

## Intrusion Detection Using Deep Learning in Wireless Body Area Networks

Navid Asadi<sup>1</sup>, Elham Hajian<sup>2\*</sup>

1. MSc. Student, Department of Computer Engineering, Univeristy of Bojnord, Bojnord, Iran.  
[navidasadi100@gmail.com](mailto:navidasadi100@gmail.com)
2. Assistant Professor, Department of Computer Engineering, Univeristy of Bojnord, Bojnord, Iran.  
\*Corresponding Author, [e.hajian@ub.ac.ir](mailto: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.

## تشخیص نفوذ با استفاده از یادگیری عمیق در شبکه‌های حسگر

### بی‌سیم بدنی

دوره پنجم، زمستان ۱۴۰۳

شماره چهارم، صص: ۱-۱۳

تاریخ دریافت: ۱۴۰۳/۰۷/۱۴

تاریخ پذیرش: ۱۴۰۳/۰۸/۲۶

نوید اسدی<sup>۱</sup>، الهام حاجیان<sup>۲\*</sup>

۱. دانشجوی کارشناسی ارشد، دانشکده فنی و مهندسی، دانشگاه بجنورد، بجنورد، ایران. [navidasadi100@gmail.com](mailto:navidasadi100@gmail.com)

۲. استادیار گروه مهندسی کامپیوتر، دانشکده فنی و مهندسی، دانشگاه بجنورد، بجنورد، ایران. (نویسنده مسئول) [E.Hajian@ub.ac.ir](mailto: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 بیماران، نیز از این امر مستثنی نیستند. این شبکه‌ها به‌دلیل کاربردهای حساس پزشکی از اهمیت ویژه‌ای برخوردارند. هرگونه 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 وظایف 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 ابداع شده‌اند 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 انجام می‌شود. مجموعه داده WBAN rssi که از Kaggle گرفته شده‌است، در ۳ کلاس مختلف نرمال، حمله نوع ۱ و حمله نوع ۲ بررسی می‌شود. سپس نمودار الگوریتم پیشنهادی برای دقت، درستی و فراخوانی و امتیاز F1 با استفاده از مجموعه داده به‌تنهایی و در ۳ کلاس مختلف ترسیم شده‌است که نشان از دقت ۰٫۷۲ دارد.

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

## ۱. مقدمه

نخست داده‌های جمع‌آوری‌شده را تحلیل می‌کند و در جریان آماده‌سازی قرار می‌دهد. با استفاده از الگوریتم یادگیری عمیق، ویژگی‌هایی از ترافیک شبکه استخراج می‌شود که موجب بالا رفتن نرخ تشخیص نفوذ می‌شوند. سپس معماری چندلایه بر اساس شبکه عصبی با تعریف تعداد لایه‌ها، تعداد نرون‌ها در هر لایه و پارامترهای آن‌ها تنظیم می‌شود. سپس مدل بر روی داده‌های آموزشی، آموزش داده می‌شوند. الگوریتم Adam برای بهینه‌سازی وزن‌های شبکه عصبی استفاده می‌شود. در نهایت عملکرد الگوریتم بر روی داده‌های تست برای اندازه‌گیری دقت، ارزیابی می‌گردد. خلاصه‌نویسی این مقاله عبارت‌است از ارائه روشی مبتنی بر یادگیری عمیق برای انتخاب بهترین ویژگی‌ها از میان داده‌های جمع‌آوری‌شده به منظور بالا بردن نرخ تشخیص نفوذ در ترافیک شبکه حسگر بی‌سیم بدنی.

## ۲. تاریخچه

محمد عثمان و همکاران [۳] شبکه‌های حسگر بی‌سیم بدنی را از زاویه انتقال داده بررسی کرده‌اند. ایشان انتقال داده را در این شبکه به چهاربخش (۱) جمع‌آوری داده توسط حسگر (۲) انتقال به گره چاهک (۳) انتقال به دروازه اینترنت و (۴) انتقال به پزشک، تقسیم کرده‌اند و سپس به بررسی تهدیدهای امنیتی هر بخش پرداخته‌اند. از آنجاکه حسگرهای قرارگرفته بر روی بدن بیمار ممکن است از دقت کافی در اندازه‌گیری برخوردار نباشند، ضروری است تا مقادیر اندازه‌گیری شده توسط حسگرها بررسی شوند. هرگونه مقدار اندازه‌گیری شده 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 از فیلتر کالمن استفاده کرده‌اند. ایشان از فیلتر کالمن برای پیش‌بینی مقدار اندازه‌گیری‌شده توسط حسگر استفاده می‌کنند. با محاسبه مقدار همگرایی بین این دو مقدار و پایش دیگر جنبه‌های سلامتی بیمار، می‌توانند مقادیر اندازه‌گیری شده اشتباه را شناسایی کنند.

جی‌ها [5] با افزودن یک دستگاه خارجی به شبکه حسگر بی‌سیم بدن، به نام MEDMON امنیت آن را تأمین کرده‌است. این دستگاه برای هردو مرحله داده آزمایشی و داده واقعی در نزدیک محل شبکه حسگر بی‌سیم قرار گرفته و برای بیمارهای مختلف آموزش می‌بیند. بدین ترتیب می‌تواند میان ویژگی‌های رفتاری شبکه‌های حسگر بی‌سیم بدن اولویت‌بندی کرده و رفتار عادی و ناهنجار را طبقه‌بندی کند. MEDMON برای تشخیص ناهنجاری، سیگنال‌های موجود در شبکه حسگر بی‌سیم، بدن را نظارت کرده و بعد از تحلیل آن‌ها تشخیص می‌دهد که ترافیک موجود، مربوط به یک ترافیک عادی است یا به یک ترافیک ناهنجار تعلق دارد.

