Electronic and Cyber Defense
Vol. 13, No.4, 2025 (Serial No. 30) .pp.73-94
ISSN: 2322-4347 , E-ISSN: 2980-8979
1986 Imam Hossein Comprehensive University

A Hybrid and Intelligent Model for Anomaly Detection in Internet of Things Using Ensemble Learning and Deep Autoencoders

Hadi Tarazodar[1], Karamollah Bagherifard [2*], Samad Nejatian [3], Hamid Parvin [4], Razieh Malekhosseini [5]

[1] Ph.D. Student, Department of computer Engineering ,Yas.C., Islamic Azad University ,Yasuj, Iran, …Email: hadi.tarazodar@iau.ac.ir

[2] Associate Professor, Department of computer Engineering ,Yas.C., Islamic Azad University ,Yasuj, Iran …([*]Correspondence:) Email: Ka.bagherifard@iau.ac.ir

[3] Assistant Professor, Department of Electrical Engineering ,Yas.C., Islamic Azad University ,Yasuj, Iran … Email: Sa.nejatian@iau.ac.ir

[4] Associate Professor, Department of computer Engineering , NoM.C., Islamic Azad University , Noorabad Mamasani, Iran … Email: Parvin@iaut.ac.ir

[5] Assistant Professor, Department of computer Engineering ,Yas.C., Islamic Azad University ,Yasuj, Iran … Email: Malekhoseini.r@iau.ac.ir

ARTICLE INFO

Article history:

Article Type: Research paper

Received: 29 October 2025

Revised: 7 December 2025

Accepted: 8 December 2025

Available online: 13 December 2025

Keywords:

Internet of Things

Anomaly Detection

Stacked Autoencoder

Deep Autoencoder

Ensemble Learning

Dynamic Feature Selection

Adaptive combination of models

Cybersecurity

ABSTRACT

The Internet of Things (IoT) has become a critical infrastructure of the modern world by providing a platform for automated communication between millions of smart devices. The dramatic growth in the number of these devices and the increase in their features such as diversity, scalability, and mobility have also significantly expanded security threats. In particular, the emergence of hidden and complex threats that manifest through unusual behavioral patterns in the network has doubled the need for advanced anomaly detection methods. In this paper, a new model based on ensemble learning is presented that improves the anomaly detection performance in the Internet of Things by combining deep learning techniques and machine learning algorithms. After performing the data preprocessing process, key features were extracted using Stacked Auto Encoder (SAE) and Deep Auto Encoder (DAE), and in the next step, an ensemble learning framework consisting of a decision tree (DT), a multilayer perceptron (MLP), a probabilistic neural network (PNN), and its weighted version (WPNN) was used to identify anomalies. Among the innovations of this research are the design of a dynamic feature selection mechanism in the encoder layer and the proposal of an adaptive weighting scheme for combining the output of ensemble models, which has led to improved accuracy in detecting unknown attacks and reduced false positive rates. The proposed model was evaluated on several valid datasets, including NSL-KDD, BoT-IoT, IoT-NI, IoT-23, and the results show a high accuracy of 99.3% and an F1 score of 99.2% in the combined IoT-DS2 dataset. The false positive rate (FPR) is reported to be below 2% and the false negative rate (FNR) is reported to be below 1.5% in most datasets. Compared to the selected models, the proposed model is superior in detecting unknown attacks.

Cite this article: Tarazodar,H. Bagherifard,K. Nejatian, S. Parvin,H. Malekhosseini, R.(2025).A Hybrid and Intelligent Model for A Ensemble Learning and Deep Autoencoders. Journal of Electronic and Cyber Defense. 2025; 13(4):73-94.

DOI: https://doi.org/10.47176/ECDJ.2025.1669

Publisher: Imam Hossein University.

1.Introduction

The rapid growth of the Internet of Things (IoT) has transformed modern digital ecosystems by enabling seamless communication among interconnected smart devices. IoT technologies are widely deployed in critical sectors such as healthcare, transportation, smart cities, industrial automation, agriculture, and environmental The rapid growth of the Internet of Things (IoT) has significantly transformed modern digital ecosystems by enabling seamless communication among interconnected smart devices. IoT technologies are widely deployed across critical sectors, including healthcare, transportation, smart cities, industrial automation, agriculture, and environmental monitoring. These systems rely on real-time data exchange, lightweight communication protocols, and distributed sensing infrastructures to enhance operational efficiency and automation. Despite these advantages, the proliferation of IoT devices has introduced substantial security and privacy challenges.

IoT networks are inherently vulnerable due to device heterogeneity, limited processing capabilities, constrained memory resources, and the absence of standardized security frameworks. Such constraints render traditional security mechanisms insufficient for detecting sophisticated cyber threats. Consequently, IoT environments have become prime targets for Distributed Denial of Service (DDoS) attacks, botnet intrusions, data injection, spoofing, and zero-day exploits. Signature-based intrusion detection systems are particularly ineffective against such threats because they depend on predefined attack signatures and fail to detect unknown anomalies.

To address these limitations, machine learning techniques have been widely adopted for anomaly detection in IoT traffic. However, classical machine learning approaches rely heavily on manual feature engineering and often struggle with high-dimensional and nonlinear network data. Deep learning models overcome these challenges by automatically extracting hierarchical feature representations, although they typically require high computational resources and may produce elevated false alarm rates.

Recent research indicates that ensemble learning can enhance detection reliability by combining multiple classifiers. Nevertheless, many existing hybrid frameworks lack adaptive feature optimization and dynamic decision fusion mechanisms. Therefore, this study proposes a hybrid anomaly detection framework that integrates deep autoencoder-based feature extraction with adaptive ensemble classification to improve detection accuracy while reducing false positives.

2.Objectives

The primary objectives of this research are as follows:

- To develop a robust anomaly detection framework tailored to securing IoT network environments against advanced and evolving cyber threats.
- To design a hybrid deep feature extraction mechanism by integrating Stacked Autoencoders (SAE) and Deep Autoencoders (DAE) to capture complex nonlinear traffic behaviors.
- To introduce a dynamic feature selection strategy based on neuron activation analysis to remove redundant features and enhance computational efficiency.
- To construct an adaptive weighted ensemble classification model combining Decision Tree (DT), Multilayer Perceptron (MLP), Probabilistic Neural Network (PNN), and Weighted Probabilistic Neural Network (WPNN).
- To evaluate the proposed framework using benchmark IoT intrusion detection datasets based on metrics such as Accuracy, F1-Score, False Positive Rate, and False Negative Rate.
- To compare the performance of the proposed model with existing hybrid and deep learning intrusion detection approaches

3.Methodology

The proposed anomaly detection framework consists of three major phases: data preprocessing, deep feature extraction with dynamic selection, and ensemble-based classification.

In the preprocessing phase, raw IoT traffic datasets are cleaned to remove duplicate, missing, and inconsistent records. Categorical attributes are encoded into numerical form, and all features are normalized to ensure uniform scaling. The processed data is then divided into training and testing subsets for unbiased evaluation.

For deep feature extraction, two complementary architectures—Stacked Autoencoders (SAE) and Deep Autoencoders (DAE)—are employed. SAE learns hierarchical compressed representations through multi-layer encoding, while DAE enhances robustness by learning noise-resilient nonlinear transformations. These models convert high-dimensional traffic data into compact latent feature vectors while preserving essential behavioral characteristics.

A dynamic feature selection mechanism is embedded within the encoding layers. Feature importance is determined using neuron activation magnitudes. Features with low activation values are pruned using an adaptive threshold, reducing redundancy, eliminating noise, lowering computational cost, and improving classification performance.

The optimized feature vectors are then classified using an adaptive ensemble model comprising Decision Tree, Multilayer Perceptron, Probabilistic Neural Network, and Weighted Probabilistic Neural Network. Each classifier generates independent predictions, and their outputs are fused through adaptive weighting based on performance confidence to produce the final anomaly detection result.

4. Results and Discussion

The proposed framework was evaluated using several benchmark IoT intrusion detection datasets, including NSL-KDD, BoT-IoT, IoT-23, MQTT, and IoT-DS2, which contain diverse attack categories such as DDoS, DoS, botnets, reconnaissance, and protocol exploits.

Experimental results demonstrate high detection effectiveness. On the IoT-DS2 dataset, the model achieved accuracy exceeding 99%, with F1-scores above 99%, false positive rates below 2%, and false negative rates below 1.5%. The deep autoencoder architectures successfully captured nonlinear traffic patterns, while the dynamic feature selection mechanism reduced dimensionality without sacrificing discriminative capability, thereby improving computational efficiency.

Comparative analysis with existing hybrid and deep learning intrusion detection models indicates that the proposed approach provides higher detection accuracy, lower false alarm rates, improved detection of unknown attacks, and greater robustness on imbalanced datasets. The adaptive ensemble weighting mechanism further enhanced classification stability by balancing the strengths of individual classifiers.

5.Conclusion

This study presented a hybrid IoT anomaly detection framework integrating deep autoencoder-based feature extraction with adaptive ensemble learning. The combination of stacked and deep autoencoders enabled robust and noise-tolerant representation learning, while the embedded dynamic feature selection mechanism reduced irrelevant features and computational overhead.

In the classification phase, the adaptive weighted ensemble composed of Decision Tree, Multilayer Perceptron, Probabilistic Neural Network, and Weighted Probabilistic Neural Network significantly enhanced detection precision while minimizing false alarms.

Extensive experimental evaluations confirmed the superiority of the proposed framework, achieving detection accuracy exceeding 99% with very low error rates. The findings demonstrate that integrating deep representation learning with intelligent ensemble fusion offers an effective, scalable, and reliable solution for securing IoT environments.

Future work may focus on lightweight deployment for edge devices, federated intrusion detection frameworks, real-time streaming analysis, and explainable artificial intelligence techniques for interpretable threat detection.

«پدافند الکترونیک و سایبری»
سال سیزدهم، شماره ۴، زمستان ۱۴۰۴؛ ص ۹۵-۷۳
شاپا الکترونیکی: ۸۹۷۹-۲۹۸۰ شاپا چاپی: ۴۳۴۷-۲۳۲۲

ارائه مدل ترکیبی و هوشمند برای تشخیص ناهنجاری در اینترنت اشیا با رویکرد یادگیری گروهی و رمزگذارهای عمیق

هادی ترازودار[۱]، کرم اله باقری فرد[۲*]، صمد نجاتیان[۳]، حمید پروین[۴]، راضیه ملک حسینی[۵]

[۱]دانشجوی دکتری ، گروه مهندسی کامپیوتر ، واحد یاسوج، دانشگاه آزاد اسلامی، یاسوج، ایران... رایانامه: hadi.tarazodar@iau.ac.ir
[۲]دانشیار ، گروه مهندسی کامپیوتر ، واحد یاسوج، دانشگاه آزاد اسلامی، یاسوج، ایران... (نویسنده مسئول) رایانامه: Ka.bagherifard@iau.ac.ir
[۳]دانشیار ، گروه مهندسی برق ، واحد یاسوج، دانشگاه آزاد اسلامی، یاسوج، ایران... رایانامه: Sa.nejatian@iau.ac.ir
[۴]دانشیار ، گروه مهندسی کامپیوتر ، واحد نورآباد ممسنی، دانشگاه آزاد اسلامی، نورآباد ممسنی ، ایران... رایانامه: Parvin@iaut.ac.ir
[۵]استادیار ، گروه مهندسی کامپیوتر ، واحد یاسوج، دانشگاه آزاد اسلامی، یاسوج، ایران... رایانامه: Malekhoseini.r@iau.ac.ir

چکیده

اینترنت اشیا (IoT) با فراهم‌کردن بستری برای ارتباط خودکار میان میلیون‌ها دستگاه هوشمند، به یکی از زیرساخت‌های حیاتی دنیای مدرن تبدیل شده است. رشد چشمگیر تعداد این دستگاه‌ها و افزایش ویژگی‌هایی مانند تنوع، مقیاس‌پذیری و تحرک‌پذیری آن‌ها، تهدیدات امنیتی را نیز به طور قابل‌توجهی گسترش داده است. به‌ویژه ظهور تهدیدات پنهان و پیچیده که از طریق الگوهای رفتاری غیرمعمول در شبکه بروز می‌کنند، ضرورت بهره‌گیری از روش‌های پیشرفته تشخیص ناهنجاری را دوچندان کرده است.در این مقاله، مدلی نوین مبتنی بر یادگیری گروهی ارائه شده است که با ترکیب تکنیک‌های یادگیری عمیق و الگوریتم‌های یادگیری ماشین، عملکرد تشخیص ناهنجاری‌ها در اینترنت اشیا را بهبود می‌بخشد. پس از انجام فرایند پیش‌پردازش داده‌ها، ویژگی‌های کلیدی با استفاده از رمزگذار خودکار پشته‌ای (SAE) و رمزگذار خودکار عمیق (DAE) استخراج و در مرحله بعد چارچوب یادگیری گروهی متشکل از درخت تصمیم(DT) ، پرسپترون چندلایه(MLP) ، شبکه عصبی احتمالی (PNN) و نسخه وزنی آن (WPNN) برای شناسایی ناهنجاری‌ها به‌کار گرفته شده است.از نوآوری‌های این تحقیق می‌توان به طراحی سازوکار انتخاب پویای ویژگی در لایه رمزگذار و همچنین پیشنهاد طرح وزن‌دهی تطبیقی برای ترکیب خروجی مدل‌های گروهی اشاره کرد که منجر به بهبود دقت در تشخیص حملات ناشناخته و کاهش نرخ مثبت کاذب شده است.مدل پیشنهادی بر روی چندین مجموعه‌داده معتبر از جمله NSL-KDD ، BoT-IoT، IoT-NI، IoT-23 ارزیابی و نتایج نشان‌دهنده دقت بالای ۹۹,۳٪ و امتیاز F1 معادل ۹۹,۲٪ در مجموعه‌داده ترکیبی IoT-DS2 است. نرخ مثبت کاذب (FPR) در اغلب مجموعه‌داده‌ها زیر ۲٪ و نرخ منفی کاذب (FNR) کمتر از ۱,۵٪ گزارش شده است. در مقایسه با مدل‌های منتخب مدل پیشنهادی در شناسایی حملات ناشناخته برتری دارد.

