوتوث یا شبکهٔ محلی به سایت یک پزشک یا به یک پایگاه دادهٔ پزشکی برای نگهداری سوابق یا به یک سیستم هشداردهنده، فرستاده‌می‌شود. معماری ارتباطات داخل BAN بر اساس ویژگی‌های سیستم در شرایط خاصی انجام‌می شود و این می‌تواند بر روی کارایی سیستم از طرق مختلفی همچون مصرف انرژی، توانایی در رفتار کردن با انواع بارهای ترافیکی، پایداری شبکه، انتخاب پروتکل MAC ، تأخیر انتقال و تداخل کاربران تأثیر بگذارد[۲۱].

۲،۳. حمله در شبکه‌های حسگر بی‌سیم بدنی

حملات متفاوتی در شبکه‌های حسگر بی‌سیم بدنی قابل‌اجرا است. بعضی از این حملات روی شبکه (در لایه‌های مختلف) بعضی دیگر بر روی محرمانگی و درستی اعتبار داده‌ها ممکن است به وقوع بپیوندد. در ادامه به برخی از آن‌ها به اختصار اشاره‌می‌شود[۲۲].

حملهٔ ارسال انتخابی: این حمله شامل گره مهاجمی است که از رسیدن بسته‌ها به دستگاه اصلی جلوگیری‌می‌کند.

حملهٔ تزریق داده کاذب: در این نوع حمله، گره مخرب، داده هایی برخلاف داده‌های حس‌شده توسط حسگر را به دستگاه اصلی ارسال‌می‌کند.

حملهٔ سیبل: در این حمله، گره مهاجم تغییر قیافه داده و به عنوان یکی از مجموعه گره‌های متعدد شبکه معرفی‌می‌شود.

حملهٔ حفره: در این حمله، گره ناهنجار، خود را به عنوان یک گره با منابع زیاد معرفی‌می‌کند تا حسگرهای دیگر بسته‌های خود را از طریق مسیر گره ناهنجار عبوردهند.

حملهٔ استراق سمع: در این حمله گره مهاجم، با استفاده از یک آنتن قوی، می‌تواند به داده‌های ارسالی از دیگر گره‌های حسگر بی سیم بدن گوش داده و بدین ترتیب، تمامی داده‌ها را سرقت‌کند.

حملهٔ زمان‌بندی: این حمله هنگام تنظیم زمان‌بندی پروتکل ارتباطی انجام‌می‌شود. برای مثال، در پروتکل تقسیم زمانی گره مخرب، زمان ارسال بسته را برای تمامی گره‌ها یکسان قرارمی‌دهد. بدین ترتیب بسته‌های ارسالی به‌علت تصادم از بین خواهندرفت.

حملهٔ جلوگیری از سرویس: این حمله عبارت از انواع تلاش‌هایی است که یک گره مهاجم انجام‌می‌دهد تا یک گره دیگر نتواند خدماتی به سایر گره‌ها ارائه‌دهد.

در شبکه‌های حسگر بی‌سیم بدن از سه نوع حملهٔ معروف جلوگیری از سرویس به شرح زیر می‌توان استفاده‌کرد:

حملهٔ حفره سیاه: در این حمله گره مهاجم در آغاز خود را به عنوان چاهک معرفی‌می‌کند. بدین ترتیب گره مهاجم می‌تواند تمامی بسته‌های دریافتی را از بین ببرد.

حملهٔ حفره خاکستری: در این حمله گره مهاجم مانند حملهٔ حفره سیاه خود را به عنوان گره چاهک معرفی‌می‌کند، با این تفاوت که بسته‌های دریافتی را انتخابی و یا تصادفی از بین می‌برد.

حملهٔ سیل‌آسا: در این حمله گره مهاجم بسته‌های اطلاعاتی را به‌صورت سیل‌آسا به سمت گره قربانی ارسال‌می‌کند. دریافت و پردازش بسته‌های سیل‌آسا به‌وسیله گره قربانی علاوه بر آنکه مصرف انرژی گره را افزایش‌می‌دهد، موجب پر شدن بافر ورودی گره شده و امکان دریافت بسته‌های جدید را از بین خواهدبرد.

۳،۳. سیستم تشخیص نفوذ

نفوذ، فعالیتی است که توسط آن محرمانگی، درستی یا دسترسی به منابع دچار اختلال می‌شود. تشخیص نفوذ درواقع شناسایی دستیابی‌های غیرمجاز به حملات انجام‌شده به شبکه است. سامانهٔ تشخیص نفوذ وظیفهٔ نظارت بر فعالیت سامانه، تجزیه و تحلیل بسته‌های شبکه، تعیین الگوی حملات و ارزیابی در ستی و یکپارچگی فایل‌ها را بر عهده دارد. معمولاً سامانه‌های تشخیص نفوذ با ساختار سه سطحی زیر توصیف‌می‌شوند:

•واحد نظارت: وظیفهٔ ثبت رخدادها را بر عهده دارد. رخدادهای سامانه توسط این واحد جهت تشخیص و تحلیل ثبت‌می‌شوند. همچنین نمایش هشدار به مدیر شبکه یا مسئول نظارت و پیگیری رویدادهای شبکه برعهده این واحد است.

•واحد تشخیص و تحلیل: اطلاعات ثبت‌شده توسط واحد نظارت را به عنوان ورودی دریافت‌می‌کند و سپس براساس این اطلاعات به یکی از روش‌های مبتنی‌بر سوءاستفاده یا ناهنجاری، مدل ساخته‌می‌شود. حملات و تهدیدات امنیتی به کمک مدل ساخته‌شده تمایز داده‌می‌شوند.

•واحد هشدار: وظیفه انجام رفتار مناسب با نوع حمله را داراست. این واحد در صورت نیاز اخطارهای مناسب را برای ثبت یا نمایش به واحد نظارت ارسال‌می‌کند.