در [6] سیستم مراقبت بهداشتی مبتنی بر ابر توسط رانی و همکاران پیشنهاد شده‌است که در آن داده‌ها فقط توسط کاربران مجاز قابل دسترس است. این سیستم از روش ماشین بردار پشتیبان<sup>۲</sup> برای پیش‌بینی شرایط بیماران و بیماری‌های مورد انتظار و همچنین از

شبکه حسگر بی‌سیم بدنی<sup>۱</sup> یکی از تکنیک‌ها و فناوری‌های مهم در زمینه پزشکی می‌باشد که به منظور حمایت از برنامه‌های کاربردی حوزه سلامت بر روی تلفن همراه نصب می‌شود. این شبکه‌ها مجموعه‌ای از تعداد معینی حسگر درون یا روی بدن انسان است که سیگنال‌های زیستی انسان مانند: درجه حرارت، فشارخون، الکتروکاردیوگرافی را از طریق حسگرهای متصل به بدن انسان دریافت و به یک مرکز پزشکی برای بررسی اطلاعات ارسال می‌کنند. استفاده از حسگر بی‌سیم بدنی، موجب استفاده بهینه از منابع بیمارستانی و تشخیص زودهنگام علائم پزشکی و در نهایت کاهش هزینه‌های مراقبت پزشکی شده‌است. از آنجاکه در شبکه‌های حسگر بی‌سیم ارسال داده از طریق همه‌پخش انجام می‌شود، هرگونه حمله سایبری مانند استراق‌سمع، 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 مسیری‌ها و ساختار گره‌ها تأثیر بگذارند، فرآیندهای مسیریابی را تغییر دهند، تغییراتی غیرقانونی در شبکه انجام دهند یا داده‌های تحریف شده بسازند. تمامی موارد نام‌برده می‌توانند به راحتی از طریق پیاده‌سازی حملات روی این نوع از شبکه‌ها به تجهیزات نظارتی در بدن انسان، القاء شود و تأثیر سوء داشته باشد. 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].

به دلیل 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 استفاده کرد.

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 شناسایی و گزارش حملات است. یکی از مزایای سیستم‌های تشخیص نفوذ در مقابل روش‌های امنیتی دیگر، پوشش طیف وسیعی از حملات در شبکه‌های حسگر و به تبع آن حسگر بدنی است. محققان سیستم‌های تشخیص نفوذ مختلفی را برای شبکه‌های حسگر ارائه کرده‌اند اما با توجه به محدودیت‌های موجود در شبکه‌های حسگر بی‌سیم، طراحی سیستم تشخیص نفوذ مؤثر و کارا که قابل استفاده 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 انجام می‌شود. این سامانه پیشنهادی با هدف شناسایی حملات و افزایش نرخ تشخیص،

داده کاوی برای یادگیری ماشین استفاده می‌کند. یادگیری ماشین در کشف حملات به داده‌ها نقشی ندارد.

علا بدلطیف و همکاران سیستمی را پیاده سازی کرده‌اند که تغییرات زمان را تشخیص داده و ناهنجاری را در چند علائم حیاتی بدن بیمار پیش‌بینی می‌کند [۷]. سیستم از سه بلوک تشکیل شده است، جمع‌آوری و تجمیع داده‌ها، ارسال به ابر و ذخیره‌سازی داده به فرمت رمزگذاری شده. آخرین بلاک از مدل‌های ریاضی بدون رمزگشایی استفاده می‌کند که تغییرات ناهنجاری و در نتیجه حملات را تشخیص می‌دهد.

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

الزهرانی و همکاران در [9] اگرچه ناشناس بودن، غیرقابل ردیابی و محافظت در برابر حمله داخلی ممتاز را انجام داده‌اند ولی به دلیل محاسبات و پارامترهای سنگین از گره سطح اول که باعث می‌شود مهاجم مقادیر پارامترهای جعلی را در طول ارتباط ارسال کند، در برابر حمله انکار سرویس<sup>۲</sup> آسیب‌پذیر است.

همچنین اودلو و همکاران [10] یک پروتکل احراز هویت سبک‌وزن برای شبکه‌های حسگر بی سیم بدنی براساس جفت شدن دو خطی 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 ایمن می‌کند اما زمان محاسبات و پیچیدگی بالایی دارد.

در [۱۱] توسط تانگراسو سیستم جلوگیری از نفوذ ارائه شده‌است که منجر به کاهش معنادار تعداد حملات سیستم شبکه بدنی بی سیم می‌شود. در این پژوهش از شبکه عصبی متراکم استفاده شده که داده یادگیری‌اش را از چندین مجموعه داده به دست می‌آورد. در این پژوهش از طریق استفاده از پایگاه داده انکار سرویس توزیع شده به عنوان تست مدل آموزش دیده می‌تواند حملات را شناسایی کند. استفاده از شبکه عصبی متراکم در این پژوهش، بهبود قابل توجه نرخ تشخیص و پیشگیری را در مقایسه با مدل‌های دیگر یادگیری عمیق در شبیه‌سازی نشان می‌دهد.

شاکر در [۱۲] با استفاده از یادگیری عمیق، طبقه‌بندی قابل اعتماد و غیرقابل اعتماد انجام می‌دهد. سپس برای حذف درایه‌های تکراری از داده 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 مقایسه شده‌است که نشان از برتری این روش در دقت و تأخیر می‌باشد.

در [13] توسط لیا برای انجام مسیریابی درست و انتخاب بهینه سرخوشه از الگوریتم ازدحام مرغ ماهی‌خوار و پیرانای قرمز<sup>۴</sup> استفاده می‌شود. زمانی که سرخوشه به صورت بهینه انتخاب می‌گردد، مسیریابی بهینه با الگوریتم RPESA اجرامی‌شود. سپس داده‌های ارسالی با استفاده از این طرح برای تشخیص بیماری به یک شبکه

عصبی بازگشتی آبخاری گشاد شده<sup>۵</sup> فر ستاده می‌شود. پارامترها با استفاده از RPESA به صورت بهینه در الگوریتم شبکه عصبی بازگشتی آبخاری بهینه انتخاب می‌شوند و خروجی بیماری طبقه‌بندی شده از الگوریتم به دست می‌آید. رویکرد مسیریابی انرژی کارآمد مبتنی بر رویکرد تعاملی پیاده‌سازی می‌شود.

آرتی در [۱۴] از شبکه نرم‌افزار محور برای داشتن چارچوبی امن در اکوسیستم بهداشتی اینترنت اشیا و ترکیب یادگیری عمیق و یادگیری ماشین برای شناسایی حملات شبکه در داده حسگرهای بهداشتی استفاده کرده‌است. همچنین به صورت کارا بر وسایل متصل شده و رفتارهای ناخواسته نظارت می‌کنند.

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 ترکیب کرده و توسط آن‌ها یک روش بهینه‌سازی برای سیستم تشخیص نفوذ ارائه شده‌است که نرخ تشخیص بالا و اطلاعات درست می‌دهد. برای بهینه‌سازی دید، الگوریتم ژنتیک وزن دار و جنگل تصادفی ترکیب شده استفاده می‌شود که بهترین زیرمجموعه را برای رسیدن به نرخ کشف بالا تولید می‌کند. برای این هدف از طبقه بندی رگرسیون لجستیک برای یادگیری ماشین استفاده می‌نماید. نتایج حاکی از آن است که در پارامترهای دقت و نرخ تشخیص و F1، تابع بهینه سازی به خوبی عمل کرده‌است. ترکیب الگوریتم ژنتیک و جنگل تصادفی به نرخ تشخیص ۹۸٫۸٪ و نرخ پیش‌بینی غلط ۰٫۸٪ می‌رسد.