مشخصات مقاله

تاریخچه مقاله:
نوع مقاله: علمی پژوهشی
دریافت۱۴۰۴/۰۷/۱۷
بازنگری: ۱۴۰۴/۰۹/۰۳
پذیرش: ۱۴۰۴/۰۹/۱۵
ارائه آنلاین: ۱۴۰۴/۱۰/۰۷

کلید واژه ها:
اینترنت اشیا
تشخیص ناهنجاری
رمزگذار خودکار پشته‌ای
رمزگذار عمیق
یادگیری گروهی
انتخاب پویای ویژگی
ترکیب تطبیقی مدل‌ها
امنیت سایبری

۱- .**استناد:**ترازو دار، هادی، باقری فرد، کرم اله، نجاتیان، صمد، پروین، حمید، ملک حسینی، راضیه. ارائه مدل ترکیبی و هوشمند برای تشخیص ناهنجاری در اینترنت اشیا با رویکرد یادگیری گروهی و رمزگذارهای عمیق، پدافند الکترونیک وسایبری.(۱۴۰۴)؛۱۳ (۴): ۹۵-۷۳
.DOR:https://doi.org/10.47176/ECDJ.2025.1669

ناشر: دانشگاه جامع امام حسین(ع).

۱-مقدمه

گسترش شتابان اینترنت، زمینه‌ساز توسعه فراگیر اینترنت اشیا (IoT)[1] شده است. سهولت دسترسی، هزینه پایین، و نقش مؤثر این فناوری در زندگی روزمره انسان‌ها از جمله عوامل کلیدی در توسعه آن به‌شمار می‌روند. هم‌زمان، پیشرفت در فناوری‌های بی‌سیم امکان طراحی گره‌های هوشمند کم‌هزینه را فراهم کرده که قادر به جمع‌آوری، تحلیل و انتقال داده‌ها به‌صورت بی‌سیم هستند [۱].

اینترنت اشیا شامل مجموعه‌ای گسترده از دستگاه‌های هوشمند است که توانایی حس‌کردن شرایط محیطی، پردازش اطلاعات، ذخیره‌سازی داده‌ها و برقراری ارتباط با سایر سامانه‌ها را دارا هستند. کاربرد گسترده این فناوری در حوزه‌هایی نظیر صنعت، حمل‌ونقل، خانه‌های هوشمند، سلامت، کشاورزی و پایش محیط‌زیست، منجر به ارتقا کیفیت خدمات و افزایش بهره‌وری شده است [۲]. با این وجود، زیرساخت‌ها و خدمات IoT به دلیل محدودیت منابع، ناهمگونی دستگاه‌ها و استفاده از پروتکل‌های نوظهور، با چالش‌های امنیتی گسترده‌ای روبرو هستند [۳].

ساختار اینترنت اشیا معمولاً بر اساس معماری‌های چندلایه طراحی می‌شود که شامل لایه‌های ادراک، شبکه، پردازش، کاربرد و کسب‌وکار است [۴]. این معماری مدیریت مؤلفه‌ها را تسهیل می‌کند، اما پیچیدگی ارتباطات، تنوع تجهیزات و نبود استانداردهای جامع، زمینه‌ساز تهدیدات امنیتی متنوعی شده است. به‌ویژه در بستر اینترنت اشیای صنعتی(IIoT)[2] که داده‌ها حساس بوده و زمان پاسخ‌دهی از اهمیت بالایی برخوردار است، امنیت یکی از چالش‌های اساسی به شمار می‌آید[۵].

یکی از راهکارهای متداول برای مقابله با تهدیدات امنیتی، استفاده از سیستم‌های تشخیص نفوذ (IDS) [3] است این سیستم‌ها با تحلیل ترافیک شبکه و شناسایی رفتارهای غیرعادی، تلاش می‌کنند حملات را در مراحل اولیه شناسایی کنند. بااین‌حال، مدل‌های سنتی IDS که مبتنی بر امضا یا قوانین ثابت هستند، در شناسایی حملات پنهان، ناشناخته یا با نرخ تکرار پایین، عملکرد مطلوبی ندارد [۶].

در سال‌های اخیر، یادگیری ماشین[4] و به‌ویژه یادگیری عمیق[5] ، به ابزارهایی نویدبخش در این زمینه تبدیل شده‌اند. مدل‌های سنتی یادگیری ماشین، گرچه سبک‌ترند، اما به ویژگی‌های استخراج‌شده به‌صورت دستی وابسته‌اند و در شناسایی الگوهای پیچیده دچار ضعف‌اند مدل‌های یادگیری عمیق قادرند الگوهای پیچیده رفتاری را در داده‌های حجیم و غیرخطی استخراج کنند [۷، ۸]؛ اما چالش‌هایی مانند نیاز به داده‌های زیاد، زمان آموزش طولانی، وابستگی به منابع محاسباتی بالا، و نرخ هشدار کاذب همچنان مانع کاربرد گسترده آن‌ها در محیط‌های IoT شده‌اند. افزون بر آن، ساختار نامتوازن داده‌ها (تعداد کم نمونه‌های حمله نسبت به رفتارهای عادی)، نویز ذاتی در داده‌های حسگر و پویایی ترافیک شبکه، دقت سیستم‌های تشخیص ناهنجاری[6] را کاهش می‌دهند از سوی دیگر، پژوهش‌های اخیر نشان داده‌اند که ترکیب چند مدل در قالب یادگیری گروهی[7] می‌تواند به بهبود دقت و پایداری تشخیص کمک کند[۹]. اما در بسیاری از رویکردهای موجود، سازوکار مؤثری برای انتخاب خودکار ویژگی‌های کلیدی یا تعیین وزن مناسب برای خروجی مدل‌ها در نظر گرفته نشده است.پژوهش حاضر با هدف پاسخ به چالش‌های فوق، یک چارچوب هوشمند تشخیص ناهنجاری مبتنی بر رمزگذارهای عمیق و یادگیری گروهی ارائه می‌دهد. نوآوری این مدل در سه محور اصلی قابل بیان است :

۱. استفاده هم‌زمان از دو نوع رمزگذار خودکار پشته‌ای(SAE) [8] و عمیق (DAE)[9] جهت استخراج ویژگی‌های غیرخطی، فشرده و مقاوم به نویز، در کنار طراحی سازوکاری برای انتخاب پویای ویژگی‌ها بر اساس تحلیل ضرایب فعال‌سازی در لایه‌های میانی رمزگذارها،
۲. به‌کارگیری ترکیب تطبیقی وزنی خروجی چهار مدل یادگیری شامل درخت تصمیم(DT)[10] ، پرسپترون چندلایه(MLP)[11] ، شبکه عصبی احتمالی (PNN)[12] و نوع وزنی آن (WPNN)[13] باهدف کاهش نرخ هشدار کاذب و افزایش دقت در تشخیص حملات ناشناخته.

[1] Internet of Things
[2] Industrial Internet of Things
[3] Intrusion Detection System
[4] Machine Learning
[5] Deep Learning
[6] Anomaly Detection
[7] Ensemble Learning
[8] Stacked autoencoder network
[9] Deep autoencoder network
[10] Decision Trees
[11] Multilayer perceptron
[12] Probabilistic Neural Network
[13] weighted PNN

چارچوب پیشنهادی با درنظرگرفتن محدودیت‌های منابع در محیط‌هایIoT ، و تمرکز بر ویژگی‌های حیاتی ترافیک شبکه طراحی شده است. عملکرد مدل با استفاده از مجموعه‌داده‌های معتبرNSL-KDD ، BoT-IoT، IoT-23، IoT-NI، MQTT، MQTTsetو IoT-DS2 ارزیابی شده و نتایج حاکی از برتری قابل‌توجه آن نسبت به روش‌های مرجع موجود است. از جمله مهم‌ترین حملاتی که در این مقاله مورد بررسی قرار گرفته‌اند می‌توان به حملاتDDoS ، DoS، اسکن پورت(Port Scan) ، نفوذ مبتنی بر پروتکلMQTT ، حملات بات‌نت (مانند Mirai وToriiی) ،حملات مهندسی اجتماعی، سرقت داده (Data Theft) **و** حملات فرمان و کنترل (C&C) اشاره کرد .

ساختار مقاله به شرح زیر تنظیم شده است: در بخش دوم، مروری بر تحقیقات مرتبط ارائه شده است. بخش سوم به پیش‌پردازش داده‌ها، استخراج ویژگی‌ها با رمزگذارهای خودکار، و طراحی مدل یادگیری گروهی می‌پردازد. در بخش چهارم مجموعه‌داده‌ها معرفی شده‌اند، بخش پنجم شامل تحلیل تجربی و نتایج آزمایش‌ها است، و نهایتاً بخش ششم به نتیجه‌گیری و پیشنهادهای آتی اختصاص دارد.

۲-کارهای مرتبط

در سال‌های اخیر، انواع مختلفی از رویکردهای مبتنی بر یادگیری گروه به‌منظور تشخیص ناهنجاری‌ها در IoT در ادبیات پژوهشی ارائه شده‌اند.

مدلی با نام ELBA-IoT برای شناسایی حملات بات‌نت در شبکه‌های IoT معرفی شده است که از ویژگی‌های رفتاری ترافیک شبکه استفاده کرده و با بهره‌گیری از یادگیری گروهی، قادر به تشخیص ترافیک غیرعادی از دستگاه‌های آسیب‌پذیر IoT است. در این رویکرد، سه تکنیک مختلف یادگیری ماشین بر پایه درخت تصمیم (شاملAdaBoost ، RUSBoostو Bagging) مورد ارزیابی قرار گرفته‌اند [۱۰].

در مطالعه‌ای دیگر [۱۱]، یک رویکرد گروهی مبتنی بر Stacking برای تشخیص ناهنجاری‌های شبکه‌های IoT پیشنهاد شده است. در این مدل، از ترکیب شبکه عصبی کانولوشنی (CNN)[14] و شبکه عصبی بازگشتی (RNN)[15] به‌عنوان یادگیرنده‌های پایه استفاده شده است. مزیت این روش، استفاده از داده‌های واقعی و ناهمگون است، که می‌تواند چالش‌های موجود در مجموعه‌داده‌های کوچک‌تر را کاهش دهد و بستر آموزشی مناسبی فراهم کند. خان و همکاران [۱۲] رویکردی بر مبنای گروهی از مدل‌های LSTM ارائه کرده‌اند. آن‌ها از درخت تصمیم برای تجمیع خروجی مدل‌ها استفاده کرده و الگوریتم پیشنهادی را بر روی مجموعه‌داده ToN_IoT و در زمینه اینترنت اشیا پزشکی (IoMT)[16] به‌کار برده‌اند.

آلوتایبی و الیاس [۱۳] نیز رویکردی گروهی مبتنی بر stacking پیشنهاد کردند که در آن جنگل تصادفی (RF)[17]، DT، رگرسیون لجستیک (LR)[18] و k-نزدیک‌ترین همسایه (KNN)[19] به‌عنوان یادگیرنده پایه و LR به‌عنوان مدل نهایی تجمیع به‌کاررفته است.

گاد و همکاران [۱۴] از الگوریتم XGBoostبرای شناسایی ناهنجاری‌ها در شبکه‌های IoT استفاده کرده‌اند. این مطالعه با بهره‌گیری از سه زیرمجموعه از چهار نسخه مجموعه‌داده ToN_IoT و در دو سناریوی طبقه‌بندی باینری و چند کلاسه، عملکرد موفقی را گزارش می‌دهد.

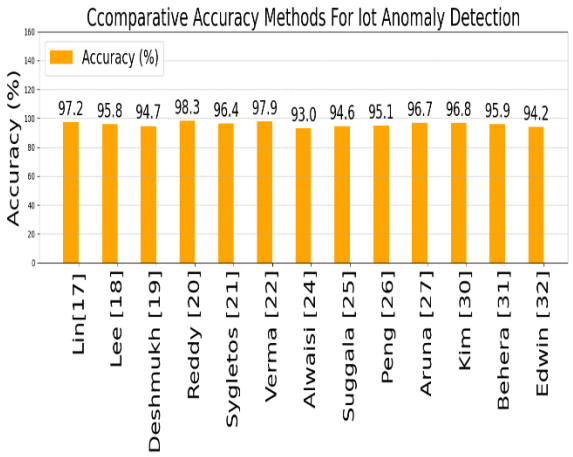
در مطالعه‌ای دیگر [۱۵]، چندین الگوریتم یادگیری گروهی مانند XGBoost، Adaboost، Bagging، RFو Extra Trees برای تشخیص نفوذ در اینترنت اشیای صنعتی (IIoT) و با استفاده از مجموعه‌داده ToN_IoT Telemetry مورد بررسی قرار گرفته‌اند. بر اساس نتایج، XGBoostدر هر دو نوع طبقه‌بندی، بهترین عملکرد را ارائه داده است،

در حوزه سیستم‌های کنترل صنعتی(SCADA) ، مطالعه [۱۶] چارچوبی مبتنی بر یادگیری گروهی با استفاده از مجموعه‌ای از شبکه‌های باور عمیق (DBN)[20] ا ارائه کرده که نتایج امیدبخشی را در تشخیص ناهنجاری‌ها نشان می‌دهد.

در شکل ۱، دقت مدل‌های نوین ترکیبی مبتنی بر رمزگذارهای خودکار عمیق و یادگیری گروهی برای تشخیص ناهنجاری در شبکه‌های اینترنت اشیا بین سال‌های ۲۰۲۳ تا ۲۰۲۵ مقایسه شده است. نتایج نشان می‌دهد که مدل‌های پیشنهادی در سال‌های اخیر پیشرفت‌های قابل ملاحظه‌ای داشته‌اند، به‌ویژه از نظر دقت، کاهش نرخ خطا و بهبود عملکرد کلی در تشخیص ناهنجاری‌ها.

[14] Convolutional Neural Network
[15] Recurrent Neural Networks

[16] Internet of Medical Things
[17] Random Forest
[18] Logistic Regression
[19] k-Nearest Neighbors
[20] Deep Belief Networks



شکل ۱: مقایسه دقت مدل‌های نوین تشخیص ناهنجاری در iot

به‌منظور تحلیل و مقایسه مدل‌های نوین ترکیبی مبتنی بر رمزگذارهای خودکار عمیق و الگوریتم‌های یادگیری گروهی در حوزه تشخیص ناهنجاری در اینترنت اشیا، جدول ۱ به بررسی ساختار، مجموعه‌داده، دقت عملکرد و ویژگی‌های کلیدی ۱۹ پژوهش اخیر طی سال‌های ۲۰۲۳ تا ۲۰۲۵ پرداخته است.