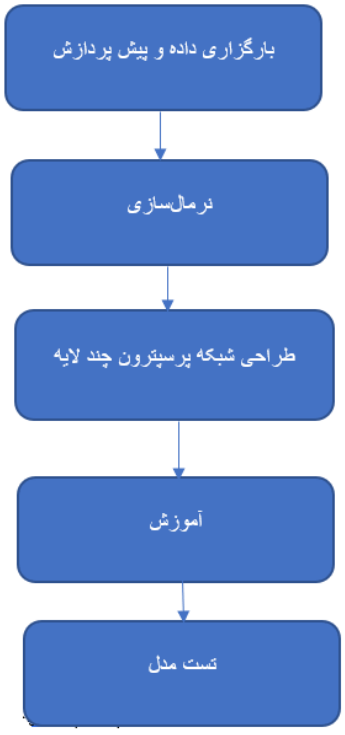
۴. الگوریتم پیشنهادی

افزایش دقت برای تشخیص حملات مختلف در شبکهٔ حسگر بدنی بسیار مهم می‌باشد. تحقیقات زیادی در این زمینه صورت‌گرفته‌است. یکی از این روش‌ها، استفاده از سیستم‌های شبکهٔ پرسپترون چندلایه - از روش‌های یادگیری عمیق- می‌باشد که برای حل چالش دقت ارائه‌شده‌است. افزایش تعداد لایه‌های پنهان کارایی شبکه را بهبودمی‌دهد. افزایش لایه‌ها و عمیق‌کردن شبکه، ویژگی‌ها و خروجی شبکه را به واقعیت بیشتر نزدیک می‌کند ولی بار محاسباتی را نیز

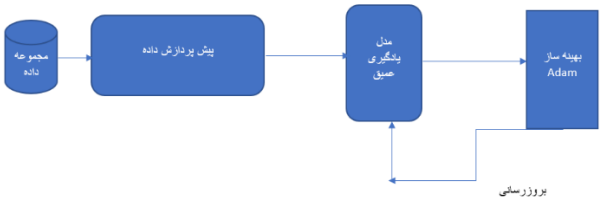
افزایش‌می‌دهد. بنابراین انتخاب تعداد لایه‌ها بسیار مهم است. یکی از الگوریتم‌های مشهور در بهینه‌سازی وزن‌ها در لایه‌ها روش گرادیان کاهشی است. تابع فعالساز جزء اصلی شبکهٔ عصبی می‌باشد. این تابع مشخص‌می‌کند که گره فعال است یا خیر. یکی از توابع فعالساز پرکاربرد، RELU[11] می‌باشد. با توجه به اهمیت ویژگی‌ها و نتایج به‌دست‌آمده، ممکن است گرهی فعال یا غیرفعال گردد. این تابع به‌دلیل دارا بودن ویژگی خطی، همگرایی الگوریتم گرادیان کاهشی را سریع‌تر می‌کند.

۱،۴. فلوچارت الگوریتم پیشنهادی

در الگوریتم پیشنهادی برای تجزیه و تحلیل بهتر داده در جهت بهبود دقت در سیستم‌های تشخیص نفوذ از PANDAS استفاده‌می‌شود. PANDAS کتابخانه‌ای برای پردازش و تحلیل داده‌ها در زبان پایتون است. با این ابزار می‌توان داده‌ها را بارگزاری، پاکسازی، تبدیل و تحلیل کرد. سپس با طراحی شبکه‌های عصبی پرسپترون چندلایه از الگوریتم ADAM[12] جهت بهینه‌سازی وزن‌ها و تابع فعالساز RELU استفاده‌شده‌است. در فاز اول، پیش پردازش و تحلیل با PANDAS انجام‌می‌شود. در فاز دوم نرمال‌سازی داده انجام‌شده در فاز سوم، شبکه‌های پرسپترون چندلایه جهت تشخیص حملات از داده‌های نرمال استفاده‌می‌شود. در فاز چهارم مدل ساخته‌شده با داده‌های آزمایشی جهت بررسی عملکرد دقت در الگوریتم پیشنهادی اجرامی‌شود تا میزان دقت بررسی‌شود. شکل ۲، این فلوچارت را نشان‌می‌دهد. مدل الگوریتم پیشنهادی نیز در شکل ۳، آمده‌است.



شکل ۲: فلوچارت الگوریتم پیشنهادی



شکل ۳: مدل سیستم الگوریتم پیشنهادی

۲،۴. جزئیات الگوریتم پیشنهادی

- **بارگذاری داده‌ها و پیش‌پردازش**

در ابتدا، مجموعه داده‌های WBAN rssi که از kaggle گرفته شده‌است، با استفاده از PANDAS بارگذاری‌می‌شود. مجموعهٔ داده شامل چندین ویژگی است که هر نمونه به عنوان معمولی یا یک نوع حمله برچسب‌گذاری شده‌است.

- **نرمال‌سازی**

یکی از مراحل کلیدی پیش پردازش که اجرا شده است، نرمال‌سازی داده‌ها است. با استفاده از MinMaxScaler از کتابخانه sklearn.preprocessing، همه ویژگی‌ها در محدوده ۰ تا ۱ مقیاس شده است. این مرحله در یادگیری عمیق بسیار مهم است زیرا از ایجاد مشکل تفاوت های بزرگ در هنگام آموزش در مقادیر ویژگی ها جلوگیری می‌کند. شبه‌کد زیر در مورد نرمال‌سازی می‌باشد.

```
from sklearn.preprocessing import MinMaxScaler
scaler = MinMaxScaler()
X_train_scaled = scaler.fit_transform(X_train)
X_test_scaled = scaler.transform(X_test)
```

نرمال سازی تضمین‌می‌کند که همه ویژگی‌ها به‌طور یکسان در فرآیند آموزش مدل نقش دارند و توانایی مدل را برای همگرایی مؤثر بهبود می‌بخشد.

- **معماری مدل**

برای مدل یادگیری عمیق، از Keras با API متوالی برای ساختن یک شبکهٔ عصبی ساده و پیش‌خور استفاده‌شده‌است.

برای داده های ورودی و پردازش آن ها از شبکهٔ عصبی عمیق استفاده شده است. این شبکه دارای ۳ لایهٔ پنهان می‌باشد. به منظور پردازش هر لایه باید از تابع فعالساز استفاده‌شود.

تابع فعالساز از جمله ابرپارامترهایی است که باید قبل از آموزش شبکه مشخص شود. این توابع در تمام لایه‌های شبکه باید تعریف شود. برای انتخاب توابع فعالساز پروسپترون چندلایه نمی‌توان از هر تابعی استفاده‌کرد بلکه باید حتماً ماهیت مشتق‌پذیری، پیوسته، یک نوا نزولی را داشته‌باشد و همچنین مشتق اول آن به‌راحتی قابل‌محاسبه باشد. این لایه‌ها در ادامه بیان‌می‌شود.

لایهٔ ورودی

لایهٔ ورودی ویژگی‌ها را دریافت‌می‌کند. فرض‌شده‌است که مجموعهٔ داده دارای ۱۰ ویژگی است. بنابراین لایهٔ ورودی به گونه‌ای پیکربندی‌شده‌است که بردارهایی با این اندازه را انتظار داشته‌باشد.

لایه‌های پنهان

شـــبکه دارای ســـه لایهٔ مخفی اســـت و هر کدام به گونه‌ای پیکربندی شده‌اند که از خروجی لایهٔ قبلی یادبگیرند.