آشیش در [۱۶] سیستم فیزیکی سایبری پزشکی ارائه کرده که از حسگرهایی با هزینه کم برای تشخیص زمان واقعی، نظارت و تصمیم‌گیری تشکیل شده‌است. داده‌های حساس MCPS توسط شخص سوم قابل اعتماد پردازش می‌شوند. بنابراین انتقال داده از مالک به شخص سوم در معرض آسیب‌پذیری از فعالیت‌های مخرب قرار می‌گیرد. همچنین می‌توان حملات از درون شبکه را به راحتی انجام داد و اطلاعات محرمانه بیمار را به بیرون منتقل کرد. 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<sup>۶</sup>، مانند تلفن هوشمند پزشکی<sup>۷</sup>، پیشنهاد می‌کند. میزان اعتماد SMD/MSP را می‌توان با استفاده از پارامترهای رفتاری مختلف با مدل شهرت بنا ارزیابی کرد. مجموعه‌ای از قوانین تصمیم‌گیری براساس درجه اعتماد محاسبه شده به صورت پویا برای بررسی سطح نفوذ گره و فرآیند تولید هشدار پیشنهاد شده‌است. عملکرد مدل پیشنهادی دقت ۹۳٫۹٪ را نشان می‌دهد.

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

کرده است. با استفاده از روش‌های ترکیبی، شامل ترکیب معماری شبکه‌های عصبی، ویژگی‌ها، خروجی‌ها و ترکیب نتایج از شبکه‌های عصبی مختلف، تنوع و قدرت تشخیص مدل افزایش می‌یابد و درستی و عملکرد آن بهبود می‌یابد.

در [۱۸] توسط کامل، به دلیل باز بودن محیط اینترنت اشیاء و آسیب‌پذیر بودن وسایل، روشی برای تشخیص نفوذ ارائه کرده‌است. ارائه سیستم تشخیص نفوذ دو لایه مبتنی بر طبقه‌بند KNN برای جداسازی ترافیک عادی از حمله و شبکه مصنوعی پرسپترون چند لایه برای تشخیص نوع حمله استفاده شده‌است. سپس دقت، صحت و فراخوانی برر سی شده‌است. جدول ۱ خلاصه‌ای از مطالعات پیشین را براساس نحوه تشخیص نفوذ نشان می‌دهد.

جدول ۱: خلاصه‌ای از مطالعات پیشین

معايب	مزایا	نحوه تشخیص نفوذ			
		احراز هویت	انتقال داده	داده	مراجعه
			مسیریابی	ترافیک	
	ارتباطات زیاد	امنیت	*		[۳]
	محاسبات زیاد	تشخیص ناهنجاری		*	[۴]
	سخت‌افزار اضافه	امنیت ارتباطات	*		[۵]
	سخت‌افزار اضافه	معماری جدید	*		[۶]
	سربار اضافه	رمزنگاری	*		[۷]
	افزایش تأخیر	کاهش الگوها	*		[۸]
	مقایسه با یک روش کم	زمان محاسبات کم	*		[۹]
	فقط احراز هویت	کاهش تعداد کلیدهای عمومی	*		[۱۰]
	نداشتن راه‌حل برای حملات	کاهش تعداد حملات	*		[۱۱]
	نداشتن راه‌حل حمله	تشخیص گره‌های تحت حمله	*		[۱۲]
	نداشتن راه‌حل حمله	مسیریابی بهینه	*		[۱۳]

[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 شرح داده می‌شود.

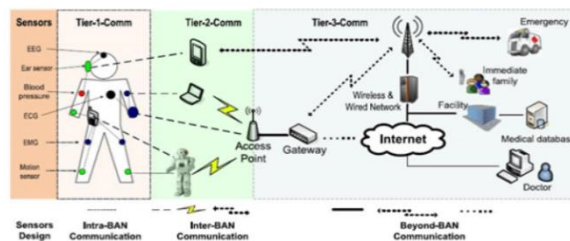
#### ۳.۱ معماری الگوریتم پیشنهادی

با توجه به عملکرد متفاوت شبکه‌های حسگر بی‌سیم بدنی، هر گره می‌تواند نسبت به وظایفش از اجزای متنوعی تشکیل شده باشد ولی در حالت کلی هر گره متشکل است از: واحد پردازش مرکزی، فرستنده - گیرنده رادیویی، منبع تغذیه که می‌تواند از طریق باتری یا سلول‌های خورشیدی یا ترکیب هر دو، انرژی مورد نیاز سیستم را فراهم کند، یک یا تعدادی حسگر که داده‌های مورد نظر را جمع‌آوری می‌کنند، انواع حافظه‌های جانبی در صورت نیاز، سیستم موقعیت‌یاب جهانی<sup>۱</sup> در صورت نیاز و سایر اجزایی که بسته به کاربردهای متفاوت می‌تواند در هر گره گنجانده شود [۱۹].

عواملی چون اقتصادی بودن سیستم، قابلیت مورد انتظار، تعداد انبوه گره‌ها و نهایتاً عملی شدن ایده‌ها در محیط واقعی، موجب محدودیت‌های سخت‌افزاری در هر گره می‌شود. یک WBAN متشکل از تعدادی گره حسگر و یک هماهنگ‌کننده است، هر گره از باتری، حسگر، عملگر، پردازشگر، حافظه و فرستنده گیرنده تشکیل شده است [۲۰].

معماری شبکه، سازمان‌دهی منطقی دستگاه‌های ارتباطی در یک سیستم است. در این بخش سیستم نظارت بر سلامتی بیمار که متشکل از سه لایه است، بررسی می‌شود.

۱. ارتباطات درون BAN لایه شبکه حسگر
۲. ارتباطات بین BAN لایه شبکه محاسبات
۳. ارتباطات فراتر از BAN لایه 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 نشان می‌دهد. ECG، EEG، EMG، حسگرهای حرکتی و حسگرهای فشارخون که داده‌های خود را به دستگاه سرور شخصی<sup>۱۰</sup> ارسال می‌کنند. سپس این داده‌ها در شبکه‌های حسگر بی سیم بدنی برای تشخیص بیماری از طریق ارتباط بلوتوث یا شبکه محلی به سایت یک پزشک یا به یک پایگاه داده پزشکی برای نگهداری سوابق یا به یک سیستم هشداردهنده، فرستاده می‌شود. معماری ارتباطات داخل BAN بر اساس ویژگی‌های سیستم در شرایط خاصی انجام می‌شود 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 بی سیم بدنی

حملات متفاوتی در شبکه‌های حسگر بی سیم بدنی قابل اجرا 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 اشاره می‌شود [۲۲].