جدول ۱: مقایسه مدل‌های تشخیص ناهنجاری در اینترنت اشیا

نویسنده (سال)	مدل معماری	نوع داده	دقت (%)
لین و همکاران (۲۰۲۵) [۱۷]	AE+ ML Ensemble	ICS	97.2
لی و همکاران (۲۰۲۵) [۱۸]	FL Lightweight	IIoT	95.8
دشموخ و همکاران (۲۰۲۵) [۱۹]	Federated DL	IoT+Finance	94.7
ردی و همکاران (۲۰۲۵) [۲۰]	Graph-ResNet + Hawk-Bee	IoT Wireless	98.3
سیگلتوس و همکاران (۲۰۲۵) [۲۱]	CNN Hybrid	IoT General	96.4
ورما و همکاران (۲۰۲۵) [۲۲]	Ensemble + EO	IIoT	97.9
علی و همکاران (۲۰۲۵) [۲۳]	DPS-DL	IoT	91.7
الویسی(۲۰۲۵) [۲۴]	CNN Lite	6G-IoT	93.0
سوگولا و همکاران (۲۰۲۵) [۲۵]	GANN + Blockchain	SmartGrid	94.6
پنگ و همکاران (۲۰۲۵) [۲۶]	Adversarial CNN	Industrial IoT	95.1
اوئرا (۲۰۲۵) [۲۷]	AE + LSTM+CNN	IoT Time Series	96.7
ماشالی (۲۰۲۵) [۲۸]	Hybrid AE + Ensemble	BoT-IoT	97.5
لی (۲۰۲۵) [۲۹]	Masked AE	Industrial IoT	96.8
کیم (۲۰۲۵) [۳۰]	MTD-AD (AE+Defense)	Smart Grid	95.9
بحارا (۲۰۲۵) [۳۱]	AE+Classifier	Pumping IoT	94.2
ادوین (۲۰۲۵) [۳۲]	AE +BiGRU+DBN+ Walrus	BoT-IoT	98.1
یان (۲۰۲۵) [۳۳]	Autoencoder Ensemble	IoT Malware	97.6
فان (۲۰۲۵) [۳۴]	Rule-extracted AE	Smart City	94.9
سارانیا (۲۰۲۵) [۳۵]	Multilayer AE	Cross-layer IoT	95.2
نایت (۲۰۲۵) [۳۶]	DASVDD	Smart Cities	96.3
کومار (۲۰۲۵) [۳۷]	Graph AE	Finance IoT	93.8
بزنجانی (۲۰۲۳) [۳۸]	Conv-AE + Blockchain	Healthcare IoT	96.0

وو و همکاران [۳۹] یک چارچوب تشخیص ناهنجاری تطبیقی به نام AEWAE [۲۱] را معرفی کردند که از چهار الگوریتم یادگیری آنلاین در قالب یک ساختار یادگیری گروهی ترکیبی بهره می‌برد. این چارچوب شامل سه مرحله اصلی است: پیش‌پردازش داده‌های IoT، یادگیری مدل پایه، و ادغام آنلاین مدل‌ها. برای تنظیم بهینه وزن‌ها در فرآیند ترکیب، از الگوریتم بهینه‌سازی ازدحام ذرات (PSO) استفاده شده است. نتایج تجربی در محیط‌های پویا و داده‌های بلادرنگ نشان می‌دهد که AEWAE عملکرد پایداری در تشخیص ناهنجاری دارد و نسبت به روش‌های منفرد دقت بالاتری ارائه می‌دهد.

عبدالله و همکاران [۴۰] یک مدل تشخیص نفوذ در حوزه اینترنت اشیای پزشکی (IoMT) ارائه دادند که مبتنی بر یادگیری گروهی چندمدلی و تمرکز بر شناسایی تهدیدات وب است. آن‌ها با استفاده از ویژگی‌هایی نظیرIP ، اندازه بسته و نوع پروتکل، داده‌های ترافیک شبکه را تجزیه‌وتحلیل کرده و از طبقه‌بندهایی همچون XGBoost، KNN، درخت تصمیم، جنگل تصادفی و AdaBoost برای ترکیب و طبقه‌بندی بهره بردند.

[21] Adaptive Exponentially Weighted Average Ensemble

نتایاگابیری **و** همکاران [۴۱] یک رویکرد یادگیری گروهی جدید با نام OMICمعرفی کردند که یک طبقه‌بندی‌کننده نفوذ چندکلاسی بهینه‌شده برای تشخیص ناهنجاری در مقیاس بزرگ در محیط‌های IoT است. این مدل از ترکیب LightGBM و XGBoost در یک خط لوله پردازش حافظه‌محور استفاده می‌کند و با به‌کارگیری روش‌هایی مانند نمونه‌برداری تطبیقی، یادگیری حساس به هزینه، و پردازش تکه‌ای پویا، چالش‌های عدم‌تعادل کلاس و مقیاس‌پذیری را هدف قرار می‌دهد.

رحمان و همکاران [۴۲] یک سیستم تشخیص نفوذ مبتنی بر یادگیری گروهی Stacking به نام SIDS-Stacked معرفی کردند که با بهره‌گیری از رویکرد مبتنی بر Stacked، دقت و انعطاف‌پذیری سیستم‌های IDS را در شبکه‌های SDN افزایش می‌دهد. آن‌ها از ترکیب چند الگوریتم یادگیری از جمله نزول گرادیان تصادفی، رگرسیون لجستیک، جنگل تصادفی، و شبکه‌های عصبی عمیق (DNN) برای ایجاد یک مدل چندلایه استفاده کردند.

تانور و همکاران [۴۳] مدل LightEnsemble-Guard را برای تشخیص ناهنجاری در دستگاه‌های IoT بلادرنگ با منابع محدود پیشنهاد کردند. این مدل یک چارچوب یادگیری گروهی سبک‌وزن است که از سه طبقه‌بندLightGBM ، XGBoostو Extra Trees **با** رأی‌گیری اکثریت استفاده می‌کند. این چارچوب، با توازن دقیق بین دقت و کارایی، پاسخی عملی و مقیاس‌پذیر برای امنیت بلادرنگ در محیط‌های IoT با محدودیت منابع ارائه می‌دهد و از بسیاری از مدل‌های سنتی پیشی گرفته است.

دهدشتی فرد و همکاران [۴۴] یک مدل یادگیری گروهی ترکیبی برای تشخیص ناهنجاری در شبکه‌های بی‌سیم مبتنی بر استاندارد IEEE 802.11 ارائه کردند. در این مدل با ادغام قابلیت‌های شبکه عصبی عمیق(DNN)[۲۲] ، جنگل تصادفی، XGBoost و LightGBM و استفاده از رگرسیون لجستیک **به** عنوان متا-طبقه‌بند، دقت عملکرد تشخیص بهبود یافته است.

در سایر پژوهش‌ها نیز مانند [۴۵] ، [۴۶] ، [۴۷] و[۴۸] به این موضوع پرداخته شده است.

با وجود عملکرد قابل‌توجه بسیاری از مدل‌های پیشین، بیشتر آن‌ها فاقد سازوکار انتخاب پویای ویژگی و ترکیب تطبیقی مدل‌ها هستند. برخلاف آن‌ها، مدل پیشنهادی ما با ادغام دو رمزگذار عمیق و بهره‌گیری از یادگیرنده‌های متنوع با وزن‌دهی هوشمند، توانسته دقت و پایداری بالاتری ارائه دهد. همچنین، برخلاف روش‌هایی مانند[۱۷] AE+ML Ensemble یا[۲۱] CNN Hybridکه با نرخ هشدار کاذب بالا یا نیازمندی محاسباتی سنگین مواجه‌اند، چارچوب ما با انتخاب ویژگی‌های بهینه و حذف نویز، نرخ مثبت کاذب را به کمتر از ۲٪ کاهش داده است.

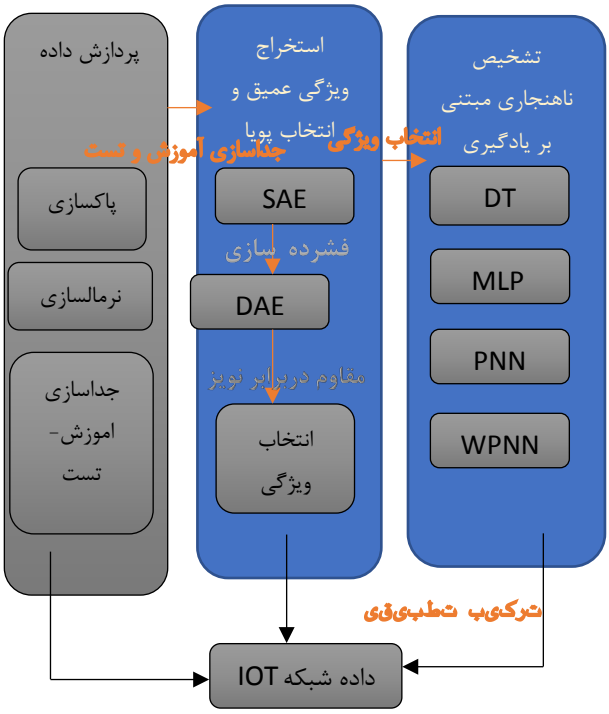
مرور پژوهش‌های اخیر نشان می‌دهد که استفاده از رویکردهای یادگیری گروهی و رمزگذارهای عمیق در تشخیص ناهنجاری در شبکه‌های IoT به نتایج امیدوارکننده‌ای منجر شده است. بااین‌حال، چالش‌هایی همچون نرخ هشدار کاذب بالا، دشواری در شناسایی حملات ناشناخته، ضعف در مدیریت داده‌های نامتوازن، پیچیدگی ساختار مدل‌ها، وابستگی به تنظیمات دقیق و فقدان سازوکارهای انتخاب ویژگی پویا، همچنان در بسیاری از مدل‌های پیشنهادی مشاهده می‌شود. علاوه بر این، در برخی موارد، محدودیت در تعمیم‌پذیری مدل‌ها به سناریوهای واقعی و متغیر، اثربخشی آن‌ها را کاهش داده است. ازاین‌رو، نیاز به طراحی چارچوبی هوشمند، سازگار و دقیق که بتواند بر این محدودیت‌ها غلبه کند، به‌شدت احساس می‌شود. پژوهش حاضر باتکیه‌بر این نیاز، چارچوبی ترکیبی مبتنی بر رمزگذارهای عمیق و یادگیری گروهی تطبیقی ارائه می‌دهد که باهدف ارتقای دقت، پایداری و تطبیق‌پذیری در تشخیص ناهنجاری‌های پیچیده در محیط‌های ناهمگون اینترنت اشیا طراحی شده است.

۳- مدل پیشنهادی

مدل پیشنهادی این مقاله باهدف تشخیص ناهنجاری در شبکه‌های اینترنت اشیا، از یک چارچوب چندمرحله‌ای بهره می‌برد که بر پایهٔ ترکیب رمزگذارهای عمیق و الگوریتم‌های یادگیری گروهی طراحی شده است. این چارچوب شامل سه جز اصلی است: (۱)پیش‌پردازش داده‌ها، (۲) استخراج و انتخاب پویای ویژگی‌های عمیق و (۳) شناسایی ناهنجاری با بهره‌گیری از گروهی از یادگیرنده‌های متنوع و یک مکانیزم وزن‌دهی تطبیقی.

نوآوری روش پیشنهادی در سه سطح قابل‌توجه است: نخست، طراحی مکانیزم انتخاب پویای ویژگی‌ها در لایه‌های میانی رمزگذار عمیق که موجب حذف ویژگی‌های غیرمؤثر و افزایش دقت نهایی مدل می‌گردد. دوم، پیشنهاد یک سازوکار ترکیب تطبیقی وزن‌ها در چارچوب یادگیری گروهی که بر اساس ارزیابی اعتماد هر الگوریتم، خروجی مدل‌ها را بادقت بالا تلفیق می‌کند. سوم، تجمیع رمزگذارهای خودکار عمیق و گروهی از یادگیرنده-های متنوع به‌خصوص wpnn در یک ساختار یکپارچه، که باعث افزایش تاب‌آوری مدل در برابر داده‌های نویزی و ناهنجاری‌های پیچیده می‌شود. معماری کلی روش پیشنهادی در شکل ۲ به‌صورت شماتیک نمایش‌داده‌شده است.

[22] Deep neural networks



شکل ۲: معماری روش پیشنهادی

۳-۱-پیش‌پردازش داده‌ها

نخستین مرحله به پاک‌سازی[۲۳] و نرمال‌سازی[۲۴] داده‌ها اختصاص دارد. در این مرحله، داده‌های تکراری و نامعتبر از جریان ورودی حذف شده، مقادیر عددی به‌منظور هم‌ترازی ویژگی‌ها، مقیاس‌گذاری می‌شوند، و مقادیر گمشده[۲۵] یا نویزی[۲۶] اصلاح می‌گردند. سپس داده‌ها به‌صورت ساختارمند به دو بخش آموزش و آزمایش تفکیک می‌شوند تا زمینه لازم برای پردازش مدل فراهم گردد.

۳-۲- استخراج و نمایش ویژگی‌ها

در گام دوم، هدف مدل کاهش ابعاد داده و تمرکز بر ویژگی‌هایی است که بیشترین نقش را در تفکیک رفتارهای عادی از ناهنجار دارند در این مرحله، از یک سازوکار انتخاب پویای ویژگی نیز استفاده شده است که با تحلیل تدریجی ضرایب فعال‌سازی در لایه‌های میانی رمزگذار، ویژگی‌های کم‌اهمیت را حذف و درعین‌حال وزن‌دهی مجدد به بردار ویژگی را انجام می‌دهد. این فرایند باعث کاهش سربار محاسباتی و بهبود دقت در مرحله بعدی می‌شود. شبه‌کد مربوط به فرایند استخراج ویژگی‌ها در الگوریتم ارائه شده است.

Algorithm 1: Feature Extraction with Deep Autoencoders and Dynamic Feature Selection
Input: Raw network data
Output: Optimized feature vector

1: function $Feature\_Extraction(input\_path)$
2: $raw\_data \leftarrow LoadData(input\_path)$
3: $preprocessed\_data \leftarrow Preprocess(raw\_data)$
4:
5: # SAE for hierarchical feature extraction
6:
$features\_SAE \leftarrow SAE\_Encoder(preprocessed\_data)$
7:
8: # DAE for robust compressed representation
9: $features\_DAE \leftarrow DAE\_Encoder(features\_SAE)$
10:
11: # Dynamic feature selection based on activation weights
12:
$optimized\_features \leftarrow Dynamic\_Feature\_Selector(features\_DAE)$
13:
14: return $optimized\_features$
15: end function

16: function SAE_Encoder(input)
17: train SAE model with multiple hidden layers
18:
$features \leftarrow forward\_pass\ through\ trained\ SAE$
19: return $features$
20: end function

21: function $DAE\_Encoder(input)$
22: train DAE model with noise-injected input
23:
$features \leftarrow compressed\_output\ from\ trained\ DAE$
24: return $features$
25: end function

26: function $Dynamic\_Feature\_Selector(features)$
27: for each feature F_i in features do
28:
$activation\_weight \leftarrow compute\_activation(F_i)$
29: if $activation\_weight < threshold$ then
30: remove F_i from $features$
31: end if
32: end for
33: return $filtered\_features$
34: end function

برای نمایش بهینه و خودکار ویژگی‌ها در داده‌های IOT، از ساختارهای رمزگذار خودکار و نمایش ویژگی عمیق مبتنی بر نگاشت‌های غیرخطی استفاده شده است. این ساختار پیش از تغذیه داده‌ها به مدل یادگیری، ویژگی‌های کلیدی را استخراج و بازنمایی می‌کند. در این مرحله، از ویژگی‌های قانونی[۲۷] و

[23] Cleaning
[24] Normalization
[25] Missing Values
[26] Noise
[27] Legitimate

ناهنجار[۲۸] جهت آموزش مدل تشخیص ناهنجاری استفاده می‌گردد.