لایه ۱: یک لایهٔ کاملاً متصل با ۶۴ واحد نرون استفاده‌شده‌است که فعالســاز ReLU نیز اضــافه‌شــده‌اســت. این لایه الگوهای اســاســی را از داده‌های ورودی می‌گیرد.

لایه ۲: دومین لایهٔ مخفی دارای ۳۲ واحد نرون استفاده‌شده‌است که فعالســاز ReLU نیز اضــافه‌شــده‌اســت. این لایه بر روی بازنمایی‌های آموخته‌شـــده در لایهٔ اول اســـتوار اســـت و الگوهای پیچیده‌تری را استخراج‌می‌کند.

لایه ۳: لایه پنهان ســوم دارای ۱۶ واحد نرون اســتفاده‌شــده‌اســت و شـــامل فعالســـاز ReLU اســـت. این لایه نمایش‌های آموخته‌شـــده را اصلاح‌می‌کند و آن‌ها را برای لایهٔ خروجی آماده‌می‌کند.

ReLU (واحد خطی اصــلاح‌شــده) یک تابع فعالســاز متداول اســت که غیرخطی بودن را به مدل معرفی‌می‌کند و با اجتناب از م شکل گرادیان ناپدیدشدن به همگرایی سریعتر کمک‌می‌کند.

این تابع در صـــورتی که ورودی کمتر از ۰ باشـــد، تابع فعالســـازی ReLUصفر (۰) و در غیر این صورت مقدار خام را خروجی می‌دهد. به عبارت دیگر، اگر مقدار ورودی بیشـــتر از ۰ باشـــد، تابع ReLU همان مقدار ورودی را خروجی می‌دهد. عملکرد تابع فعالســـازی ReLU از جهات بسیاری مشابه عملکرد نرون‌های زیستی ما است. معادله (۱) این تابع فعالساز را نشان‌می‌دهد.

$$F(x)=max(x,0) \qquad (۱)$$

ReLU یک تابع غیرخطی اســت و برخلاف تابع ســیگموید با خطاهای پس‌انتشار مواجه‌نمی‌شود. علاوه بر این، اگر در شبکه‌های عصبی بزرگتر به جای تابع سیگموید از تابع ReLU ا ستفاده شود، سرعت مدل سازی بیشتر خواهدبود، به عبارت دیگر مدت زمان مدل‌سازی کاهش‌می‌یابد.

- ✓ باورپذیری بیولوژیکی: این تابع برخلاف تابع پادتقارن tanh ، یک‌جانبه است.
- ✓ فعال‌ســازی پراکنده: برای مثال، در شــبکه‌ای که به صــورت تصادفی مقداردهی شده‌است، حدود ۵۰ درصد از واحدهای پنهان، فعال‌می‌شوند (و خروجی آن‌ها غیرصفر خواهدبود).
- ✓ انتشـــار بهتر گرادیان: در این تابع برخلاف توابع فعالســـازی سیگموید، مشکل محوشدگی گرادیان کمتری دارد.
- ✓ محاسبات اساسی: در این تابع فقط از مقایسه، جمع و ضرب استفاده‌می‌شود.
- ✓ مقیاس‌پذیر(for a>=0 : max (0, a x) = a max (0 , x

لایهٔ خروجی

لا یهٔ خروجی نهایی با ۳ واحد نرون و یک تابع فعالســـاز softmax پیکربندی شده‌ا ست. هر واحد مربوط به یک کلاس در کار طبقه‌بندی است که هر کلاس یک حمله را نشان‌می‌دهد. تابع softmax احتمالاتی را برای هر کلاس مشخص‌می‌کند و کلاسی که بیشترین احتمال را دارد به عنوان پیش‌بینی انتخاب‌می‌شود. شبه‌کد زیر در مورد استفاده از تابع softmax است.

```
from tensorflow.keras.models import Sequential
model =  from tensorflow.keras.layers import Dense
()Sequential
model.add(Dense(64, input_shape=(10,), activation='relu')) #
Input Layer with 10 features
model.add(Dense(128, activation='relu'))  # Hidden Layer 1
model.add(Dense(64, activation='relu'))  # Hidden Layer 2
model.add(Dense(3, activation='softmax'))  # Output Layer
```

تـابع softmax کـه از آن در لایـهٔ خروجی اســـتفاده‌می‌شـــود، تعمیم‌یافته‌هایی از تابع فعالســاز ســیگموئید بوده و برای حل مشــکلات مربوط به دســـته‌بندی از آن اســـتفاده‌می‌شـــود. این تابع امکانی را فراهم‌می‌کند که پیش‌بینی احتمالاتی را برای مسأله دسـته‌بندی بیش از دودسته انجاممی‌دهد و به صورت معادله (۲) تعریف‌می‌شود.

$$S(y_i)= e^{y_i} /(\sum e^{y_j}) \qquad (۲)$$

مدل شامل:

لایهٔ ورودی:۱۰ نرون (برای ۱۰ویژگی)

سه لایه پنهان:

۶۴ نرون (لایه ۱)

۳۲ نرون (لایه ۲)

۱۶ نرون (لایه ۳)

لایهٔ خروجی: ۳ نرون (برای ۳ کلاس)

لا یهٔ ورودی داده‌ها را به اولین لا یهٔ پنهان تغذ یه‌می‌کند، جایی که ویژگی‌های اساسی یادمی‌گیرند.

همان‌طور که داده‌ها در هر لایهٔ پنهان حرکت‌می‌کنند، لایهٔ شـــبکه الگوهای پیچیده‌تری را جذب‌می‌کند.

در نهایت لایهٔ خروجی برای هر کلاس احتمالاتی را تولیدمی‌کند و کلاسی که بیشترین احتمال را دارد به عنوان پیش‌بینی انتخاب‌می‌شود.

- **آموزش مدل**

برای آموزش این مدل، از ب‌هینه‌ســاز Adam اســتفاده‌شــده‌اســت که به‌دلیل کارایی آن در کاربردهای یادگیری عمیق و ازدست‌دادن آنتروپی متقاطع طبقه‌بندی شده‌ا ست که برای م سائل طبقه‌بندی چندکلا سه مناسب است.

این مدل بیش از ۵۰ دوره با اندازه د سته‌ای ۳۲ آموزش داده شد. در طول تمرین، وزن‌های مدل مکرراً برای به حداقل رســـاندن عملکرد تلفات و بهبود دقت طبقه‌بندی، تنظیم شده‌است. شبه‌کد زیر این موارد را نشان‌می‌دهد.

```
model.compile(optimizer='adam',
loss='categorical_crossentropy', metrics=['accuracy'])
0, batch_size=32, ۵model.fit(X_train, y_train, epochs=
validation_data=(X_test, y_test))
```

هر دوره شامل چندین گذر از داده‌های آموز شی بود و در پایان ۵۰ دوره، عملکرد مدل تثبیت‌شد و به دقت معقولی دست‌یافت.