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

حمله تزریق داده کاذب: در این نوع حمله، گره مخرب، داده‌هایی برخلاف داده‌های حس شده توسط حسگر را به دستگاه اصلی ارسال می‌کند.

حمله سیل: در این حمله، گره مهاجم تغییر قیافه داده و به عنوان یکی از مجموعه گره‌های متعدد شبکه معرفی می‌شود.

حمله حفره: در این حمله، گره ناهنجار، خود را به عنوان یک گره با منابع زیاد معرفی می‌کند تا حسگرهای دیگر بسته‌های خود را از طریق مسیر گره ناهنجار عبور دهند.

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

حمله زمان بندی: این حمله هنگام تنظیم زمان بندی پروتکل ارتباطی انجام می‌شود. برای مثال، در پروتکل تقسیم زمانی گره مخرب، زمان ارسال بسته را برای تمامی گره‌ها یکسان قرار می‌دهد. بدین ترتیب بسته‌های آرسالی به علت تصادم از بین خواهند رفت.

حمله جلوگیری از سرویس: این حمله عبارت از انواع تلاش‌هایی است که یک گره مهاجم انجام می‌دهد تا یک گره دیگر نتواند خدماتی به سایر گره‌ها ارائه دهد.

در شبکه‌های حسگر بی سیم بدن از سه نوع حمله معروف جلوگیری از سرویس به شرح زیر می‌توان استفاده کرد:

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

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

حمله سیل آسا: در این حمله گره مهاجم بسته‌های اطلاعاتی را به صورت سیل آسا به سمت گره قربانی ارسال می‌کند. دریافت و پردازش بسته‌های سیل آسا به وسیله گره قربانی علاوه بر آنکه مصرف انرژی گره را افزایش می‌دهد، موجب پر شدن بافر ورودی گره شده و امکان دریافت بسته‌های جدید را از بین خواهد برد.

### ۳.۳. سیستم تشخیص نفوذ

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

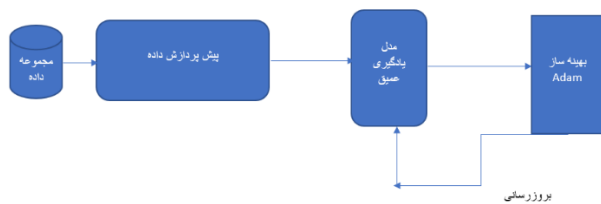
• واحد نظارت: وظیفه ثبت رخدادها را بر عهده دارد. رخدادهای سامانه توسط این واحد جهت تشخیص و تحلیل ثبت می‌شوند. همچنین نمایش هشدار به مدیر شبکه یا مسئول نظارت و پیگیری رویدادهای شبکه بر عهده این واحد است.

• واحد تشخیص و تحلیل: اطلاعات ثبت شده توسط واحد نظارت را به عنوان ورودی دریافت می‌کند و سپس بر اساس این اطلاعات به یکی از روش‌های مبتنی بر سوءاستفاده یا ناهنجاری، مدل ساخته می‌شود. حملات و تهدیدات امنیتی به کمک مدل ساخته شده تمایز داده می‌شوند.

• 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 ارسال می‌کند.

### ۴. الگوریتم پیشنهادی

افزایش دقت برای تشخیص حملات مختلف در شبکه حسگر بدنی بسیار مهم می‌باشد. تحقیقات زیادی در این زمینه صورت گرفته است. یکی از این روش‌ها، استفاده از سیستم‌های شبکه پرسپترون چندلایه - از روش‌های یادگیری عمیق - می‌باشد که برای حل چالش دقت ارائه شده است. افزایش تعداد لایه‌های پنهان کارایی شبکه را بهبود می‌دهد. افزایش لایه‌ها و عمیق کردن شبکه، ویژگی‌ها و خروجی شبکه را به واقعیت بیشتر نزدیک می‌کند ولی بار محاسباتی را نیز



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 شده است، با استفاده از PANDAS بارگذاری می‌شود. مجموعه داده شامل چندین ویژگی است که هر نمونه به عنوان معمولی یا یک نوع حمله برچسب‌گذاری شده است.