فرض کنید مجموعه‌داده‌های ورودی به‌صورت $X_n = \{x_1 . x_2 . \dots . x_n\} . X_n \in \mathbb{R}^n$ باشد و همچنین بردار خروجی بازسازی‌شده به‌صورت $X_n^{'} = \{x_1^{'} . x_2^{'} . \dots . x_n^{'}\}$ در نظر گرفته شود. حال، مجموعه ویژگی‌ها با $F_n = \{f_1 . f_2 . \dots . f_n\}$ و لایه‌های پنهان شبکه با h_n نمایش داده می‌شوند.

رمزگذار خودکار نوعی شبکه عصبی چندلایه است که از دو بخش اصلی تشکیل شده است: رمزگذار[۲۹] و رمزگشا[۳۰]. هدف این شبکه، فشرده‌سازی داده ورودی و بازسازی آن با کمترین میزان خطا است. ساختار رمزگذار به‌صورت رابطه (۱) تعریف می‌شود:

$$E_n = f(W_1 X_n + b_1) \quad (1)$$

که در آن f تابع فعال‌سازی رمزگذار، W_1 ماتریس وزن، و b_1 بردار بایاس است. به‌طور مشابه، رمزگشا خروجی را از طریق رابطه (۲) بازسازی می‌کند:

$$X_n^{'} = g(W_2 h_n + b_2) \quad (2)$$

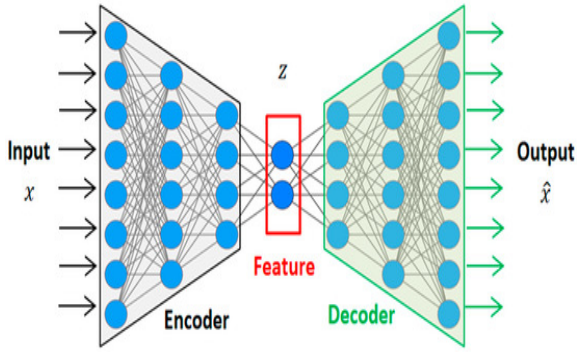
که g تابع فعال‌سازی رمزگشا، W_2 وزن‌های لایه خروجی، و b_2 بایاس متناظر است .

هر یک از پارامترهای مدل رمزگذار خودکار، به‌گونه‌ای بهینه‌سازی می‌شوند که خطای بازسازی بین ورودی و خروجی، حداقل شود. در این مقاله، دو نوع رمزگذار برای استخراج و نمایش ویژگی‌ها به‌کارگرفته‌شده است:

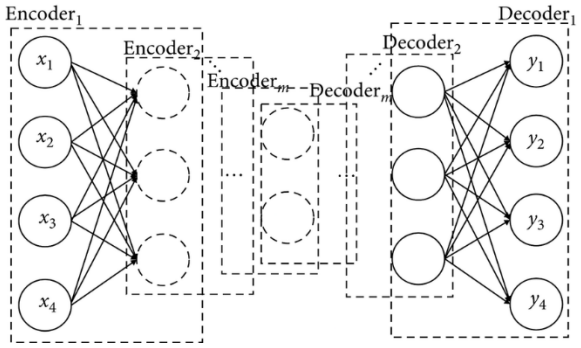
- رمزگذار خودکار پشته‌ای (SAE): با یادگیری سلسله‌مراتبی از داده‌های خام، ویژگی‌های فشرده‌شده‌ای تولید می‌کند که در لایه‌های بعدی به‌عنوان ورودی استفاده می‌شوند.
- رمزگذار خودکار عمیق (DAE): با دارابودن چندین لایه پنهان، قابلیت نمایش پیچیده‌تری از داده‌ها را فراهم می‌کند و مقاوم‌سازی در برابر نویز را ممکن می‌سازد.

مزیت اصلی رمزگذارهای عمیق، توانایی در استخراج نمایش‌های سطح بالا و انتزاعی از داده‌ها است که در بهبود عملکرد مدل‌های تشخیص ناهنجاری نقش مهمی ایفا می‌کند.

همان‌طور که در شکل ۳ نشان داده شده، ساختار رمزگذار خودکار عمیق شامل چندین لایه فشرده‌سازی و بازسازی است. همچنین در شکل ۴ ساختار رمزگذار پشته‌ای ترسیم شده است که در آن هر لایه به‌صورت تدریجی ویژگی‌های ورودی را فشرده‌سازی کرده و به لایه بعد منتقل می‌کند. در این رمزگذارها، نوع کم‌کامل[۳۱] مورد استفاده قرار گرفته است؛ به‌طوری‌که تعداد نرون‌های لایه‌های پنهان کمتر از ورودی بوده و در نتیجه، شبکه مجبور به یادگیری نمایش‌های کلیدی‌تر از داده‌ها می‌شود.



شکل ۳: رمزگذاری خودکار عمیق[۴۹]



شکل ۴: رمزگذاری خودکار پشته‌ای[۵۰]

در این پژوهش، رمزگذارهای SAE و DAE برای استخراج ویژگی‌های کلیدی و کاهش ابعاد داده به کار گرفته شده‌اند . SAE با یادگیری سلسله‌مراتبی، الگوهای رفتاری شبکه را به‌خوبی مدل‌سازی می‌کند و DAE با حذف نویز، بازنمایی فشرده و مؤثری از داده‌ها ارائه می‌دهد. همچنین، با استفاده از سازوکار انتخاب پویای ویژگی، ویژگی‌های کم‌اهمیت حذف و ویژگی‌های مؤثر تقویت می‌شوند. این ترکیب باعث بهبود دقت، کاهش هشدارهای کاذب و افزایش توان شناسایی حملات ناشناخته در مدل تشخیص نفوذ می‌شود.

[28] Anomal
[29] Encoder
[30] Decoder
[31] Undercomplete

مکانیزم انتخاب پویای ویژگی مبتنی بر تحلیل ضرایب فعال‌سازی در لایه‌های میانی رمزگذار طراحی شده است. پس از استخراج بردار ویژگی فشرده‌شده از طریق رمزگذارهای SAE وDAE ، میزان فعال‌سازی هر نرون (ویژگی) در طول کل داده‌های آموزشی محاسبه می‌شود. اگر میانگین فعال‌سازی یک ویژگی از آستانه مشخصی کمتر باشد، آن ویژگی به‌عنوان ویژگی کم‌اهمیت شناخته شده و حذف می‌گردد. این آستانه به‌صورت تجربی و با تحلیل توزیع فعال‌سازی‌ها تنظیم می‌شود.

این فرایند به‌صورت کاملاً پویا و تطبیقی انجام می‌شود و در هر نوبت آموزش، ویژگی‌های مؤثر به‌صورت خودکار تقویت و ویژگی‌های کم‌اثر حذف می‌شوند. در نتیجه، این روش برخلاف روش‌های ایستا مانند تحلیل مؤلفه‌های اصلی(PCA)[۳۲] ، اطلاعات متقابل (MI)[۳۳] و الگوریتم‌های درخت تصمیم با ساختار شبکه عمیق کاملاً یکپارچه بوده و بدون نیاز به اجرای جداگانه عمل می‌کند. مقایسه روش پیشنهادی با روش‌های ذکرشده نشان داد که استفاده از انتخاب پویای ویژگی، باعث افزایش دقت شناسایی ناهنجاری، کاهش نرخ هشدارهای کاذب و بهبود پایداری مدل در مواجهه با داده‌های نویزی شده است. جدول ۲ این مقایسه را نشان می‌دهد.

جدول ۲: مقایسه روش پیشنهادی و روش‌های انتخاب ویژگی

معیار مقایسه	روش پیشنهادی	PCA	اطلاعات متقابل (MI)	مبتنی بر درخت تصمیم
نوع روش	پویا، درون-مدلی، وابسته به شبکه	آماری، ایستا	آماری، ایستا	یادگیری‌محور، برون‌مدلی
تطبیق با داده	بله	خیر	خیر	محدود
جداسازی قبل از آموزش	ندارد	دارد	دارد	دارد
یکپارچگی با شبکه عصبی عمیق	کامل	ندارد	ندارد	ندارد
حذف ویژگی نویز و کم‌اهمیت	بالا	متوسط	پایین	متوسط
رابطه غیرخطی بین ویژگی	بله	خیر	محدود	نسبتاً
استفاده با داده بزرگ	بالا	بالا	متوسط	متوسط

[32] Principal Component Analysis
[33] Mutual Information

۳-۳-تشخیص ناهنجاری با یادگیری گروهی

پس از تبدیل داده‌های خام به نمایش برداری فشرده، مرحله نهایی شامل فرایند یادگیری و تصمیم‌گیری است. روش تشخیص ناهنجاری پیشنهادی بر مبنای یادگیری گروهی عمیق است که از ترکیب چهار الگوریتم مختلف تشکیل شده است: پرسپترون چندلایه (MLP)، درخت تصمیم (DT)، شبکه عصبی احتمالی (PNN) و شبکه عصبی احتمالی وزنی (WPNN).

خروجی این چهار مدل از طریق یک سازوکار ترکیب تطبیقی ارزیابی می‌شود که وزن هر مدل را بر اساس میزان اعتماد به تصمیم آن با درنظرگرفتن معیارهایی مانند نرخ پیش‌بینی مثبت و صحت طبقه‌بندی تنظیم می‌نماید. این سازوکار وزن‌دهی تطبیقی موجب کاهش نرخ مثبت کاذب (FPR)[۳۴] و افزایش دقت در شناسایی حملات ناشناخته می‌گردد.

۳-۳-۱-پرسپترون چندلایه (MLP)

پرسپترون چندلایه (MLP) نوعی شبکه عصبی مصنوعی است که به طور گسترده‌ای در مسائل طبقه‌بندی به کار گرفته می‌شود. این مدل از یک الگوریتم یادگیری پیش‌خور[۳۵] همراه با پس‌انتشار خطا[۳۶] بهره می‌برد که طی آن، پارامترهای شبکه با استفاده از مشتقات جزئی و روش گرادیان نزولی به‌روزرسانی می‌شوند. در این مقاله، از یک طبقه‌بند MLP شامل سه‌لایه پنهان، هر یک با ۱۰۰ نورون، استفاده شده است. در تمامی لایه‌ها، تابع فعال‌سازی ReLUبه‌صورت $\sigma(z) = \max(0, z)$ به‌کارگرفته‌شده است. برای آموزش مدل، از تابع زیان آنتروپی متقاطع استفاده شده و فرایند بهینه‌سازی با بهره‌گیری از الگوریتم Adam با نرخ یادگیری $\eta = 0.001$ و اندازه دسته برابر با ۶۴ انجام شده است.

۳-۳-۲- درخت تصمیم (DT)

درخت تصمیم، مدلی مبتنی بر ساختار سلسله‌مراتبی و گره محور است که به طور گسترده در مسائل طبقه‌بندی داده‌ها مورداستفاده قرار می‌گیرد. این مدل با تقسیم بازگشتی داده‌ها در هر گره به زیرمجموعه‌های کوچک‌تر، فرایند تصمیم‌گیری را انجام می‌دهد. در هر گره، تقسیم‌بندی بر اساس یک معیار ارزیابی

[34] False Positive Rate
[35] FeedForward
[36] Backpropagation

کیفیت صورت می‌گیرد تا بهترین تفکیک ممکن حاصل شود. در این مقاله، معیار آنتروپی[۳۷] به‌عنوان شاخص اصلی برای ارزیابی کیفیت تقسیم‌بندی انتخاب شده است. گره‌های میانی درخت، وظیفه انجام تصمیم‌گیری مرحله‌به‌مرحله و هدایت نمونه‌ها به سمت برچسب‌های خروجی را بر عهده دارند، درحالی‌که گره‌های برگ نمایانگر نتایج نهایی طبقه‌بندی هستند.

۳-۳-۳- شبکه عصبی احتمالی (PNN)

شبکه عصبی احتمالی(PNN) ، نوعی شبکه عصبی پیش‌خور[۳۸] چندلایه است که از چهارلایه اصلی تشکیل شده است: لایه ورودی، لایه الگو، لایه جمع و لایه خروجی (مطابق با شکل ۳). این شبکه را می‌توان به‌عنوان تعمیمی از تحلیل تشخیص خطی (LDA)[۳۹] در چارچوب تحلیل تشخیص هسته‌ای (KDA)[۴۰] در نظر گرفت. هدف PNN یافتن ترکیب‌های خطی بهینه‌ای از ویژگی‌ها است که بتوانند به طور مؤثری کلاس‌های مختلف را از یکدیگر تفکیک کنند.

در PNN تابع چگالی احتمال پنجره پارزن هر کلاس را با استفاده از نمونه‌های مجموعه آموزشی تخمین می‌زند .هر گره از شبکه، تابع چگالی احتمال را برای ورودیx ، نمونه آموزشی x_i و کلاس c_kمطابق رابطه (۳) محاسبه می‌کند:

$$p(\boldsymbol{x} \mid \boldsymbol{x}_i . C_k) = \frac{1}{\sigma}\omega\left(\frac{\boldsymbol{x}-\boldsymbol{x}_i}{\sigma}\right) \quad (۳)$$

که در آن x_i نمونه iام و x نمونه ورودی ()ωتابع وزن و σ پارامتر هموارسازی است گره‌ها بر اساس کلاس‌های نمونه آموزشی در لایه الگو گروه‌بندی می‌شوند و هر گروه برای لایه بعدی جمع‌بندی می‌شود تا احتمال کلاس را بدست آورد. در لایه جمع، گره-های c_k^{th} مقادیر لایه الگوی کلاس‌های c_k^{th} را جمع می‌کنند. این جمع بر اساس تخمینگر پنجره گاوسی یا پارزن مختلط همانطور که در رابطه (۴) تعریف شده است تخمین زده می‌شود.

$$\hat{f}_{C_k}(\boldsymbol{x}) = \frac{1}{n_{C_k}\sigma}\sum_{i=1}^{n_{C_k}} \omega\left(\frac{\boldsymbol{x}-\boldsymbol{x}_i}{\sigma}\right) \quad (۴)$$

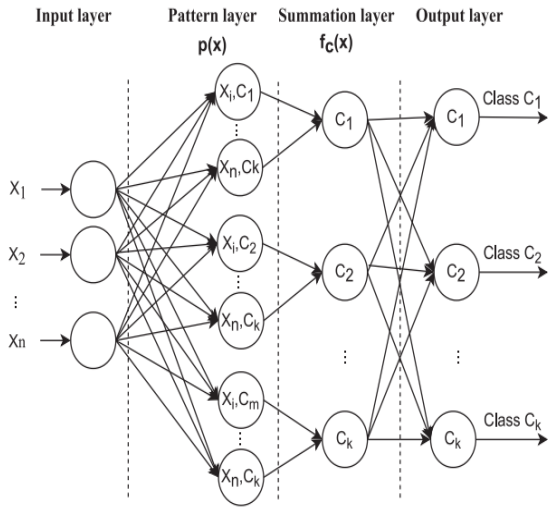
که n_{C_k} تعداد نمونه‌های کلاس C_k است.