الگوریتم بهینه‌سازی و به‌روزرسانی وزن‌ها

بهینه سازها الگوریتم‌هایی ه ستند که به‌وا سطه به‌روز سانی وزن‌ها در شبکه تلاش در جهت کم کردن تابع ضرر دارد. برای بهینه‌کردن مقدار وزن‌ها و تنظیم در این پژوهش از الگوریتم ADAM استفاده‌می‌شود.

برآورد تکانهٔ تطبیقی (ADAM)، روشی جهت محاسبهٔ نرخ یادگیری تطبیقی برای هر پارامتر می‌باشد. این الگوریتم از مزایای الگوریتم‌های Adagradو RMSprop استفاده‌می‌کند و میانگین فروپاشی نمایی از گرادیان‌های گذشته را در vt ذخیره‌می‌کند. علاوه بر این، ADAM، میانگین تکان‌های دوم گرادیان را در mt ذخیره‌می‌کند.

mt و به ترتیب مقادیر میانگین و واریانس غیرمتمرکزند که با معادلات (۳) و (۴) نشان‌داده‌می‌شود.

$$m_t= \beta_1 m_{t-1}+(1-\beta_1)g_t \quad (۳)$$

$$v_t= \beta_2 v_{t-1}+(1-\beta_2)g_t^2 \quad (۴)$$

ADAM م یانگین های تحرک نمایی گراد یان و گراد یان مربع را با معادلات (۵) و (۶) کنترل‌می‌کند.

$$\widehat{m_t}=\frac{m_t}{1-\beta_1^t} \quad (5)$$

$$\widehat{v_t}=\frac{v_t}{1-\beta_2^t} \quad (۶)$$

معادله نهایی برای به‌روزرسانی وزن‌ها:

$$w_{t+1}=w_t-\frac{\eta}{\sqrt{\hat{v}_t}}\odot\widehat{m_t} \quad (۷)$$

β_1 و β_2 در بازه ۰ تا ۱ قراردارند.

w_{t+1} : وزن جدید

w_t: وزن قبلی

η: نرخ یادگیری

$\hat{v}_t$: گرادیان مربع

$\hat{m}_t$: تحرک‌نمایی گرادیان

الگوریتم ADAM از سایر روش های تطبیقی بهتر عمل‌می‌کند و خیلی سریع همگرا می‌شود. همچنین بر سایر مشکلاتی که الگوریتم‌های بهینه‌سازی همانند فروپاشی نرخ یادگیری، واریانس بالا در بهنگام‌سازی و همگرایی آهسته غلبه‌کرده‌اند، غلبه‌می‌کند.

- **تست مدل**

پس از آموزش، مدل بر روی مجموعهٔ دادهٔ آزمایشی WBAN rssi تست شده‌است تا عملکرد آن ارزیابی‌شود. این ارزیابی شامل گزارش طبقه‌بندی است که شامل معیارهایی مانند دقت، فراخوانی و امتیاز F1 برای هر کلاس است.

۵. ارزیابی الگوریتم پیشنهادی

در این قسمت، الگوریتم پیشنهادی در نرم‌افزار پایتون و کتابخانه‌های آن، با استفاده از مجموعه داده WBAN rssi که از Kaggle گرفته‌شده‌است، با تنظیم ابرپارامترها پیاده‌سازی شده‌است. این الگوریتم در پارامترهای دقت، درستی، خطا و فراخوانی ارزیابی و بررسی شده‌است.

مجموعه داده WBAN rssi پیوند بین حسگرها در بدن می باشد. ۱۱ گره به ترتیب در نقاط مختلف بدن، سر، سینه، کمر، بازوی چپ، بازوی راست، دست چپ، دست راست، ساق چپ، ساق راست، پای چپ و پای راست قرارگرفته‌اند که با استفاده از چیپ‌های nRF52832 در فرآیند پیاده‌روی تست‌می‌شوند. آزمایش حدود ۱ ساعت طول می‌کشد و تعدادی پارامترهای مهم روی این چیپ قراردارد که مقادیر را ذخیره‌می‌نماید. هر گره شامل ۱۱ ستون و بالغ بر ۱۸۰۰۰۰ ردیف می‌باشد. محتوای چند سطر آخر ستون اول، مقدار متوسط، مقدار واریانس، انحراف معیار مجموعهٔ داده می‌باشد. ستون‌های دوم تا یازدهم پیوند rssi از گره حسگر به چاهک می‌باشد. محتوای ردیف اول، مشخصات گره چاهک می‌باشد.

برای سنجش میزان کارایی مدل، مجموعهٔ داده به سه قسمت داده‌های آموزشی، آزمایشی و اعتبارسنجی تقسیم‌می‌شود. ابتدا آموزش در بخش بزرگی از داده‌ها انجام می شود که در این پژوهش ۸۰ در صد داده‌ها در نظر گرفته شده است. سپس برای سنجش میزان کارایی مدل و قابلیت تعمیم‌دهی آن از داده‌های آزمایشی استفاده می‌شود. تعمیم‌دهی در داده‌هایی صورت می‌گیرد که مدل آن را م شاهده نکرده است که در این پژوهش ۲۰ درصد باقی‌مانده داده را پوشش می‌دهد.

ابرپارامترها در شبکهٔ عصبی عمیق که از چهار لایه شامل لایهٔ ورودی، سه لایهٔ پنهان و یک لایهٔ خروجی تشکیل شده ا ست، تنظیم می‌شوند. تعداد نرون‌ها در لایهٔ ورودی ۱۰ عدد می‌باشد که تعداد ویژگی‌ها در شبکه می‌باشد و به‌صورت برداری در شبکه تزریق‌می‌شود. تعداد نرون‌ها در لایهٔ خروجی ۳ می‌باشد که مربوط به ۳ کلاس مختلف می‌باشد. کلاس صفر، داده نرمال، کلاس یک، حمله نوع یک و کلاس دو، حمله نوع دو می‌باشد.

تابع فعالساز برای لایه‌های ورودی و پردازش، RELU و برای لایهٔ خروجی Softmax می باشد. از الگوریتم بهینه‌ساز ADAM برای پیداکردن وزن‌ها و تنظیم بهینه استفاده‌می‌شود. جدول ۲ ابرپارامترها و مقادیر آن‌ها را نشان‌می‌دهد.