### • نرمال‌سازی

یکی از مراحل کلیدی پیش‌پردازش 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 تفاوت‌های بزرگ در هنگام آموزش در مقادیر ویژگی‌ها 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)
```

نرمال‌سازی تضمین می‌کند 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 شبکه عصبی ساده و پیش‌خور استفاده شده است.

برای داده‌های ورودی و پردازش آن‌ها از شبکه عصبی عمیق استفاده شده است. این شبکه دارای ۳ لایه پنهان می‌باشد. به منظور پردازش هر لایه باید از تابع فعال‌ساز استفاده شود.

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 پرسپترون چندلایه نمی‌توان از هر تابعی استفاده کرد بلکه باید حتماً ماهیت مشتق‌پذیری، پیوسته، یک‌نوا نزولی را داشته‌باشد و همچنین مشتق اول آن به راحتی قابل محاسبه باشد. این لایه‌ها در ادامه بیان می‌شود.

### لایه ورودی

لایه ورودی ویژگی‌ها را دریافت می‌کند. فرض شده است که مجموعه داده دارای ۱۰ ویژگی است. بنابراین لایه ورودی به گونه‌ای پیکربندی شده است که بردارهایی با این اندازه را انتظار داشته‌باشد.

افزایش می‌دهد. بنابراین انتخاب تعداد لایه‌ها بسیار مهم است. یکی از الگوریتم‌های مشهور در بهینه‌سازی وزن‌ها در لایه‌ها روش گرادیان کاهشی است. تابع فعال‌ساز جزء اصلی شبکه عصبی می‌باشد. این تابع مشخص می‌کند که گره فعال است یا خیر. یکی از توابع فعال‌ساز پرکاربرد،  $ReLU^{11}$  می‌باشد. با توجه به اهمیت ویژگی‌ها و نتایج به‌دست‌آمده، ممکن است گره‌های فعال یا غیرفعال گردد. این تابع به دلیل دارا بودن ویژگی خطی، همگرایی الگوریتم گرادیان کاهشی را سریع‌تر می‌کند.

### ۱،۴. فلوجارت الگوریتم پیشنهادی

در الگوریتم پیشنهادی برای تجزیه و تحلیل بهتر داده در جهت بهبود دقت در سیستم‌های تشخیص نفوذ از PANDAS استفاده می‌شود. PANDAS کتابخانه‌ای برای پردازش و تحلیل داده‌ها در زبان پایتون است. با این ابزار می‌توان داده‌ها را بارگذاری، پاکسازی، تبدیل و تحلیل کرد. سپس با طراحی شبکه‌های عصبی پرسپترون چندلایه از الگوریتم  $ADAM^{12}$  جهت بهینه‌سازی وزن‌ها و تابع فعال‌ساز  $RELU$  استفاده شده است. در فاز اول، پیش‌پردازش و تحلیل با PANDAS انجام می‌شود. در فاز دوم نرمال‌سازی داده انجام شده در فاز سوم، شبکه‌های پرسپترون چندلایه جهت تشخیص حملات از داده‌های نرمال استفاده می‌شود. در فاز چهارم مدل ساخته شده با داده‌های آزمایشی جهت بررسی عملکرد دقت در الگوریتم پیشنهادی اجرا می‌شود تا میزان دقت بررسی شود. شکل ۲، این فلوجارت را نشان می‌دهد. مدل الگوریتم پیشنهادی نیز در شکل ۳، آمده است.



شکل ۲: فلوجارت الگوریتم پیشنهادی

## لایه‌های پنهان

شبکه دارای سه لایه مخفی است و هر کدام به گونه‌ای پیکربندی شده‌اند که از خروجی لایه قبلی یادگیرند.

لایه ۱: یک لایه کاملاً متصل با ۶۴ واحد نرون استفاده شده است که فعالساز ReLU نیز اضافه شده است. این لایه الگوهای اساسی را از داده‌های ورودی می‌گیرد.

لایه ۲: دومین لایه مخفی دارای ۳۲ واحد نرون استفاده شده است که فعالساز ReLU نیز اضافه شده است. این لایه بر روی بازنمایی‌های آموخته شده در لایه اول استوار است و الگوهای پیچیده‌تری را استخراج می‌کند.

لایه ۳: لایه پنهان سوم دارای ۱۶ واحد نرون استفاده شده است و شامل فعالساز ReLU است. این لایه نمایش‌های آموخته شده را اصلاح می‌کند و آن‌ها را برای لایه خروجی آماده می‌کند.

ReLU (واحد خطی اصلاح شده) یک تابع فعالساز متداول است که غیرخطی بودن را به مدل معرفی می‌کند و با اجتناب از مشکل گرادینان ناپدید شدن به همگرایی سریعتر کمک می‌کند.

این تابع در صورتی که ورودی کمتر از ۰ باشد، تابع فعالساز ReLU صفر (۰) و در غیر این صورت مقدار خام را خروجی می‌دهد. به عبارت دیگر، اگر مقدار ورودی بیشتر از ۰ باشد، تابع ReLU همان مقدار ورودی را خروجی می‌دهد. عملکرد تابع فعالساز ReLU از جهات بسیاری مشابه عملکرد نرون‌های زیستی ما است. معادله (۱) این تابع فعالساز را نشان می‌دهد.

$$F(x) = \max(x, 0) \quad (1)$$

ReLU یک تابع غیرخطی است و برخلاف تابع سیگموئید با خطاهای پس‌انتشار مواجه نمی‌شود. علاوه بر این، اگر در شبکه‌های عصبی بزرگتر به جای تابع سیگموئید از تابع ReLU استفاده شود، سرعت مدل سازی بیشتر خواهد بود، به عبارت دیگر مدت زمان مدل سازی کاهش می‌یابد.

✓ باورپذیری بیولوژیکی: این تابع برخلاف تابع پادتقارن  $\tanh$ ، یک‌جانیه است.

✓ فعال سازی پراکنده: برای مثال، در شبکه‌ای که به صورت تصادفی مقداردهی شده است، حدود ۵۰ درصد از واحدهای پنهان، فعال می‌شوند (و خروجی آن‌ها غیر صفر خواهد بود).

✓ انتشار بهتر گرادینان: در این تابع برخلاف توابع فعالساز سیگموئید، مشکل محوشدگی گرادینان کمتری دارد.

✓ محاسبات اساسی: در این تابع فقط از مقایسه، جمع و ضرب استفاده می‌شود.

✓ مقیاس پذیر (  $\max(0, ax) = a \max(0, x)$  for  $a \geq 0$  )

## لایه خروجی

لایه خروجی نهایی با ۳ واحد نرون و یک تابع فعالساز softmax پیکربندی شده است. هر واحد مربوط به یک کلاس در کار طبقه‌بندی است که هر کلاس یک حمله را نشان می‌دهد. تابع softmax احتمالاتی

را برای هر کلاس مشخص می‌کند و کلاسی که بیشترین احتمال را دارد به عنوان پیش‌بینی انتخاب می‌شود. 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
```

تابع softmax که از آن در لایه خروجی استفاده می‌شود، تعمیم یافته‌هایی از تابع فعالساز سیگموئید بوده و برای حل مشکلات مربوط به دسته‌بندی از آن استفاده می‌شود. این تابع امکانی را فراهم می‌کند که پیش‌بینی احتمالاتی را برای مسأله دسته‌بندی بیش از دودسته انجام می‌دهد و به صورت معادله (۲) تعریف می‌شود.

$$S(y_i) = e^{y_i} / (\sum e^{y_j}) \quad (2)$$

مدل شامل:

لایه ورودی: ۱۰ نرون (برای ۱۰ ویژگی)

سه لایه پنهان:

۶۴ نرون (لایه ۱)

۳۲ نرون (لایه ۲)

۱۶ نرون (لایه ۳)

لایه خروجی: ۳ نرون (برای ۳ کلاس)

لایه ورودی داده‌ها را به اولین لایه پنهان تغذیه می‌کند، جایی که ویژگی‌های اساسی یاد می‌گیرند.

همان‌طور که داده‌ها در هر لایه پنهان حرکت می‌کنند، لایه شبکه الگوهای پیچیده‌تری را جذب می‌کند.

در نهایت لایه خروجی برای هر کلاس احتمالاتی را تولید می‌کند و کلاسی که بیشترین احتمال را دارد به عنوان پیش‌بینی انتخاب می‌شود.

## • آموزش مدل

برای آموزش این مدل، از بهینه‌ساز Adam استفاده شده است که به دلیل کارایی آن در کاربردهای یادگیری عمیق و ازدست دادن آن‌تروپی متقاطع طبقه‌بندی شده است که برای مسائل طبقه‌بندی چندکلاسه مناسب است.

این مدل بیش از ۵۰ دوره با اندازه دسته‌ای ۳۲ آموزش داده شد. در طول تمرین، وزن‌های مدل مکرراً برای به حداقل رساندن عملکرد تلفات و بهبود دقت طبقه‌بندی، تنظیم شده است. شبه‌کد زیر این موارد را نشان می‌دهد.

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

هر دوره شامل چندین گذر از داده‌های آموزشی بود و در پایان ۵۰ دوره، عملکرد مدل تثبیت شد و به دقت معقولی دست یافت.