بنابراین، لایه جمع به نگاشت نمونه‌های ورودی به کلاس‌های احتمالی می‌پردازد. برای نمونه‌های جدید، تابع چگالی می‌تواند بدون نیاز به آموزش مجدد تخمین زده شود.

تابع وزن $\omega(\cdot)$ معمولاً یک هسته شعاعی پایه (RBF)[۴۱] است که فاصله بین نمونه شناخته‌شده و ورودی ناشناخته را اندازه‌گیری می‌کند. هرچه فاصله کمتر باشد، وزن بیشتری به آن اختصاص می‌یابد.

پارامتر هموارسازی σ پراکندگی RBF را زمانی که به اوج خود در مرکز وزن می‌رسد، تعیین می‌کند.

مزایای PNN شامل حساسیت پایین به داده‌های پرت، قابلیت یادگیری سریع ویژگی‌های جدید و کاهش هزینه بازآموزی در صورت افزایش داده‌های آموزشی است. همچنین، PNN نسبت به شبکه‌های عمیق، عملکرد بهتری با داده‌های آموزشی محدود ارائه می‌دهد و در برابر حملات خصمانه مقاوم‌تر است. شکل ۵ معماری شبکه عصبی احتمالی را نشان می‌دهد.

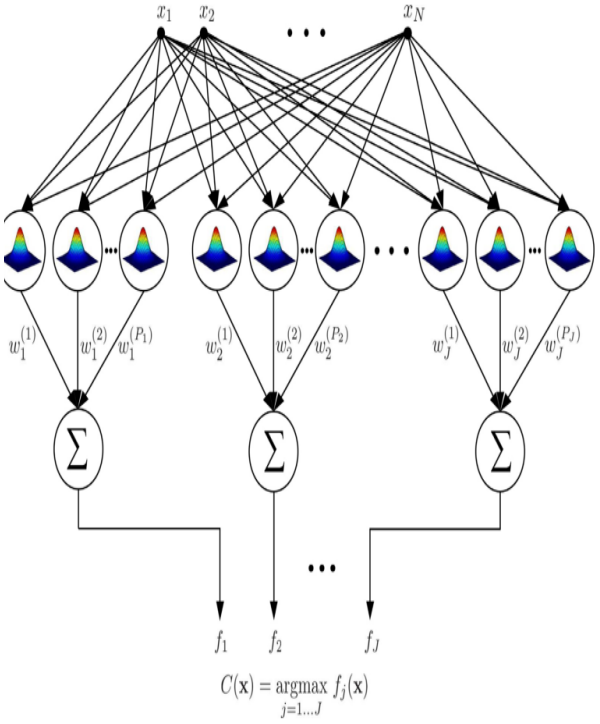


شکل ۵: معماری شبکه عصبی احتمالی (PNN) [۵۱]

۴-۳-۳- شبکه عصبی احتمالی وزنی (WPNN)

شبکه عصبی احتمالی وزنی (WPNN) نسخه توسعه‌یافته‌ای از شبکه PNN است که در آن به هر نمونه آموزشی در لایه الگو وزن خاصی اختصاص داده می‌شود. این وزن‌دهی به‌منظور افزایش دقت طبقه‌بندی و کاهش اثر داده‌های پرت یا نمونه‌های کم‌کیفیت انجام می‌گیرد. شکل ۶ معماری شبکه عصبی احتمالی وزنی را نشان می‌دهد.

[37] Entropy
[38] Feedforward Neural Network
[39] Linear Discriminant Analysis
[40] Kernel Discriminant Analysis
[41] Radial Basis Function



شکل ۶: معماری WPNN [۵۲]

تابع چگالی احتمال شرطی در لایه الگو WPNN به‌صورت رابطه (۵) اصلاح می‌شود:

$$p(\boldsymbol{x} \mid \boldsymbol{x}_i . C_k) = \frac{w_i}{\sigma}\omega\left(\frac{\boldsymbol{x}-\boldsymbol{x}_i}{\sigma}\right) \quad (۵)$$

که در آن w_i وزن اختصاص‌یافته به نمونه $\boldsymbol{x}_i$ است. این وزن‌ها معمولاً بر اساس میزان اهمیت یا قابلیت اعتماد نمونه‌ها تعیین می‌شوند.لایه جمع در WPNN به صورت وزنی در رابطه (۶)، تجمع مقادیر را بر اساس وزن‌ها انجام می‌دهد:

$$\hat{f}_{C_k}(\boldsymbol{x}) = \frac{1}{\sum_{i=1}^{n_{C_k}} w_i \sigma}\sum_{i=1}^{n_{C_k}} w_i \cdot \omega\left(\frac{\boldsymbol{x}-\boldsymbol{x}_i}{\sigma}\right) \quad (۶)$$

که n_{C_k} تعداد نمونه‌های کلاس C_k است. این ساختار اطمینان می‌دهد که نمونه‌هایی با وزن بالاتر تأثیر بیشتری بر تصمیم‌گیری نهایی دارند و به این ترتیب کارایی و دقت مدل افزایش می‌یابد.

با استفاده از تخمین چگالی پنجره‌ای پارزن وزنی در رابطه (۶)، می‌توان تابع چگالی احتمال کلاس C_k را به صورت چندبعدی و ماتریسی بیان کرد:

$$\hat{f}_{C_k}(\boldsymbol{x}) = \frac{1}{\sum_{i=1}^{n_{C_k}} w_i \det(\boldsymbol{H})}\sum_{i=1}^{n_{C_k}} w_i \cdot \frac{1}{s_i^N} k\left(\frac{\left(\boldsymbol{x}-\boldsymbol{x}_i\right)^T \boldsymbol{H}^{-1}}{s_i}\right) \quad (۷)$$

که در آن، (H) ماتریس هموارسازی قطری شامل پارامترهای h_j، s_i ضریب اصلاح نمونه و $ik(\cdot)$ کرنل چندبعدی (مثلاً کرنل کوشی) می‌باشد. تصمیم‌گیری کلاس در رابطه (۸) برای نمونه جدید $\boldsymbol{x}$ بر اساس قانون بیشینه احتمال است:

$$c(\boldsymbol{x}) = arg\max_k \hat{f}_{C_k}(\boldsymbol{x}) \quad (۸)$$

وزن‌های w_i بر اساس تحلیل حساسیت (SA) نمونه‌های آموزشی تعیین می‌شوند. حساسیت گرادیان تابع KDE نسبت به ورودی‌ها محاسبه شده و سپس وزن‌های نرمال شده برای هر نمونه از کلاس C_k به دست می‌آید:

$$w_j = \frac{1}{\|\boldsymbol{a}_j\|_n}\boldsymbol{a}_j . \boldsymbol{a}_j = \left[\frac{1}{P_j}\sum_{p=1}^{P_j} \|\hat{\nabla f}_j^{(p.r)}\|_n^2\right]^{1/2} \quad (۹)$$

که، $\boldsymbol{a}_j$ بردار حساسیت‌های تجمع شده کلاس j، P_j تعداد نمونه‌های کلاس j، و $\hat{\nabla f}_j^{(p.r)}$ گرادیان KDE نسبت به ورودی‌ها برای نمونه p است.

۳-۳-۵-چارچوب یادگیری گروهی عمیق

در مدل پیشنهادی، خروجی‌های چهار یادگیرنده $\{M_1 . M_2 . M_3 . M_4\}$ متشکل ازDT،PNN، WPNN و MLP با با استفاده از مکانیزم وزن‌دهی تطبیقی به هم ترکیب می‌شوند. وزن هر یادگیرنده براساس معیارهای اعتماد و دقت محاسبه می‌گردد و خروجی نهایی y به صورت ترکیب وزنی است:

$$y = arg\max_{c\in C}\sum_{j=1}^{4} \alpha_j \cdot p_j(c \mid \boldsymbol{x}) \quad (۱۰)$$

که در آن، α_j وزن یادگیرنده j-ام، $p_j(c \mid \boldsymbol{x})$ احتمال تخصیص داده شده به کلاس c توسط یادگیرنده j، و C مجموعه کلاس‌ها است.این وزن‌دهی تطبیقی باعث کاهش نرخ مثبت کاذب و افزایش قابلیت تشخیص حملات ناشناخته می‌شود.

یادگیری گروهی عمیق:

فرض کنید خروجی هر مدل یادگیرنده M_j برای نمونه ورودی $\boldsymbol{x}$، یک بردار احتمالاتی است:

$$\boldsymbol{p}_j(\boldsymbol{x}) = \left[p_j(c_1 \mid \boldsymbol{x}).p_j(c_2 \mid \boldsymbol{x}).\ldots.p_j(c_K \mid \boldsymbol{x})\right] \quad (11)$$

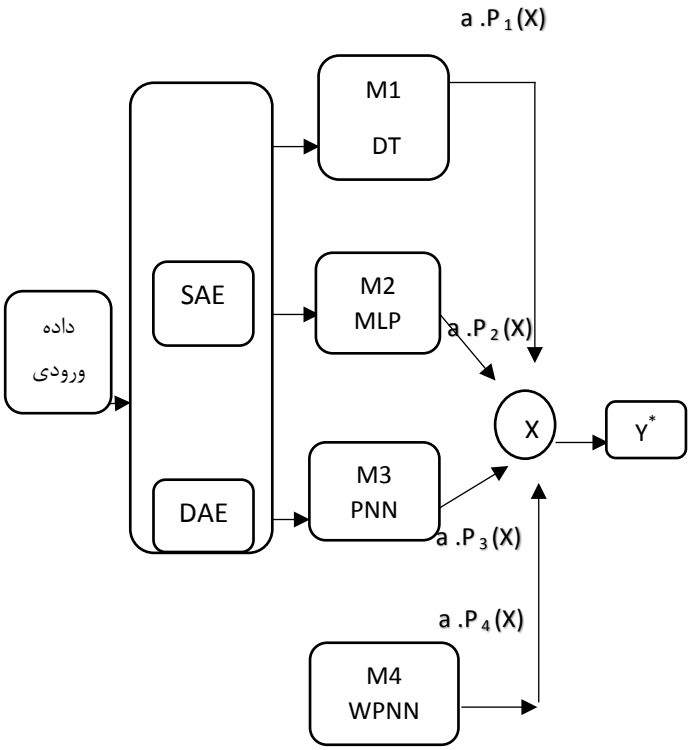
که K تعداد کلاس‌ها است. وزن‌دهی تطبیقی بر اساس ارزیابی عملکرد هر مدل (مثلاً دقت، نرخ مثبت کاذب یا معیارهای اعتماد) صورت می‌گیرد و به هر یادگیرنده وزن α_j اختصاص می‌یابد، به‌طوری که:

$$\sum_{j=1}^{4} \alpha_j = 1.\alpha_j \geq 0 \quad (12)$$

خروجی نهایی طبقه‌بندی مدل گروهی y^* به صورت رابطه (۱۳) تعریف می‌شود:

$$y^* = arg \max_{c\in\{c_1,\ldots.c_K\}} \sum_{j=1}^{4} \alpha_j \cdot p_j(c \mid \boldsymbol{x}) \quad (13)$$

نمودار بلوکی مدل یادگیری گروهی عمیق به‌صورت شکل ۷ می‌باشد.



شکل ۷: نمودار بلوکی مدل یادگیری گروهی عمیق

لازم به ذکر است که فرایند اصلی تشخیص ناهنجاری در این مدل، پس از مرحله استخراج ویژگی و درون الگوریتم‌های یادگیری گروهی انجام می‌گیرد. گره‌ها و لایه‌های خروجی مدل‌های یادگیرنده نظیر درخت تصمیم، پرسپترون چندلایه، شبکه عصبی احتمالی و نوع وزنی آن، وظیفه‌ی طبقه‌بندی نمونه‌ها به رفتارهای عادی و ناهنجار را بر عهده دارند. به‌عبارت دقیق‌تر، هر یک از این مدل‌ها با تحلیل بردار ویژگی فشرده‌شده تولیدشده توسط رمزگذارها، احتمال تعلق نمونه به کلاس ناهنجار را محاسبه کرده و خروجی نهایی از طریق یک سازوکار ترکیب تطبیقی وزنی حاصل می‌شود.

در معماری پیاده‌سازی پیشنهادی، تشخیص ناهنجاری‌ها توسط گره‌های لبه[42] **یا** گره‌های میان‌افزار[43] انجام می‌شود. به دلیل سربار پردازشی مدل ترکیبی شامل رمزگذارهای خودکار و یادگیرنده‌های گروهی، اجرای آن بر روی گره‌های IoT با منابع محدود مانند حسگرها امکان‌پذیر نیست. داده‌های شبکه از طریق گره‌های جمع‌آوری‌کننده یا دروازه‌ها[44] ارسال شده و در محیط لبه یا ابری پردازش می‌شوند. این رویکرد امکان تحلیل بلادرنگ نسبی و پایداری عملکرد در شبکه‌های مقیاس‌پذیر را فراهم می‌سازد.

۴- مجموعه داده‌ها

مجموعه‌داده‌های BoT-IoT[۵۳] ، IoT-NI[۵۴]، IoT-23 [۵۵]، MQTT[۵۶]، MQTTset[۵۶]و NSLKDD[۵۷] برای ارزیابی مدل‌های پیشنهادی مورداستفاده قرار گرفتند. اولین مرحله شامل پردازش فایل‌های pcap مجموعه‌داده‌های BoT-IoT [۵۸]، Network Intrusion IoT[۵۹] ، IoT-23[۶۰]، MQTT-IoT-IDS2020[۶۱] و MQTTset[۶۲] بود.