جدول ۲: ابرپارامترها و مقادیر آن‌ها

ابرپارامتر	مقدار
تعداد لایه‌ها	۴
تعداد نرون لایه اول	۶۴
تعداد نرون لایه دوم	۳۲
تعداد نرون لایه سوم	۱۶
تعداد نرون لایه چهارم	۳
تابع فعالساز	Relu,Softmax
تابع زیان	Cross entropy
الگوریتم بهینه سازی	ADAM
دوره	۵۰
اندازه دسته	۳۲
نرخ یادگیری	0.0002

۱،۵. تحلیل ارزیابی

در زیر به تعدادی ازمعیارها که با آن‌ها می‌توان عملکرد الگوریتم‌ها را بررسی‌کرد اشاره و نتایج به‌دست‌آمده حاصل از مدلسازی روش پیشنهادی تحلیل‌می‌شود.

- **دقت**[۱۳]: نسبت مشاهدات مثبت پیش‌بینی‌شده صحیح به کل مثبت‌های پیش‌بینی‌شده. معادله (۸) این مقدار را نشان‌می‌دهد.

$$\text{Precision}=\frac{TP}{TP+FP} \quad (۸)$$

- **فراخوانی**[۱۴]: نسبت مشاهدات مثبت پیش‌بینی شده درست به همه مشاهدات در کلاس واقعی. معادله (۹) این مقدار را نشان‌می‌دهد.

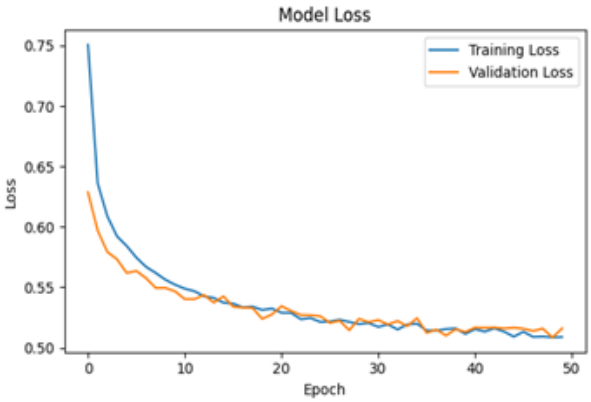
$$\text{Recall}=\frac{TP}{TP+FN} \quad (۹)$$

- **امتیاز F1**: میانگین هارمونیک از دقت و فراخوانی برای نمای متعادل از عملکرد مدل. معادله (۱۰) این مقدار را نشان‌می‌دهد.

$$F1=\frac{2*Precision*Recall}{Precision+Recall} \quad (۱۰)$$

- **خطا**[۱۵]

اختلاف بین مقادیر حاصل از مدل و مقدار واقعی، خطا گفته‌می‌شود. طبق شکل ۴ میزان خطا بعد از ۵۰ دوره به میزان قابل‌توجهی کاهش یافته‌است.



شکل ۴: میزان خطا در حالت آموزش و اعتبارسنجی

- **درستی**[۱۶]

تعداد پیش‌بینی‌های درست بازگردانده شده توسط مدل، درستی نامیده‌می‌شود. نحوهٔ عملکرد آن در شکل ۵ در دو حالت آموزش و اعتبارسنجی دیده‌می‌شود. معادله (۱۱) درستی را نشان‌می‌دهد.

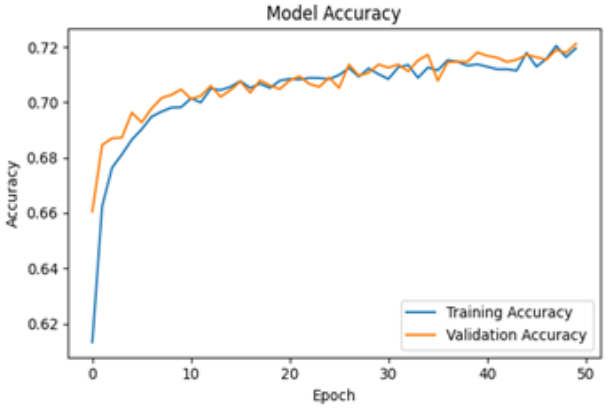
$$\text{Accuracy}=\frac{TP+TN}{TP+TN+FP+FN} \quad (۱۱)$$

TP[۱۷]: مثبت واقعی (پیش‌بینی‌های درست)

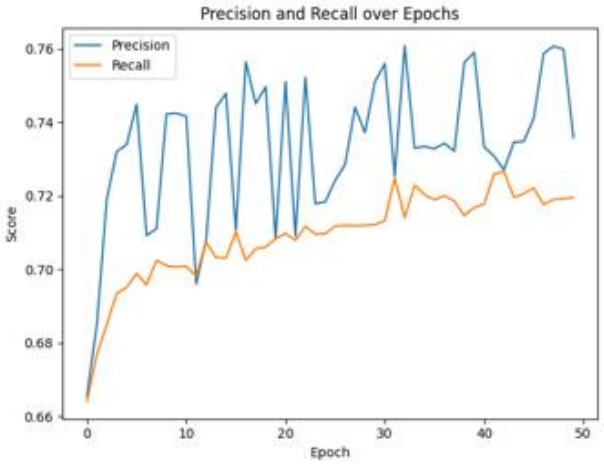
FP[۱۸] مثبت کاذب (پیش‌بینی غلط مدل)

FN[۱۹]: منفی کاذب (مواردی که انتظار پیش‌بینی می‌رود ولی مدل پیش‌بینی نکرده‌است)

TN[۲۰]: منفی واقعی (پیش‌بینی‌های نادرست)



شکل ۵: نمودار درستی در دو حالت آموزش و اعتبارسنجی



شکل ۶: نمودار دقت-فراخوانی

شکل ۶ دو معیار کلیدی را نشان‌می‌دهد که تا ۵۰ دوره ردیابی شده‌است.

دقت در طول آموزش نوسان بیشتری را نشان‌می‌دهد از حدود ۶۶٪ شروع‌می‌شود و در چند دورهٔ اول به سرعت به ۷۳٪ می‌رسد. این معیار همچنین نوسانات قابل‌توجهی دارد و حتی تا حدود ۷۶٪ نیز می‌رسد. نوسانات زیاد، نشان از اهمیت دقت مدل نسبت به فرآیند آموزش است. در پایان آموزش، دقت در حدود ۷۴-۷۵٪ پایدار می‌شود.

فراخوانی الگوی بهبود تدریجی و پایدارتری را نشان‌می‌دهد.از حدود ۶۶٪ شروع‌می‌شود (مشابه با دقت) ولی در مقایسه با دقت، راحت‌تر بهبود می‌یابد. همچنین در طول تمرین نوسانات کمتری را نشان‌می‌دهد.