## الگوریتم بهینه‌سازی و به‌روزرسانی وزن‌ها

بهینه‌سازی‌ها الگوریتم‌هایی هستند که به‌واسطه به‌روزرسانی وزن‌ها در شبکه تلاش در جهت کم کردن تابع ضرر دارد. برای بهینه‌کردن مقدار وزن‌ها و تنظیم در این پژوهش از الگوریتم ADAM استفاده می‌شود.

برآورد تکانه تطبیقی (ADAM)، روشی جهت محاسبه نرخ یادگیری تطبیقی برای هر پارامتر می‌باشد. این الگوریتم از مزایای الگوریتم‌های RMSprop و Adagrad استفاده می‌کند و میانگین فروپاشی نمایی از گرادینت‌های گذشته را در  $v_t$  ذخیره می‌کند. علاوه بر این، ADAM، میانگین تکانه‌های دوم گرادینت را در  $m_t$  ذخیره می‌کند.

$m_t$  و به ترتیب مقادیر میانگین و واریانس غیرمتمرکزند که با معادلات (۳) و (۴) نشان داده می‌شود.

$$m_t = \beta_1 m_{t-1} + (1 - \beta_1) g_t \quad (3)$$

$$v_t = \beta_2 v_{t-1} + (1 - \beta_2) g_t^2 \quad (4)$$

ADAM میانگین‌های حرکت‌نمایی گرادینت و گرادینت مربع را با معادلات (۵) و (۶) کنترل می‌کند.

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

$$\hat{v}_t = \frac{v_t}{1 - \beta_2^t} \quad (6)$$

معادله نهایی برای به‌روزرسانی وزن‌ها:

$$w_{t+1} = w_t - \frac{\eta}{\sqrt{\hat{v}_t}} \hat{m}_t \quad (7)$$

$\beta_1$  و  $\beta_2$  در بازه ۰ تا ۱ قرار دارند.

$w_{t+1}$ : وزن جدید

$w_t$ : وزن قبلی

$\eta$ : نرخ یادگیری

$\hat{v}_t$ : گرادینت مربع

$\hat{m}_t$ : حرکت‌نمایی گرادینت

الگوریتم ADAM از سایر روش‌های تطبیقی بهتر عمل می‌کند و خیلی سریع همگرا می‌شود. همچنین بر سایر مشکلاتی که الگوریتم‌های بهینه‌سازی همانند فروپاشی نرخ یادگیری، واریانس بالا در بهنگام‌سازی و همگرایی آهسته غلبه کرده‌اند، غلبه می‌کند.

### • تست مدل

پس از آموزش، مدل بر روی مجموعه داده آزمایشی WBAN rssi تست شده‌است تا عملکرد آن ارزیابی شود. 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 گرفته شده‌است، 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 می‌باشد. 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 قرار گرفته‌اند که با استفاده از چیپ‌های nRF52832 در فرآیند پیاده‌روی تست می‌شوند. آزمایش حدود ۱ ساعت طول می‌کشد و تعدادی پارامترهای مهم روی این چیپ قرار دارد که مقادیر را ذخیره می‌نماید. هر گره شامل ۱۱ ستون و بالغ بر ۱۸۰۰۰۰ ردیف می‌باشد. محتوای چند سطر آخر ستون اول، مقدار متوسط، مقدار واریانس، انحراف معیار مجموعه 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، مجموعه داده به سه قسمت داده‌های آموزشی، آزمایشی و اعتبارسنجی تقسیم می‌شود. ابتدا آموزش در بخش بزرگی از داده‌ها انجام می‌شود که در این پژوهش ۸۰ درصد 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 مشاهده نکرده است که در این پژوهش ۲۰ درصد باقی‌مانده داده را پوشش می‌دهد.

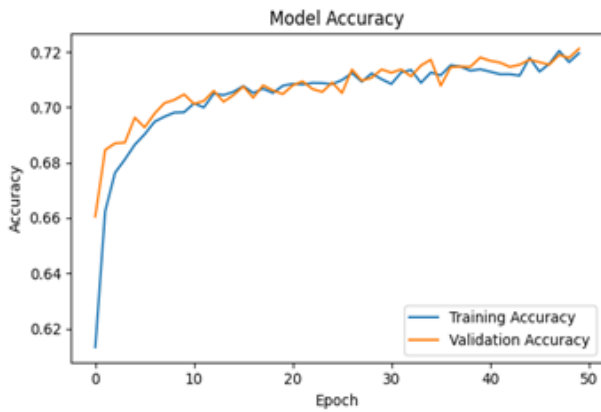
ابریارامترها در شبکه عصبی عمیق که از چهار لایه شامل لایه ورودی، سه لایه پنهان و یک لایه خروجی تشکیل شده است، تنظیم می‌شوند. تعداد نرون‌ها در لایه ورودی ۱۰ عدد می‌باشد که تعداد ویژگی‌ها در شبکه می‌باشد و به‌صورت برداری در شبکه تریقی می‌شود. تعداد نرون‌ها در لایه خروجی ۳ می‌باشد که مربوط به ۳ کلاس مختلف 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 لایه خروجی Softmax می‌باشد. از الگوریتم بهینه‌ساز ADAM برای پیدا کردن وزن‌ها و تنظیم بهینه استفاده می‌شود. جدول ۲ ابرپارامترها و مقادیر آن‌ها را نشان می‌دهد.

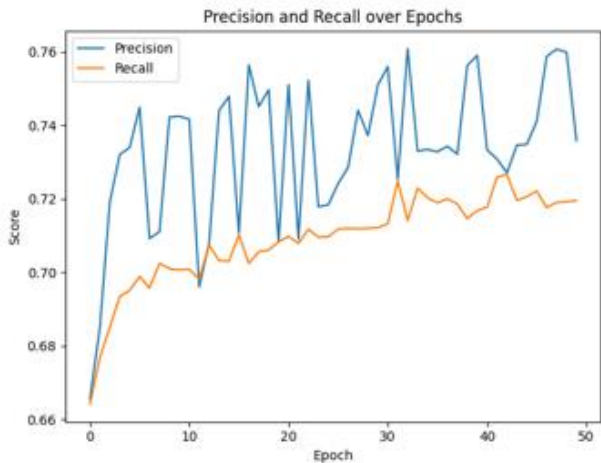
جدول ۲: ابرپارامترها و مقادیر آن‌ها

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

### ۱.۵. تحلیل ارزیابی



شکل ۵: نمودار درستی در دو حالت آموزش و اعتبارسنجی



شکل ۶: نمودار دقت-فراخوانی

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

دقت در طول آموزش نوسان بیشتری را نشان می‌دهد از حدود ۶۶٪ شروع می‌شود و در چند دوره اول به سرعت به ۷۳٪ می‌رسد. این معیار همچنین نوسانات قابل توجهی 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 پایداری را نشان می‌دهد. از حدود ۶۶٪ شروع می‌شود (مشابه با دقت) ولی در مقایسه با دقت، راحت‌تر بهبود می‌یابد. همچنین در طول تمرین نوسانات کمتری را نشان می‌دهد.