در مرحله اول، فایل‌های pcap این مجموعه‌داده‌ها استخراج و پردازش شدند تا ۸۰ ویژگی به‌صورت فایل CSV تولید گردد. برچسب‌گذاری نمونه‌ها بر اساس معیارهای از پیش تعریف‌شده برای هر مجموعه‌داده انجام شده است. نمونه‌هایی که شامل شناسه جریان، IP منبع، پورت مبدأ، IP مقصد و مهر زمانی برای مشخص‌کردن ارتباطات در شبکه IoT بودند، از تمامی مجموعه‌ها حذف گردیدند.

ویژگی‌های غیرعددی به مقادیر عددی تبدیل شده و نمونه‌های تکراری در فایل‌های CSV حذف شدند. سپس داده‌ها در بازه (-1. 1)(−1.1) نرمال شدند تا مقادیر پرت کاهش یافته و سرعت پردازش افزایش یابد. داده‌های ناقص با مقدار میانگین جایگزین

[42] Edge Nodes
[43] Fog Nodes
[44] Gateways

شده‌اند.جدول ۳ خلاصه‌ای از کلاس‌ها و تعداد نمونه‌های هر مجموعه داده را، با در نظر گرفتن حذف و حفظ نمونه‌های افزوده، ارائه می‌کند.

جدول ۳: کلاس‌ها و نمونه‌های مجموعه داده‌های BoT-IoT ، IoT-NI، IoT-23، MQTT و MQTTset

کلاس	دسته	با افزونگی	بی افزونگی	مجموعه داده
0	Normal	150202	77511	(a) BoT-IoT
1	DDoS	57027372	17420085	
2	DoS	37077674	18199716	
3	Scan	4734836	4108211	
4	Data Theft	454715	445799	
0	Normal	40073	39851	(b) IoT-NI
1	DoS	59391	59391	
2	MITM	35377	32909	
3	Mirai	415677	366971	
4	Scan	75265	72122	
0	Normal	4313776	4253672	(c) IoT-23
1	Attack	1716778	1699608	
2	Mirai	756	756	
3	File Download	8035	7707	
4	Heartbeat	12895	12648	
5	C&C	23981	20612	
6	Torii	33858	24492	
7	Port Scan	65944863	2999999	
8	DDoS	20768988	4619869	
9	Okiru	13718252	12908506	
0	Normal	334318	167159	(d) MQTT-IoT-IDS2020
1	MQTT Bruteforce	2002780	2001972	
2	Scan-A	31245	29276	
3	Scan-U	33404	27843	
4	Sparta	1252259	1217198	
0	Normal	440699	420136	(e) MQTTset
1	Bruteforce	4547	4513	
2	MQTTFlood	77793	77756	
3	MalariaDoS	11408	11265	
4	Malformed	3580	3535	
5	SlowITe	3044	3044	

توصیف مختصر بستر داده‌ها:

- BoT-IoT تولید شده شامل ماشین‌های مجازی متصل به اینترنت و شبکه محلی (LAN) است. ترافیک عادی توسط ابزار Ostinato و حملات توسط سیستم کالی‌لینوکس تولید می‌شود. کلاس‌ها شامل Normal، DDoS، DoS، Scan و Data Theft است. کلاس DDoSو DoS با هم ترکیب شده‌اند.
- IoT-NI: شامل حملاتDoS ، MITM، Miraiو Scan است. داده‌ها از ترافیک شبکه بی‌سیم جمع‌آوری شده‌اند.
- IoT-23 توسعه‌یافته در آزمایشگاه Stratosphere دانشگاهCTU ، شامل ۲۰ رویداد مخرب و ۳ رویداد غیرمخرب از دستگاه‌های واقعی IoT است.
- MQTT-IoT-IDS2020 مجموعه‌ای شامل ۵ سناریو عملیاتی عادی و حملات مرتبط با پروتکل MQTT است.
- MQTTset شامل ترافیک IoT در یک‌خانه هوشمند شبیه‌سازی شده با ۱۰ حسگر واقعی است.

ترکیب مجموعه‌داده‌هاIoT-DS2 :

برای ایجاد مجموعه‌داده جامع‌تر، مجموعه‌هایBoT-IoT ، IoT-NI، IoT-23، MQTTو MQTTset ترکیب شده‌اند و مجموعه‌داده جدیدی به نام IoT-DS2تشکیل شده است. این مجموعه‌داده شامل ۱۸ کلاس حمله و یک کلاس عادی است. نمونه‌های داده در IoT-DS2 به شرح جدول ۴ تقسیم‌بندی شده‌اند.

جدول ۴: کلاس‌ها و نمونه‌های مجموعه داده IoT-DS2 و زیرمجموعه‌های آن

دسته	BoT-IoT	IoT-NI	IoT-23	MQTT	MQTTset	IoT-DS2
Normal	-	-	4253672	-	-	2000000
DDoS	17420085	-	-	-	-	500000
DoS	-	59391	-	-	-	59391
MITM ARP Spoofing	-	32909	-	-	-	32909
Mirai	-	366971	-	-	-	366971
MQTT Bruteforce	-	-	-	2001972	-	500000
Sparta	-	-	-	1217198	-	500000
Theft	445799	-	-	-	-	445799
Attack	-	-	1699608	-	-	500000
C&C	-	-	20612	-	-	20612
File Download	-	-	7707	-	-	7707
Heartbeat	-	-	12648	-	-	12648

500000	-	-	1290 8506	-	-	Okiru
500000	-	-	-	-	946268	OS Scan
500000	-	-	2999 999	-	-	Port Scan
24492	-	-	24492	-	-	Torii
77756	77756	-	-	-	-	MQTT Flood
3535	3535	-	-	-	-	Malformed
3044	3044	-	-	-	-	SlowITe

برای ارزیابی مدل‌ها، داده‌ها به دو بخش ۸۰٪ آموزش و ۲۰٪ تست تقسیم شدند. سپس داده‌های آموزشی مجدداً به ۸۰٪ آموزش و ۲۰٪ اعتبارسنجی تفکیک شدند. تکنیک حذف ویژگی بازگشتی با استفاده از الگوریتم جنگل تصادفی برای انتخاب ۶۴ ویژگی کلیدی در مجموعه داده IoT-DS2 به‌کار گرفته شد. برای مجموعه داده NSLKDD از روش انتخاب ویژگی استفاده نشد و همه ویژگی‌ها در مدل‌ها لحاظ شدند.

از میان مجموعه‌داده‌های موجود، هفت مجموعه معتبر شامل NSL-KDD، BoT-IoT، IoT-NI، IoT-23، MQTT، MQTTset و IoT-DS2 انتخاب شده‌اند تا تنوع سناریوهای حمله، معماری‌های شبکه و پروتکل‌های ارتباطی در فضای اینترنت اشیا به‌درستی پوشش داده شود. ترکیب این مجموعه‌ها امکان ارزیابی جامع مدل در شرایط گوناگون و افزایش اعتبار نتایج را فراهم می‌کند.

۵-ارزیابی نتایج

مدل‌های پیشنهادی یادگیری گروهی با استفاده از درخت تصمیم (DT)، پرسپترون چندلایه (MLP)، شبکه عصبی احتمالی (PNN) و شبکه عصبی احتمالی وزنی (WPNN) با استفاده از دقت، صحت، فراخوانی، امتیاز F1، FPR (نرخ مثبت کاذب)، FNR[۴۵] (نرخ منفی کاذب) که فرمول‌های این معیارها در معادله ۱۴ تا ۱۹ ارائه شده است و ROC اعتبارسنجی شدند.

$$Accuracy = \frac{(TP + TN)}{(TP + FP + TN + FN)} \quad (۱۴)$$

$$Precision = \frac{TP}{(TP + FP)} \quad (۱۵)$$

$$Recall = Sensitivity = \frac{TP}{(TP + FN)} \quad (۱۶)$$

$$F1\ score = 2 \times \frac{(Precision \times Recall)}{(recision + Recall)} \quad (۱۷)$$

$$FPR = \frac{FP}{(FP + TN)} \quad (۱۸)$$

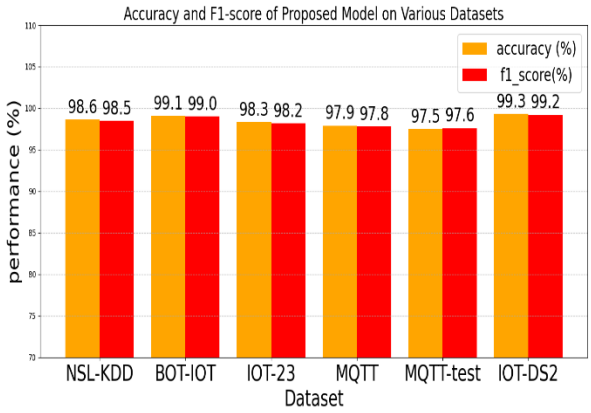
$$FNR = \frac{FN}{(FN + TP)} \quad (۱۹)$$

[45] False Negative Rate

برای ارزیابی مدل‌ها، هفت مجموعه‌داده مختلف جهت انجام آزمایش‌های طبقه‌بندی چند کلاسه و باینری استفاده شده است. این پژوهش از چارچوب Keras به همراه TensorFlow به‌عنوان Backendبرای پیاده‌سازی و اجرای تمامی آزمایش‌ها بهره برده است. تمامی فرایندهای آموزش، اعتبارسنجی و آزمون در بستر Google Colabانجام شده‌اند. لازم به ذکر است که در صورت عدم تعادل توزیع داده‌ها، مدل‌های طبقه‌بندی تمایل دارند به نفع کلاس اکثریت عمل کنند.

۵-۱-تحلیل معیار دقت و امتیاز F1

در شکل ۸ و جدول ۵، عملکرد مدل پیشنهادی در دو معیار دقت و امتیاز F1 بر روی چند مجموعه داده معتبر نشان داده شده است. دقت‌ها همگی بالای ۹۷ درصد هستند که نشان‌دهنده قابلیت اطمینان بالای مدل برای تشخیص ناهنجاری‌ها است. بیشترین دقت در مجموعه داده BoT-IoT با ۹۹,۱٪ و کمترین دقت در MQTTset با ۹۷,۵٪ ثبت شده است. امتیاز F1 نیز به طور مشابه بین ۹۷,۶٪ تا ۹۹,۰٪ قرار دارد که تعادل خوبی بین فراخوانی و دقت مدل را نشان می‌دهد.



شکل ۸ : عملکرد مدل پیشنهادی در معیار دقت و *F1*

جدول ۵: عملکرد مدل پیشنهادی در معیاردقت و امتیاز *F1*

مجموعه داده	دقت *(%)*	F1-score (%)
NSL-KDD	98.6	98.5
BoT-IoT	99.1	99
IoT-23	98.3	98.2
MQTT	97.9	97.8
MQTTset	97.5	97.6
IoT-DS2	99.3	99.2

مدل پیشنهادی روی مجموعه‌داده NSL-KDD موفق به کسب دقت ۹۸,۶٪ و امتیاز F1 برابر با ۹۸,۵٪ شده است. این نتایج نشان‌دهنده عملکرد بسیار خوب مدل در تشخیص ناهنجاری‌ها در این مجموعه داده متوازن و استاندارد است. دقت بالا به معنای

کاهش خطاهای طبقه‌بندی است و F1-score نزدیک به دقت، نشان می‌دهد که مدل توانسته است بین نرخ شناسایی حملات و کاهش هشدارهای کاذب تعادل مناسبی برقرار کند.

در مجموعه‌دادهBoT-IoT ، مدل دقت ۹۹,۱٪ و F1-score برابر با ۹۹ را ثبت کرده است. این میزان دقت بسیار بالا نشان می‌دهد که مدل پیشنهادی توانسته است به خوبی با پیچیدگی و حجم بالای داده‌های مربوط به ترافیک بات‌نت‌های اینترنت اشیا مقابله کند. عملکرد عالی در این مجموعه، تأکیدی بر توانمندی رمزگذارهای خودکار و یادگیری گروهی در استخراج و تفکیک دقیق الگوهای مخرب در برابر ترافیک عادی است.

مدل در مجموعه‌داده IoT-23 به‌دقت ۹۸,۳٪ و F1-score معادل ۹۸,۲٪ دست‌یافته است. این نتایج نشان‌دهنده قدرت مدل در شناسایی تهدیدات در محیط‌های واقعی‌تر و متنوع‌تر اینترنت اشیا است، جایی که انواع مختلف حملات و داده‌های پیچیده‌تر وجود دارد. حفظ دقت بالا در این مجموعه بیانگر انعطاف‌پذیری و سازگاری مدل در محیط‌های پر تغییر و چند کلاسه است.

مدل پیشنهادی برای داده‌های MQTT موفق به کسب دقت ۹۷,۹٪ و F1-score برابر ۹۷,۸٪ شده است. با توجه به خصوصیات پروتکل MQTT که مختص اینترنت اشیاء و انتقال پیام‌های سبک است، این دقت نشان می‌دهد که مدل قادر است الگوهای حملات و ناهنجاری‌های مختص این پروتکل را به خوبی تشخیص دهد. این امر برای امنیت در لایه انتقال داده‌های اینترنت اشیا بسیار حیاتی است.

نتایج به‌دست‌آمده از مجموعه‌داده MQTTset شامل دقت ۹۷,۵٪ و F1-score معادل ۹۷,۶٪ است. این ارقام، مدل پیشنهادی را در دسته‌بندی دقیق انواع حملات و رفتارهای غیرعادی شبکه‌های IoTبا استفاده از پروتکل MQTT قرار می‌دهد. عملکرد پایدار مدل روی این مجموعه داده نشان می‌دهد که استراتژی انتخاب ویژگی و یادگیری گروهی اثرگذار بوده و قابلیت تعمیم مدل را بهبود بخشیده است.

در مجموعه‌داده ترکیبی IoT-DS2 که از ادغام چند مجموعه‌داده مختلف تشکیل شده و شامل هجده کلاس حمله و یک کلاس نرمال است، مدل پیشنهادی به‌دقت ۹۹,۳٪ و F1-score معادل ۹۹,۲٪ دست‌یافته است. این عملکرد عالی نشان‌دهنده توانایی برجسته مدل در مقابله با پیچیدگی‌های ترکیب داده‌های متعدد و تشخیص دقیق انواع مختلف تهدیدات است. بهبود عملکرد مدل در این مجموعه‌داده نسبت به سایر مجموعه‌ها را می‌توان به طراحی رمزگذارهای خودکار عمیق و به‌کارگیری الگوریتم ترکیب تطبیقی وزن‌دهی در چارچوب یادگیری گروهی نسبت داد.