تحلیل کلی نمودار، شکاف بین دقت و فراخوانی (معمولاً ۲ تا ۴ درصد) را نشان‌می‌دهد که مدل در اجتناب از مثبت کاذب کمی بهتر از منفی کاذب است.

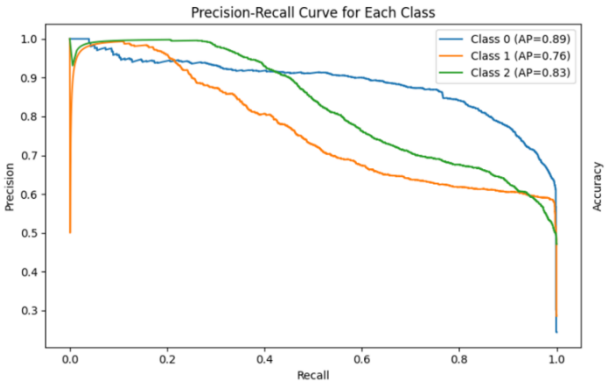
نوسانات بالا در دقت نشان‌می‌دهد که اعتماد مدل به پیش‌بینی‌های مثبت آن به‌طور قابل‌توجهی بین دوره‌ها متفاوت است.

نمودار فراخوانی پایدارتر نشان‌می‌دهد که توانایی مدل برای یافتن همهٔ موارد مرتبط در طول آموزش سازگارتر است.

هیچ کاهش قابل‌توجهی در هیچ یک از معیارها در طول زمان وجود ندارد، که نشان‌می‌دهد مدل از نظر این معیارها افراطی نیست.

رابطهٔ بین این دو معیار نشان‌می‌دهد که این مدل دقت را بر فراخوانی اولویت می‌دهد و همچنین در پیش‌بینی‌ها محافظه‌کارتر است (ترجیح می‌دهد وقتی پیش‌بینی مثبت می‌کند با اطمینان باشد).

اگر عملکرد منسجم‌تری مورد نظر باشد، ممکن است فرآیند آموزش از تکنیک‌هایی برای تثبیت پارامتر دقیق بهره‌مندشود.



شکل ۷: نمودار دقت-فراخوانی برای کلاس‌های مختلف

در شکل ۷ نمودار سه کلاس با نمرات دقت میانگین به شرح زیر نشان‌داده‌شده‌است:

AP [۲۱]- کلاس ۰: =۰,۸۹

AP - کلاس ۱: =۰,۷۶

AP - کلاس ۲: =۰,۸۳

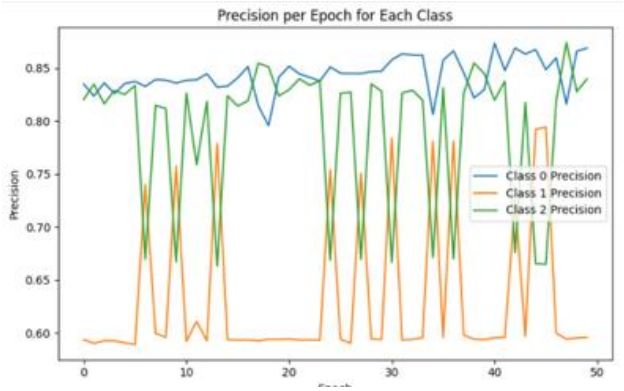
نمودار دقت-فراخوانی برای کلاس‌های صفر تا دو: نمودار منحنی دقت-فراخوانی را برای سه کلاس مختلف (کلاس ۰، ۱ و ۲) در یک طبقه‌بندی نشان‌می‌دهد. این منحنی، نموداری از دقت (محور y) در برابر فراخوان (محور x) برای طیفی از مقادیر آستانه است. نمودار نشان‌می‌دهد که کلاس ۰ بالاترین منحنی دقت-یادآوری را دارد و پس از آن کلاس ۲ و سپس کلاس ۱ قرارمی‌گیرند. یعنی کلاس ۰ بهترین عملکرد را از نظر دقت و فراخوانی در مقایسه با دو کلاس دیگر دارد. مساحت زیر منحنی نیز در پرانتز برای هر کلاس ارائه‌شده‌است که کلاس ۰ دارای بالاترین دقت است، پس از آن کلاس ۲ با ۰,۸۳ و کلاس ۱ با ۰,۷۶ قراردارند.

منحنی دقت-فراخوانی راهی برای ارزیابی مبادله بین دقت و فراخوانی برای یک مدل طبقه‌بندی فراهم‌می‌کند که می‌تواند برای درک عملکرد مدل و انتخاب آستانه‌های تصمیم مناسب مفید باشد.

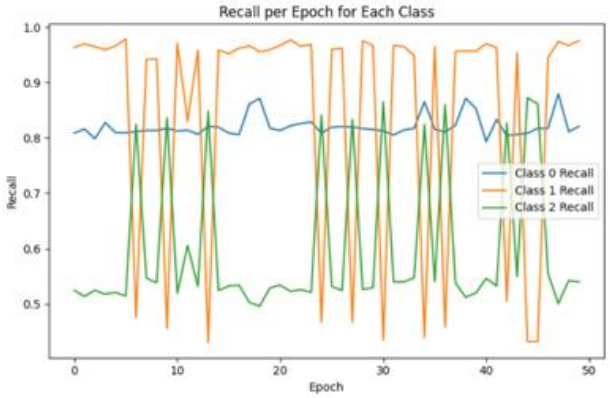
کلاس ۰ (داده عادی) دارای امتیاز F1 بالایی (۰,۸۳) است که نشان‌دهنده عملکرد خوب در تشخیص داده عادی است.

کلاس ۱ (حمله نوع ۱) RECALL کمتری دارد، به این معنی که مدل برای شناسایی برخی از نمونه‌های این کلاس مشکل داشت.

کلاس ۲ (حمله نوع ۲) RECALL خوبی دارد اما دقت کمتری دارد که نشان‌دهنده برخی موارد مثبت کاذب در این کلاس است.



شکل ۸: نمودار دقت برای هر کلاس



شکل ۹: نمودار فراخوانی برای هر کلاس

شکل‌های ۸ و۹ دو نمودار معیارهای عملکرد دقت و فراخوانی را برای هر کلاس در یک مدل طبقه‌بندی چندکلاسه در دوره‌های آموزشی نشان‌می‌دهند.

نمودار دقت در هر دوره برای هر کلاس، مقادیر دقت کلاس ۰، کلاس ۱ و کلاس ۲ را در ۵۰ دوره آموزشی نمایش‌می‌دهد. مقادیر بین ۰,۶۵ و ۰,۸۵ برای کلاس‌های مختلف در نوسان است، که نشان‌می‌دهد مدل پیش‌بینی‌های مثبت نسبتاً دقیقی انجام‌می‌دهد.