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

نوسانات بالا در دقت نشان می‌دهد که اعتماد مدل به پیش‌بینی‌های مثبت آن به‌طور قابل توجهی بین دوره‌ها متفاوت است.

نمودار فراخوانی پایداری نشان می‌دهد که توانایی مدل برای یافتن همه موارد مرتبط در طول آموزش سازگارتر است.

هیچ کاهش قابل توجهی در هیچ یک از معیارها در طول زمان وجود ندارد، که نشان می‌دهد مدل از نظر این معیارها افراطی نیست.

در زیر به تعدادی از معیارها که با آن‌ها می‌توان عملکرد الگوریتم‌ها را بررسی کرد اشاره و نتایج به‌دست‌آمده حاصل از مدلسازی روش پیشنهادی تحلیل می‌شود.

▪ **دقت**<sup>۱۲</sup>: نسبت مشاهدات مثبت پیش‌بینی‌شده صحیح به کل مثبت‌های پیش‌بینی‌شده. معادله (۸) این مقدار را نشان می‌دهد.

$$\text{Precision} = \frac{TP}{TP+FP} \quad (8)$$

▪ **فراخوانی**<sup>۱۳</sup>: نسبت مشاهدات مثبت پیش‌بینی‌شده در ست به همه مشاهدات در کلاس واقعی. معادله (۹) این مقدار را نشان می‌دهد.

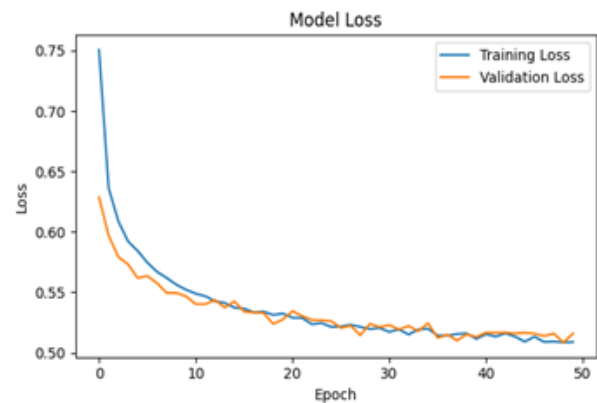
$$\text{Recall} = \frac{TP}{TP+FN} \quad (9)$$

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

$$F1 = \frac{2 * \text{Precision} * \text{Recall}}{\text{Precision} + \text{Recall}} \quad (10)$$

▪ **خطا**<sup>۱۵</sup>

اختلاف بین مقادیر حاصل از مدل و مقدار واقعی، خطا گفته می‌شود. طبق شکل ۴ میزان خطا بعد از ۵۰ دوره به میزان قابل توجهی کاهش یافته‌است.



شکل ۴: میزان خطا در حالت آموزش و اعتبارسنجی

▪ **درستی**<sup>۱۶</sup>

تعداد پیش‌بینی‌های درست بازگردانده شده توسط مدل، درستی نامیده می‌شود. نحوه عملکرد آن در شکل ۵ در دو حالت آموزش و اعتبارسنجی دیده می‌شود. معادله (۱۱) درستی را نشان می‌دهد.

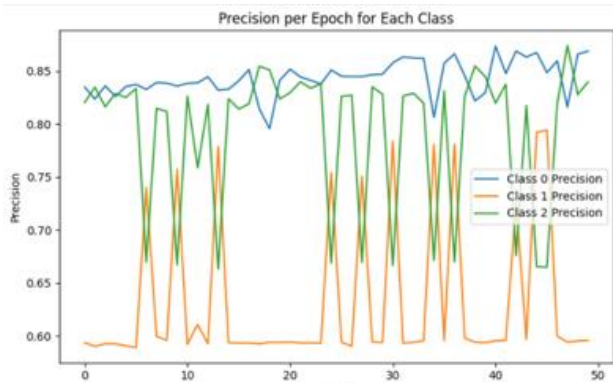
$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad (11)$$

<sup>۱۷</sup>TP: مثبت واقعی (پیش‌بینی‌های درست)

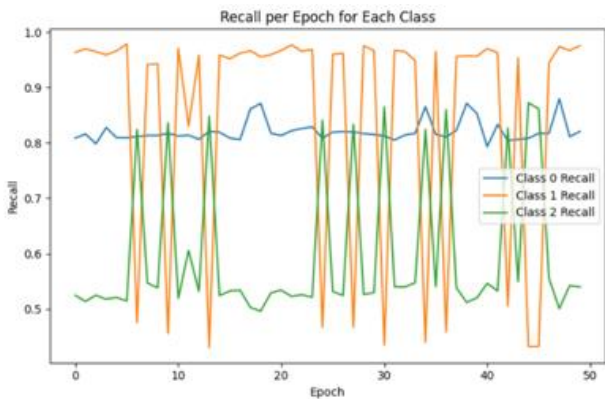
<sup>۱۸</sup>FP: مثبت کاذب (پیش‌بینی غلط مدل)

<sup>۱۹</sup>FN: منفی کاذب (مواردی که انتظار پیش‌بینی می‌رود ولی مدل پیش‌بینی نکرده‌است)

<sup>۲۰</sup>TN: منفی واقعی (پیش‌بینی‌های نادرست)



شکل ۸: نمودار دقت برای هر کلاس



شکل ۹: نمودار فراخوانی برای هر کلاس

شکل‌های ۸ و ۹ دو نمودار معیارهای عملکرد دقت و فراخوانی را برای هر کلاس در یک مدل طبقه‌بندی چندکلاسه در دوره‌های آموزشی نشان می‌دهند.

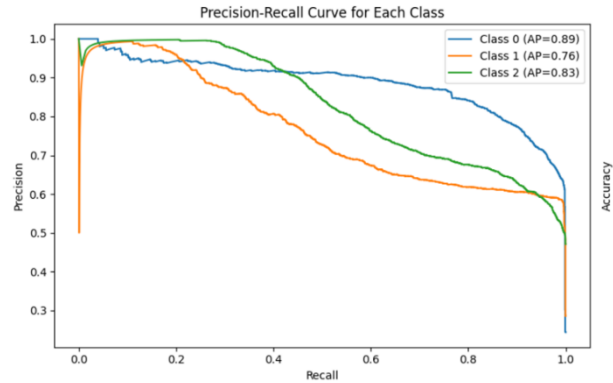
نمودار دقت در هر دوره برای هر کلاس، مقادیر دقت کلاس ۰، کلاس ۱ و کلاس ۲ را در ۵۰ دوره آموزشی نمایش می‌دهد. مقادیر بین ۰.۶۵ و ۰.۸۵، برای کلاس‌های مختلف در نوسان است، که نشان می‌دهد مدل پیش‌بینی‌های مثبت نسبتاً دقیقی انجام می‌دهد.