۲-۵-تحلیل معیار نرخ مثبت کاذب و نرخ منفی کاذب

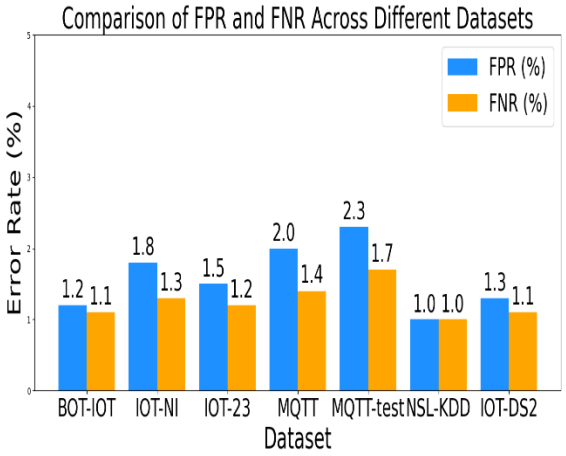
معیارهای نرخ مثبت کاذب (FPR) و نرخ منفی کاذب (FNR) از مهم‌ترین شاخص‌ها در ارزیابی کارایی سیستم‌های تشخیص ناهنجاری به‌ویژه در زمینه اینترنت اشیا هستند.

- **(FPR)** میزان نمونه‌های قانونی است که به‌اشتباه به‌عنوان ناهنجاری شناسایی شده‌اند. این مقدار پایین‌بودن آن نشان‌دهنده کاهش هشدارهای کاذب است.
- **(FNR)** میزان نمونه‌های ناهنجار است که به‌اشتباه به‌عنوان قانونی طبقه‌بندی شده‌اند. کاهش این نرخ اهمیت بسیار زیادی در شناسایی دقیق تهدیدات دارد.

جدول ۶: نرخ مثبت کاذب و منفی کاذب برای مجموعه داده‌ها

مجموعه داده	FPR %	FNR %
BoT-IoT	1.2	1.1
IoT-NI	1.8	1.3
IoT-23	1.5	1.2
MQTT	2.0	1.4
MQTTset	2.3	1.7
NSLKDD	1.0	1.0
IoT-DS2	1.3	1.1

از جدول ۶ و نمودار مربوطه (شکل ۹) می‌توان مشاهده کرد که مدل پیشنهادی توانسته است نرخ مثبت کاذب را در سطح پایینی حفظ کند، به‌ویژه در مجموعه‌داده‌هایی مانند NSL-KDD و BoT-IoTکه به ترتیب کمترین مقادیر FPR برابر با ۱,۰٪ و ۱,۲٪ را نشان می‌دهند. این موضوع بیانگر کاهش هشدارهای نادرست و بهبود کارایی عملیاتی سیستم است. نرخ منفی کاذب نیز در تمامی مجموعه‌داده‌ها کمتر از ۲٪ گزارش شده که نشان‌دهنده دقت بالای مدل در شناسایی واقعی ناهنجاری‌ها و تهدیدات است. این ویژگی، در سناریوهای امنیتی حساس که شناسایی نشدن حملات می‌تواند پیامدهای جدی به‌دنبال **داشته** باشد، از اهمیت ویژه‌ای برخوردار **است.** بالاترین FPR و FNR مربوط به مجموعه داده MQTTset است که ممکن است به دلیل پیچیدگی‌های خاص این داده و تنوع حملات آن باشد؛ با این وجود، مقادیر ارائه شده در این مجموعه نیز در بازه قابل قبول قرار دارد. به طور کلی، مدل پیشنهادی با حفظ تعادل بین کاهش FPR وFNR ، قابلیت اطمینان بالایی در تشخیص ناهنجاری‌ها ارائه می‌دهد.



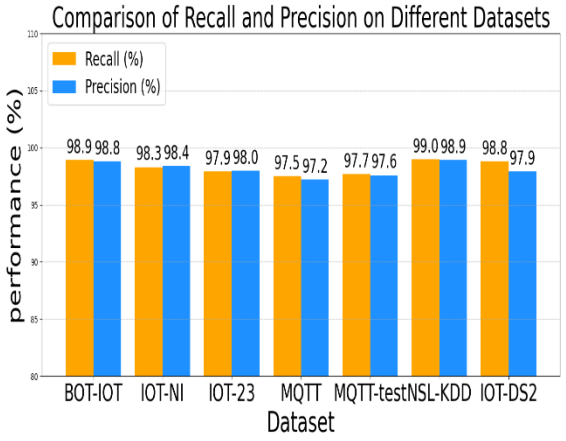
شکل۹: نمودار مقایسه FPR و FNR در مدل پیشنهادی روی مجموعه داده‌های مختلف

۵-۳- تحلیل معیار حساسیت و صحت

در ارزیابی عملکرد سیستم‌های تشخیص ناهنجاری، دو معیار حساسیت و صحت نقش بسیار مهمی ایفا می‌کنند در ارزیابی عملکرد سیستم‌های تشخیص ناهنجاری، دو معیار حساسیت و صحت نقش بسیار مهمی ایفا می‌کنند.

نتایج ارائه شده در شکل ۱۰ بیانگر عملکرد بسیار مطلوب مدل پیشنهادی در شناسایی نمونه‌های ناهنجار است، به گونه‌ای که حساسیت همه مجموعه داده‌ها بالاتر از ۹۷,۴ درصد می‌باشد. این موضوع نشان‌دهنده توانایی بالا در کشف حملات و ناهنجاری‌های مختلف در محیط‌های اینترنت اشیا است.

صحت مدل در تمامی مجموعه‌داده‌ها بیش از ۹۷٪ گزارش شده است؛ این موضوع بیانگر کاهش نرخ هشدارهای کاذب و بهبود دقت کلی سیستم در شناسایی رفتارهای ناهنجار است. در میان مجموعه داده‌ها، NSLKDD با حساسیت ۹۹. ٪ و صحت ۹۸,۹٪ بهترین عملکرد را داشته است که به دلیل ساختار کلاسیک و استاندارد بودن این مجموعه داده قابل انتظار است.عملکرد مدل روی مجموعه‌داده‌های پیچیده‌تر مانند MQTTset نیز بسیار قابل‌قبول بوده و توانسته است حفظ دقت و شناسایی بالا را تضمین کند.



شکل ۱۰: نمودار حساسیت و صحت مدل پیشنهادی روی مجموعه داده‌های مختلف

۵-۴- تحلیل نمودار ROC[46]

نمودار ROC یکی از مهم‌ترین ابزارها برای ارزیابی عملکرد مدل‌های تشخیص ناهنجاری است. این نمودار رابطه بین نرخ مثبت کاذب و حساسیت را در آستانه‌های مختلف نمایش می‌دهد. معیار کلیدی در این تحلیل، مقدار AUC[47] است که نشان‌دهنده توانایی مدل در تمایز قائل‌شدن بین کلاس‌های مثبت و منفی است.

- مقدار AUC بین ۰,۵ تا ۱ تغییر می‌کند، به طوری که مقدار نزدیک به ۱ بیانگر عملکرد بسیار عالی و مدل قوی در تشخیص نمونه‌ها است.
- مقادیر بالای AUC به معنای تعادل مناسب بین حساسیت و نرخ مثبت کاذب و در نتیجه دقت کلی بالاتر در پیش‌بینی است.

جدول۷: مقدار AUC برای مجموعه داده‌ها

مجموعه داده	AUC
BoT-IoT	0.865
IoT-NI	0.903
IoT-23	0.854
MQTT	0.980
MQTTset	0.948
NSLKDD	0.987
IoT-DS2	0.905

مقدار AUC مدل پیشنهادی برای تمام مجموعه‌داده‌ها نزدیک به عدد ۱ است، که نشان‌دهنده توانایی بالا در تشخیص دقیق نمونه‌های ناهنجار از نمونه‌های قانونی است. بالاترین مقدار AUC مربوط به مجموعه داده NSLKDD با عدد ۰,۹۸۷ می‌باشد که

[46] Receiver Operating Characteristic
[47] Area Under the Curve

بیانگر تشخیص تقریباً بی‌نقص در این مجموعه داده است. کمترین مقدار AUC در میان مجموعه داده‌ها مربوط به BoT-IoT با ۰,۸۶۵ است که همچنان عملکرد خوبی را نشان می‌دهد. این مقادیر بالا و پایدار در تمام مجموعه داده‌ها، نشانگر کارایی و تعمیم‌پذیری مدل پیشنهادی در مواجهه با داده‌های متنوع و واقعی دنیای اینترنت اشیا است. ترکیب یادگیری گروهی عمیق و رمزگذارهای خودکار، نه تنها دقت تشخیص را افزایش داده بلکه پایداری مدل را در مواجهه با تغییرات داده و نویز تضمین کرده است.

۵-۵- مقایسه با سایر روش‌های مشابه

در شکل ۱۱، مدل پیشنهادی با معماری یادگیری گروهی عمیق، موفق به کسب دقت بالاتری نسبت به سایر مدل‌ها شده است. برای نمونه:دقت مدل پیشنهادی در مجموعه داده‌های IoT به طور کلی بالای ۹۸٪ است که از بیشتر مدل‌های دیگر، مانند ML Ensemble[۱۷] با ۹۷,۲٪ و CNN Lite [۲۴] با ۹۳,۰٪ پیشی گرفته است. در حوزه‌های خاص مانند Industrial IoT و Smart Grid، مدل‌های تخصصی همچون Graph-ResNet + Hawk-Bee [۲۰] و MTD-AD [۲۹] دقت بالا اما کمتر یا نزدیک به مدل پیشنهادی ما دارند.

پژوهش [۱۷] روش که از ترکیب چندین مدل یادگیری ماشین استفاده کرده، به دقت ۹۷,۲ %دست یافته است. این تفاوت نشان‌دهنده تأثیر بهینه‌ساز های انجام شده در معماری پیشنهادی است. این مدل فاقد سازوکار انتخاب پویای ویژگی است که در روش پیشنهادی اعمال شده و منجر به دقت ۹۹,۳٪ شده است.

در [۱۸] این مدل از گراف عصبی و شبکه‌های ResNet برای تحلیل ساختارهای ارتباطی در شبکه‌های بی‌سیم استفاده می‌کند و دقت کمتری از روش پیشنهادی دارد. هرچند این معماری در تحلیل روابط توپولوژیکی موفق عمل کرده، اما پیچیدگی محاسباتی بالایی دارد.

ردی و همکاران در [۲۰] با معماری ترکیبی Graph-ResNet و الگوریتم Hawk-Bee به دقت ۹۸,۳٪ دست یافته‌اند.

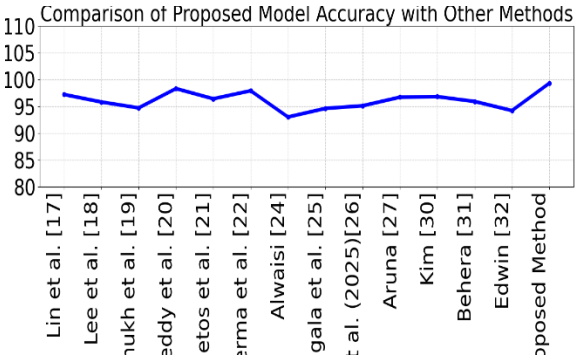
پژوهش [۲۲] با به کارگیری چارچوب گروهی و بهینه‌ساز تعادل به دقت ۹۷,۹٪ رسیده که مجدداً عملکرد پایین‌تری نسبت به روش حاضر دارد.

روش‌هایی مثل [۲۴] که با هدف کاهش هزینه محاسباتی و سبک‌سازی طراحی شده‌اند، هرچند زمان آموزش و استنتاج کمتری دارند، اما به دلیل ضعف در لایه‌های استخراج ویژگی عمیق و عدم مدیریت مناسب داده‌های نامتوازن، دقت پایین‌تری نسبت به روش پیشنهادیکسب کرده‌اند.

روش [۱۹]با یادگیری عمیق مشارکتی دقت ۹۴,۷٪ را کسب کرده و در حفظ حریم خصوصی مؤثر است، اما در تشخیص ناهنجاری‌های پیچیده نسبت به روش پیشنهادی ضعف دارد.روش [۲۳] با معماری سبک DPS-DL و دقت ۹۱,۷٪ در تحلیل داده‌های پیچیده و غیرخطی نسبت به روش پیشنهادی دقت پایینی دارد.

روش [۲۵] با ترکیب GANN و بلاکچین به دقت ۹۴,۶٪ رسیده اما در برابر حملات نوین IoT با افت دقت روبروست. روش [۲۶] با AE+LSTM+CNNدقت ۹۶,۷٪ کسب کرده و در تحلیل داده‌های زمانی قوی است، اما در داده‌های نامتوازن نسبت به روش پیشنهادی ضعف دارد. روش[۲۹] با Masked AE دقت ۹۶,۸٪ دارد و در بازیابی داده‌های ناقص خوب عمل می‌کند اما در حملات چندمرحله‌ای محدودیت که باعث شده دقت کتری نسبت به روش پیشنهادی داشته باشد.روش [۳۰] با MTD-AD دقت ۹۵,۹٪ را ارائه داده و در حملات تطبیقی مقاوم است اما در حملات حجیم عملکرد کمتری نسبت به مدل پیشنهادی دارد.

در حالی که برخی مدل‌ها مانند روش ادوین و همکاران[۳۲] با ترکیب چندین شبکه پیچیده و الگوریتم Walrus به دقت ۹۸,۱٪ دست یافته‌اند، پیچیدگی بالای معماری آن‌ها باعث افزایش هزینه محاسباتی شده است.که باعث شده دقت کمتری نسبت به روش پیشنهادی داشته باشد.



شکل ۱۱: مقایسه با سایر روش‌های مشابه

با توجه به ماهیت ترکیبی مدل پیشنهادی، تحلیل کارایی زمانی و مصرف منابع آن از اهمیت بالایی برخوردار است. آزمایش‌ها روی بستر Google Colab با GPU Tesla T4 و ۱۶ گیگابایت RAM انجام شده‌اند. زمان آموزش کامل مدل پیشنهادی برای مجموعه‌داده IoT-DS2 حدود ۲۷ دقیقه و زمان تست برای ۱۰۰۰۰۰ نمونه جدید حدود ۱,۳ ثانیه گزارش شده است. پیچیدگی زمانی بخش رمزگذار خودکار با تعداد لایه‌های L و ابعاد ویژگی d، به‌صورت تقریبی $O(l \times d^2)$ است. همچنین، زمان اجرای مدل یادگیری گروهی با فرض ترکیب تطبیقی بر

حسب تعداد مدل‌ها M و اندازه داده تست n، برابر O(M*n*d) خواهد بود.
اگرچه این مدل پیشنهادی به‌دلیل ماهیت عمیق و گروهی، نسبت به روش‌های ساده‌تر مانند درخت تصمیم منفرد دارای هزینه محاسباتی بالاتری است، اما دقت بالاتر و کاهش نرخ هشدار کاذب، این سربار را توجیه‌پذیر می‌سازد. به‌علاوه، با توجه به اجرای مدل در گره‌های لبه یا سرور، مصرف منابع در گره‌های حسگر نهایی نخواهد بود.