نمودار فراخوانی در هر دوره برای هر کلاس، مقادیر فراخوانی را برای همان سه کلاس در طول آموزش نشان‌می‌دهد. فراخوانی، کسری از پیش‌بینی‌های مثبت واقعی را از تمام نمونه‌های مثبت واقعی در داده‌ها نشان‌می‌دهد. مقادیر فراخوان نیز در محدوده ۰,۶۵-۰,۸۵ در نوسان است، که نشان‌می‌دهد مدل قادر به شناسایی بخش خوبی از موارد مثبت برای هر کلاس است.

نمودارها، بینش‌هایی در مورد عملکرد کلاس خاص مدل ارائه‌می‌دهند. ازجمله اینکه برخی از کلاس‌ها، مانند کلاس ۰ و کلاس ۱، دقت و فراخوانی پایدارتری را در مقایسه با کلاس ۲ نشان‌می‌دهند. این اطلاعات به توسعه‌دهنده کمک‌می‌کند تا عدم تعادل بالقوه یا زمینه‌های بهبود را در توانایی مدل برای پیش‌بینی دقیق و شناسایی نمونه‌های هر کلاس تشخیص‌دهد.

در زیر گزارش طبقه‌بندی برای مجموعهٔ داده آزمایش آمده‌است. این گزارش برا ساس امتیاز دقت، فراخوانی، پشتیبان و امتیاز F1 می‌با شد.

پشتیبان، تعداد نمونه‌های پاسخ صحیح است که در هر کلاس (از ۰ تا ۲) از مقادیر، هدف قرارمی‌گیرد. جدول ۳، گزارش را نشان‌می‌دهد.

Macro avg با استفاده از میانگین بدون وزن محاسبه‌می‌شود که می‌تواند مدل را در صورت ضعیف‌بودن عملکرد در کلاس‌های اقلیت جریمه‌کند. از سوی دیگر، میانگین وزن‌دار، تعداد نمونه‌های واقعی در هر کلاس را برای مقابله با عدم تعادل طبقاتی درنظرمی‌گیرد و در نتیجه به نفع طبقهٔ اکثریت می‌باشد.

برای محاسبه این معیار، ابتدا مقادیر فراخوانی یا دقت به‌دست‌آورده‌می‌شود و در نهایت میانگین آن محاسبه‌می‌گردد. معادلات (۱۲) و (۱۳) به ترتیب این معیار را برای فراخوانی و دقت نشان‌می‌دهد.

$$\text{Macro average Recall}=\frac{\sum_{i=1}^{n} Recall_i}{n} \quad (۱۲)$$

$$\text{Macro average Precision}=\frac{\sum_{i=1}^{n} Precision_i}{n} \quad (13)$$

شبه‌کد زیر در مورد جدول طبقه‌بندی می‌باشد.

```
from sklearn.metrics import classification_report
y_pred = model.predict(X_test)
y_pred_classes = np.argmax(y_pred, axis=1)
y_true_classes = np.argmax(y_test, axis=1)
print(classification_report(y_true_classes, y_pred_classes))
```

جدول۳: گزارش طبقه‌بندی برای مجموعه داده آزمایش

Model Classification Report on Test Dataset				
	Precision	Recall	F1-Score	Support
0	0.86	0.81	0.83	2325
1	0.59	0.98	0.74	2726
2	0.84	0.52	0.64	4497
Accuracy			0.72	9548
Macro avg	0.76	0.77	0.74	9548
Weighted avg	0.77	0.72	0.72	9548

۶. نتیجه‌گیری

در این پژوهش، سامانهٔ تشخیص نفوذ مبتنی بر یادگیری عمیق برای شبکه‌های حسگر بی سیم بدنی ارائه شده است. این شبکه‌ها به‌دلیل اینکه شرایط بالینی بیمار را نشان‌می‌دهند، از اهمیت ویژه‌ای برخوردار هستند. هرگونه ناهنجاری و نفوذ در این شبکه‌ها، منجر به مشکلات عدیده‌ای برای بیمار می‌شود. بنابراین مسأله تشخیص نفوذ در این شبکه‌ها بسیار مهم است. در سامانهٔ پیشنهادی تشخیص نفوذ، نخست مجموعهٔ داده توسط PANDAS بارگزاری و پیش‌پردازش می‌شود تا داده‌های معمولی از داده‌های مورد حمله واقع‌شده جداشوند. سپس ویژگی‌های مهم شناسایی‌شده بر اساس اهمیت، عددی بین صفر تا یک به آن‌ها اختصاص داده‌می شود. نرمال سازی با استفاده از MIN-MAX Scaler انجام می‌گردد. سپس، شبکه جدید با استفاده از یادگیری عمیق و ۳ لایه مخفی آن طراحی می شود. شبکه براساس این معماری با استفاده از داده‌ها اموزش داده‌می‌شود و مدل تست می‌شود. نمودارهای خطا، دقت، فراخوانی و امتیاز F1 بر اساس آن مجموعهٔ داده ترسیم‌شده‌است.

هرچند این مدل به دقت مناسب ۷۲٪ دست‌یافت، چندین زمینه برای بهبود آن وجوددارد. مدل برای مقادیر مثبت بسیار خوب عمل‌می‌کند. یعنی پیش‌بینی‌های مثبت، بسیار نزدیک به مقادیر مثبت واقعی هستند. سپس نمودارهای مورد نیاز برای هر کلاس ترسیم‌شده‌است. کلاس صفر بهترین مقدار دقت و فراخوانی را دارد. بعد از آن کلاس ۲ با ۰,۸۳ و کلاس ۱ با ۰,۷۶ دارای بیشترین دقت هستند. این مدل در حالت کلی برای مجموعهٔ داده خوب عمل‌می‌کند ولی می‌توان بهبودهای دیگر نیز در همین راستا روی مدل انجام‌داد. این بهبودها شامل تنظیم ابرپارامتر: می‌تواند با نرخ‌های مختلف یادگیری، اندازه‌های دسته‌ای و تعداد دوره‌های بهینه آزمایش‌شود.

تعادل کلاس: مدیریت مجموعه داده های نامتعادل می‌تواند فراخوانی کلاس‌های اقلیت را بهبودبخشد.

معماری‌های پیشرفته: با استفاده از شبکه‌های عصبی تکرارشونده یا شبکه‌های عصبی پیچیده برای بهبود عملکرد مدل می‌توان تست و تحقیق کرد.