نمودار فراخوانی در هر دوره برای هر کلاس، مقادیر فراخوانی را برای همان سه کلاس در طول آموزش نشان می‌دهد. فراخوانی، کسری از پیش‌بینی‌های مثبت واقعی را از تمام نمونه‌های مثبت واقعی در داده‌ها نشان می‌دهد. مقادیر فراخوانی نیز در محدوده ۰.۶۵-۰.۸۵، در نوسان است، که نشان می‌دهد مدل قادر به شناسایی بخش خوبی از موارد مثبت برای هر کلاس است.

نمودارها، بینش‌هایی در مورد عملکرد کلاس خاص مدل ارائه می‌دهند. از جمله اینکه برخی از کلاس‌ها، مانند کلاس ۰ و کلاس ۱، دقت و فراخوانی پایدارتری را در مقایسه با کلاس ۲ نشان می‌دهند. این اطلاعات به توسعه‌دهنده کمک می‌کند تا عدم تعادل بالقوه یا زمینه‌های بهبود را در توانایی مدل برای پیش‌بینی دقیق و شناسایی نمونه‌های هر کلاس تشخیص دهد.

در زیر گزارش طبقه‌بندی برای مجموعه داده آزمایش آمده است. این گزارش بر اساس امتیاز دقت، فراخوانی، پشتیبان و امتیاز F1 می‌باشد.

رابطه بین این دو معیار نشان می‌دهد 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 بهره‌مند شود.



شکل ۷: نمودار دقت-فراخوانی برای کلاس‌های مختلف

در شکل ۷ نمودار سه کلاس با نمرات دقت میانگین به شرح زیر نشان داده شده است:

- AP 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 نشان می‌دهد. این منحنی، نموداری از دقت (محور Y) در برابر فراخوانی (محور X) برای طیفی از مقادیر آستانه است. نمودار نشان می‌دهد که کلاس ۰ بالاترین منحنی دقت-یادآوری را دارد و پس از آن کلاس ۲ و سپس کلاس ۱ قرار می‌گیرند. 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 ارائه شده است که کلاس ۰ دارای بالاترین دقت است، پس از آن کلاس ۲ با ۰.۸۳ و کلاس ۱ با ۰.۷۶ قرار دارند.

منحنی دقت-فراخوانی راهی برای ارزیابی مبادله بین دقت و فراخوانی برای یک مدل طبقه‌بندی فراهم می‌کند 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.

پشتیبان، تعداد نمونه‌های پاسخ صحیح است که در هر کلاس (از ۰ تا ۲) از مقادیر، هدف قرار می‌گیرد. جدول ۳، گزارش را نشان می‌دهد. Macro avg با استفاده از میانگین بدون وزن محاسبه می‌شود که می‌تواند مدل را در صورت ضعیف بودن عملکرد در کلاس‌های اقلیت جریمه کند. از سوی دیگر، میانگین وزن دار، تعداد نمونه‌های واقعی در هر کلاس را برای مقابله با عدم تعادل طبقاتی در نظر می‌گیرد و در نتیجه به نفع طبقه اکثریت می‌باشد.

برای محاسبه این معیار، ابتدا مقادیر فراخوانی یا دقت به دست آورده می‌شود و در نهایت میانگین آن محاسبه می‌گردد. معادلات (۱۲) و (۱۳) به ترتیب این معیار را برای فراخوانی و دقت نشان می‌دهد.

$$\text{Macro average Recall} = \frac{\sum_{i=1}^n \text{Recall}_i}{n} \quad (12)$$

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

شبه کد 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))
```

جدول ۳: 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، سامانه تشخیص نفوذ مبتنی بر یادگیری عمیق برای شبکه‌های حسگر بی سیم بدنی ارائه شده است. این شبکه‌ها به دلیل اینکه شرایط بالینی بیمار را نشان می‌دهند، 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 سامانه پیشنهادی تشخیص نفوذ، نخست مجموعه داده توسط PANDAS بارگزاری و پیش پردازش می‌شود تا داده‌های معمولی از داده‌های مورد حمله واقع شده جدا شوند. سپس ویژگی‌های مهم شناسایی شده بر اساس اهمیت، عددی بین صفر تا یک به آن‌ها اختصاص داده می‌شود. نرمال سازی با استفاده از MIN-MAX

Scaler انجام می‌گردد. سپس، شبکه جدید با استفاده از یادگیری عمیق و ۳ لایه مخفی آن طراحی می‌شود. شبکه براساس این معماری با استفاده از داده‌ها آموزش داده می‌شود و مدل تست می‌شود. نمودارهای خطا، دقت، فراخوانی و امتیاز F1 بر اساس آن مجموعه داده ترسیم شده است.

هرچند این مدل به دقت مناسب ۷۲٪ دست یافت، چندین زمینه برای بهبود آن وجود دارد. مدل برای مقادیر مثبت بسیار خوب عمل می‌کند. یعنی پیش‌بینی‌های مثبت، بسیار نزدیک به مقادیر مثبت واقعی هستند. سپس نمودارهای مورد نیاز برای هر کلاس ترسیم شده است. 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 مجموعه داده خوب عمل می‌کند ولی می‌توان بهبودهای دیگر نیز در همین راستا روی مدل انجام داد. این بهبودها شامل تنظیم ابرپارامتر: می‌تواند با نرخ‌های مختلف یادگیری، اندازه‌های دسته‌ای و تعداد دوره‌های بهینه آزمایش شود.

تعادل کلاس: مدیریت مجموعه داده‌های نامتعادل می‌تواند فراخوانی کلاس‌های اقلیت را بهبود بخشد.

معماری‌های پیشرفته: با استفاده از شبکه‌های عصبی تکرار شونده 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. ۷۲ .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. Atiqzaman, "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

[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.

[١٩] 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> .

[٢٠] 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.

[٢١] 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.

[٢٢] S. Karchowdhury and M. Sen, "Survey on attacks on wireless body area network," *International Journal of Computational Intelligence & IoT*, Forthcoming, 2019.

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.v1i1i3.3579.

[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>.

- 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)

## بی نوشت

- 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)