References

[1] K. Heshan, K. Ibrahim, T. Zahir, Z. Alber, “Distributed anomaly detection for industrial wireless sensor networks based on fuzzy data modelling”, parallel and distributed computing, vol,۷۳.no. 6, pp. 790-806, 2013.

[2] S. Mambwe Kasongo, “A deep learning technique for intrusion detection system using a Recurrent Neural Networks based framework” Computer Communications,Volume 199, Pages 113-125,2023.

[3]M. Usman, M. R. Asghar, I. S. Ansari, and M.Qaraqe, "Security in Wireless Body Area Networks: From In-Body to Off-Body Communications," IEEE Access, vol. 6, pp.58064-58074, 2018.

[4]O. Salem, A. Serhrouchni, A. Mehaoua, and R.Boutaba, "Event Detection in Wireless Body Area Networks using Kalman Filter and Power Divergence," IEEE Transactions on Network and Service Management, 2018.

[5] N. K. Jha, A. Raghunathan, and M. Zhang,"Securing medical devices through wireless monitoring and anomaly detection," ed: Google Patents, 2018.

[6] A. Rani, A. Viswasa and E. Baburaj, "Secure and intelligent architecture for cloud-based healthcare applications in wireless body sensor networks", *Int. J. Biomed. Eng. Technol.*, vol. 29, no. 2, pp. 186-199, 2019.

[7] A. Alabdulatif, I. Khalil, A. R. M. Forkan and M. Atiquzzaman, "Real-time secure health surveillance for smarter health communities", *IEEE Commun. Mag.*, vol. 57, no. 1, pp. 122-129, Jan. 2019.

[8] S. Carta, S.; Podda, A.S.; Reforgiato Recupero, D.R.; Saia, R. “A Local Feature Engineering Strategy to Improve Network Anomaly Detection”. Future Internet **vol.** 12, no.177.2020.

[9] B. A. Alzahrani, S. A. Chaudhry, A. Barnawi, A. Al-Barakati and M. H. Alsharif, "A privacy preserving authentication scheme

for roaming in IoT-based wireless mobile networks", *Symmetry*, vol. 12, no. 2, pp. 287, Feb. 2020.
[10] V. Odelu, S. Saha, R. Prasath, L. Sadineni, M. Conti and M. Jo, "Efficient privacy preserving device authentication in WBANs for industrial e-health applications", Comput. Secur., vol. 83, pp. 300-312, Jun. 2019.
[11] G. Thangarasu, K. R. Alla and K. N. Kannan, "Denial of Service Mitigation in Wireless Body Area Network Using Deep Learning," 2024 IEEE 6th Symposium on Computers & Informatics (ISCI), Kuala Lumpur, Malaysia, 2024, pp. 328-332, doi: 10.1109/ISCI62787.2024.10668017.
[12] H. Shaker, M. Nariman, J. Q. Ahmed, D. Radhi. (2023). "A Deep learning approach for trust-untrust nodes classification problem in WBAN. Periodicals of Engineering and Natural Sciences (PEN)", vol.1, no.3. doi: 10.21533/pen.v11i3.3579.
[13] B. Liya, S. Krishnamoorthy, R. Arun, S. "An enhanced deep learning-based disease detection model in wireless body area network with energy efficient routing protocol". Wireless Netw , vol.30, pp. 2961–2986, 2024 https://doi.org/10.1007/s11276-024-03717-1.
[14] R. Arthi, S. Krishnaveni and S. Zeadally, "An Intelligent SDN-IoT Enabled Intrusion Detection System for Healthcare Systems Using a Hybrid Deep Learning and Machine Learning Approach," in China Communications, vol. 21, no. 10, pp. 1-21, Oct. 2024, doi: 10.23919/JCC.ja.2022-0681.
[15] C. Iwend, JH.Anajemba, C. Biamba, D. Ngabo. "Security of Things Intrusion Detection System for Smart Healthcare", Electronics. Vol.10, no.12 2021. https://doi.org/10.3390/electronics10121375.
[16] A. Singh, K.Chatterjee, and S.Chandra Satapathy "TrIDS: an intelligent behavioural trust based IDS for smart healthcare system". Cluster Computing, vol.26, no.2, pp.903–925, 2022. https://doi.org/10.1007/s10586-022-03614-2.
[17]M.R.Erfaneh noroozi,"Presenting A Hybrid Method of Deep Neural Networks to Prevent Intrusion in Computer Networks", Intelligent Multimedia Processing and Communication Systems(IMPCS),no.4, p.65, 2023.
[18]A.K..M.K.SeyedReza Kamel,"An Efficient and Light Weight Intrusion Detection for IoT Based on Fog and Cloud Using KNN Classification", Intelligent Multimedia Processing and Communication Systems(IMPCS),no.2, p.64, 2023.
[۱۹] M.Yaghoubi, K. Ahmed, Y. Miao. "Wireless Body Area Network (WBAN): A Survey on Architecture, Technologies, Energy Consumption, and Security Challenges". Journal of Sensor and Actuator Networks.;vol. 11, no. 4 , 2022. https://doi.org/10.3390/jsan11040067.
[۲۰] P. Pijush, K. Dutta, N. Anand, P.Gaurav, D. Hemanth B. Valentina Emilia, "WBAN: Driving e-healthcare Beyond Telemedicine to Remote Health Monitoring: Architecture and Protocols,Telemedicine", Technologies,Academic Press, Volume 89,NO 119, 2019.
[۲۱] A. Vidyadhar Jinnappa, D. Vijaypal Singh, P. Anubha, k. Sunil, R. Imad , "Internet of Things in healthcare: A survey on protocol standards", enabling technologies, WBAN architectures and open issues, Physical Communication,Vol. 60, No 102103,2023.
[۲۲] S. Karchowdhury and M. Sen, "Survey on attacks on wireless body area network," International Journal of Computational Intelligence & IoT, Forthcoming, 2019.

پی‌نوشت

1 Wireless Body Area Network(WBAN)

2 Support vector machine(SVM)

3 Denial of Service(DOS)

4 Red Piranha and Egret Swarm Algorithm (RPESA)

5 An Adaptive Dilated Cascaded Recurrent Neural Network (ADC-RNN)

6 Medical Cyber Physical System(MCPS)

7 Smart Medical Device(SMD)

8 Medical Smart Phone(MSP)

9 Global Position System(GPS)

10 Personal Server(PS)

11 Rectified Linear Unit(RELU)

12 Adaptive Moment Estimation(ADA M)

13 Precision

14 Recall

15 Loss

16 Accuracy

17 True Positive(TP)

18 False Positive(FP)

19 False Negative(FN)

20 True Negative(TN)

21 Average precision(AP)