۶-نتیجه‌گیری و کارهای آتی

این مقاله یک چارچوب نوین برای شناسایی ناهنجاری در محیط‌های اینترنت اشیا بر اساس ترکیب رمزگذارهای خودکار عمیق و رویکرد یادگیری گروهی ارائه داد. مدل پیشنهادی با به‌کارگیری انتخاب پویای ویژگی در لایه‌های میانی رمزگذار و استفاده از الگوریتم‌های متنوعی همچونMLP ، PNNو WPNN توانست در مواجهه با داده‌های نامتوازن، حجم بالای ویژگی‌ها و حملات ناشناخته، کارایی بالایی از خود نشان دهد. نتایج حاصل از آزمایش بر روی هفت مجموعه‌داده معتبر از جملهNSL-KDD ، BoT-IoTو IoT-23 نشان داد که چارچوب ارائه‌شده در تمامی سناریوها عملکردی پایدار، دقتی بیش از ۹۹٪، و نرخ بسیار پایین مثبت و منفی کاذب به دست آورده است. همچنین مقادیر AUC در بازه‌ی ۰,۸۵ تا ۰,۹۸ و تعادل میان حساسیت و صحت، نشانگر توان بالای مدل در شناسایی ناهنجاری‌های پیچیده و افزایش اعتمادپذیری در محیط‌های واقعی است.

از جمله مزایای برجسته مدل پیشنهادی می‌توان به تعمیم‌پذیری بالا در برابر داده‌های متنوع و پرت، کاهش زمان آموزش در مقایسه با معماری‌های پیچیده مبتنی بر Graph Neural Networks، و توانایی در شناسایی حملات ترکیبی و چندمرحله‌ای اشاره کرد. علاوه بر این، کاهش هزینه محاسباتی و پایداری عملکرد در داده‌های نویزی و چندکلاسه، بر ارزش عملی این چارچوب می‌افزاید. با این حال، نیاز به تنظیم دقیق پارامترهای اولیه و پیچیدگی نسبی در فاز طراحی از محدودیت‌های اصلی روش پیشنهادی محسوب می‌شود.

در ادامه، توسعه مدل برای پشتیبانی از داده‌های چندرسانه‌ای و انواع مختلف داده‌هایIoT ، طراحی روش‌های یادگیری آنلاین و خودسازگار برای به‌روزرسانی در زمان واقعی، ادغام با فناوری‌های امنیتی نوین نظیر بلاک‌چین و فایروال‌های هوشمند، و بهینه‌سازی مصرف انرژی و منابع محاسباتی در دستگاه‌های با محدودیت سخت‌افزاری می‌تواند مسیرهای ارزشمند تحقیقات آینده باشد.

۷- مراجع

[1] A. Čolaković, B. Karahodža, and A. H. Džubur, “QoS-Aware IoT Framework for Performance Control and Resource Management,” IntechOpen, 2025

[2] I. Rozlomii, A. Yarmilko, and S. Naumenko, “Data Security of IoT Devices with Limited Resources: Challenges and Potential Solutions,” Doors, vol. 3666, pp. 85–96, 2024

[3] N. Sharma and P. Dhiman, “A Survey on IoT Security: Challenges and Their Solutions Using Machine Learning and Blockchain Technology,” Cluster Computing, vol. 28, p. 313, 2025

[4] P. Sethi and S. R. Sarangi, “Internet of Things: Architectures, Protocols, and Applications,” Journal of Electrical and Computer Engineering, vol. 2017, no. 1, p. 9324035, 2017.

[5] Q. Meng, H. Wang, C. Zhang, and Y. Song, “Embedding Chips Over the Air: Rethink IoT Architecture for Ubiquitous Sensing,” IEEE Transactions, 2025

[6] A. Heidari and M. A. J. Jamali, “Internet of Things Intrusion Detection Systems: A Comprehensive Review and Future Directions,” Cluster Computing, vol. 26, no. 6, pp. 3753–3780, 2023

[7] S. H. Rafique, F. M. Malik, F. F. Hassan, M. A. Shuja, and J. J. P. C. Rodrigues, “Machine Learning and Deep Learning Techniques for Internet of Things Network Anomaly Detection—Current Research Trends,” Sensors, vol. 24, no. 6, p. 1968, 2024.

[8] D. Adhikari, S. Bhusal, P. Pokharel, and J. Hu, “Recent Advances in Anomaly Detection in Internet of Things: Status, Challenges, and Perspectives,” Computer Science Review, vol. 54, p. 100665, 2024.

[9] E. Krzysztoń, I. Rojek, and D. Mikołajewski, “A Comparative Analysis of Anomaly Detection Methods in IoT Networks: An Experimental Study,” Applied Sciences, vol. 14, no. 24, p. 11545, 2024.

[10] Q. Abu Al-Haija and M. Al-Dala’ien, “ELBA-IoT: An Ensemble Learning Model for Botnet Attack Detection in IoT Networks,” Journal of Sensor and Actuator Networks, vol. 11, no. 1, p. 18, 2022.

[11] D. Vasan, M. Alazab, S. Venkatraman, J. Akram, and Z. Qin, “MTHAEL: Cross-Architecture IoT Malware Detection Based on Neural Network Advanced Ensemble Learning,” IEEE Transactions on Computers, vol. 69, no. 11, pp. 1654–1667, 2020

[12] F. Khan, M. A. Jan, R. Alturki, M. D. Alshehri, S. T. Shah, and A. ur Rehman, “A Secure Ensemble Learning-Based Fog-Cloud Approach for Cyberattack Detection in IoMT,” IEEE Transactions on Industrial Informatics, pp. 1–9, 2023

[13] Y. Alotaibi and M. Ilyas, “Ensemble-Learning Framework for Intrusion Detection to Enhance Internet of Things Devices’ Security,” Sensors, vol. 23, no. 12, p. 5568, 2023.

[14] A. R. Gad, H. A. Hefny, M. A. Elsisi, and R. A. Ramadan, “A Distributed Intrusion Detection System Using Machine Learning for IoT Based on ToN-IoT Dataset,” International Journal of Advanced Computer Science and Applications, vol. 13, no. 6, 2022.

[15] J. B. Awotunde, T. O. Olwal, O. A. Osanaiye, S. Misra, and R. D. Botha, “An Ensemble Tree-Based Model for Intrusion Detection in Industrial Internet of Things Networks,” Applied Sciences, vol. 13, no. 4, p. 2479, 2023.

[16] S. Huda, J. Abawajy, M. M. Hassan, A. Almogren, and A. Gani, “Securing the Operations in SCADA-IoT Platform Based Industrial Control System Using Ensemble of Deep Belief Networks,” Applied Soft Computing, vol. 71, pp. 66–77, 2018 .

[17] Y.-C. Lin, C.-Y. Lee, and C.-H. Tsai, “Diverse Machine Learning-Based Malicious Detection for Industrial Control System,” Electronics, vol. 14, no. 10, p. 1947, 2025.

[18] S. J. Lee and I. G. Lee, “Lightweight Federated Learning-Based Intrusion Detection System for Industrial Internet of Things,” ICT Express, vol. 11, no. 2, pp. 120–128, 2025.

[19] A. Deshmukh, P. E. de la Rosa, R. V. Rodriguez, and S. Dasari, “Enhancing Privacy in IoT-Enabled Digital Infrastructure: Evaluating Federated Learning for Intrusion and Fraud Detection,” Sensors, vol. 25, no. 10, p. 3043, 2025.

[20] D. R. Reddy, S. Ramani, D. Mohan, and L. Sahukar, “Secure IoTNet: A Graph-Residual Adversarial Network Integrated with Hawk-Bee Optimizer for Intrusion Detection in IoT Wireless Networks,” International Journal of Information Security, 2025.

[21] D. Papatsaroucha, E. K. Markakis, and D. Sygletos, “Developing a Near-Real Time AI-Based Network Intrusion Detection System,” Now Publishers, 2025.

[22] P. Verma, D. O’Shea, T. Newe, N. Mehta, and N. Bharot, “ABIDS-VEM: Leveraging an Equilibrium Optimizer and Data Ramification in Association with Ensemble Learning for Anomaly-Based Intrusion Detection System,” The Journal of Supercomputing, 2025.

[23] I. Ali, M. Raza, S. Bakhet, and M. U. Saleem, “Deep Learning Enabled Data Protection and Security (DPS) Techniques for Intrusion Mitigation, and Network Vulnerabilities Detection in the Internet of Things (IoTs),” Annual Multidisciplinary Research Review, 2025.

[24] Z. Alwaisi, “Memory-Efficient and Robust Detection of Mirai Botnet for Future 6G-Enabled IoT Networks,” Internet of Things, vol. 21, 2025

[25] R. K. Suggala, J. Kumar, P. Jain, and B. K. Kumar, “Blockchain Technology for Digital Twin Security in Smart Grids Using Interpretable Generalized Additive Neural Networks,” Peer-to-Peer Networking and Applications, 2025

[26] W. Peng, H. Zhang, and Y. Liu, “Modeling Realistic Adversarial Traffic Against Deep Learning-Based Intrusion Detection System in Industrial IoT,” IEEE Internet of Things Journal, 2025.

[27] T. M. Aruna, “AI-Driven Anomaly Detection in IoT Time Series: A Hybrid Approach to Classification and Feature Extraction,” Journal of Advancement in Data Computational Science, 2025.

[28] M. Mashaly and H. Kamal, “Hybrid Deep Learning Models-Based Anomaly Detection Method for Two-Stage Binary and Multi-Class Classification of Attacks in Intrusion Detection,” Algorithms, vol. 18, no. 2, p. 69, 2025.

[29] E. Li, Z. Shang, O. Güngör, and T. Rosing, “SAFE: Self-Supervised Anomaly Detection Framework for Intrusion Detection,” arXiv preprint, arXiv:2502.07119, Feb. 2025.

[30] D. D. Kim and M. R. Asghar, “MTD-AD: Moving Target Defense as Adversarial Defense for Anomaly Detection in IoT,” IEEE Transactions on Dependable and Secure Computing, 2025.

[31] S. Behera and N. Padhy, “Classification Algorithms for Pump Control and Optimization Using Autoencoders in IoT Environments,” in IEEE Conference on Intelligent Systems, 2025.

[32] E. B. Edwin, S. Kumar, M. S. Ahmed, and P. P. Reddy, “Ensemble of Deep Learning Models with Walrus Optimization Algorithm for Botnet Detection,” Iran Journal of Computer Science, 2025.

[33] H. Yan, J. Zhang, L. Wang, and Z. Chen, “MalAE: A Feature-Optimized and Autoencoder Ensemble-Based Method for IoT Malware Classification,” IEEE Internet of Things Journal, 2025.

[34] H. Fan, S. Li, and Y. Liu, “Rule-Extracted Deep Autoencoder for Interpretable Anomaly Detection in Smart Cities,” Sensors, vol. 24, no. 5, p. 1231, 2025.

[35] R. Saranya and K. Rani, “An Ensemble Model for Multilayer Deep Autoencoder in IoT Network Attack Detection,” Computers, Materials & Continua, vol. 78, no. 1, pp. 155–170, 2025.

[36] T. Naith, A. Qamar, and H. Singh, “Distributed Anomaly Detection in IoT Networks Using Self-Organizing Deep Autoencoder Models,” Computer Networks, vol. 237, 2025.

[37] R. Kumar, S. I. Immadisetty, and A. Patel, “Graph-Based Deep Autoencoder Architecture for IoT Security,” IEEE Access, vol. 11, pp. 112023–112036, 2023.

[38] A. Bezanjani, M. Hosseinzadeh, and M. F. Khoshrou, “Blockchain-Integrated Convolutional Autoencoder for IoT-Based Healthcare Systems,” Sensors, vol. 23, no. 9, p. 4120, 2023.

[39] Y. Wu, L. Liu, Y. Yu, G. Chen, and J. Hu, “Online Ensemble Learning-Based Anomaly Detection for IoT Systems,” Applied Soft Computing, vol. 173, p. 112931, 2025

[40] A. S. Abdullah, H. J. Sunil, and M. S. H. Nazmudeen, "A new model to evaluate signature and anomaly based intrusion detection in medical IoT system using ensemble approach," SN Comput. Sci., vol. 6, no. 4, p. 347, 2025.

[41] J. P. Ntayagabiri, Y. Bentaleb, J. Ndikumagenge, and H. El Makhtoum, “OMIC: A Bagging-Based Ensemble Learning Framework for Large-Scale IoT Intrusion Detection,” Journal of Future Artificial Intelligence Technology, vol. 1, no. 4, pp. 401–416, 2025.

[42] M. S. Rahman, I. Khan, M. Z. A. Eidmum, P. Shaha, B. Muiz, N. Hasan, and M. Rahman, “Stacked Ensemble Method: An Advanced Machine Learning Approach for Anomaly-Based Intrusion Detection System,” Statistics, Optimization & Information Computing, 2025.

[43] M. U. Tanveer, K. Munir, M. Amjad, H. J. Alyamani, A. Bermak, and A. U. Rehman, “LightEnsemble-Guard:

An Optimized Ensemble Learning Framework for Securing Resource-Constrained IoT Systems," IEEE Access, 2025

[44] N. Dashtifard, H. Mahmoud, M. Idrissi, and N. Elmitwally, "Enhanced Anomaly Detection in Wireless 5G Networks with Hybrid Learning Technique Using AWID3 Dataset," Environments, vol. 2, no. 3, 2025.

[45] A. K. Tajari Siah Marzkouh, "Intrusion Detection Model in Smart Homes Based on Principal Component Analysis and Random Forest Classification," Electron. Cyber Def., vol. 12, no. 2, pp. 15–25, 2024. (in Persian)dor:https://dor.isc.ac/dor/20.1001.1.23224347.1403.12. 22.2.

[46] A. Karimi and M. R. Khosravi Farsani, "Improving the Accuracy of Code Smell Detection Using the Gray Wolf Algorithm Based on Machine Learning and Majority Voting Techniques," Electron. Cyber Def., vol. 12, no. 1, pp. 109–122, 2024. (in Persian).dor: https://dor.isc.ac/dor/20.1001.1.23224347.1403.12.1.9.7.

[47] M. Khurram and M. Rahmani Manesh, "DDOS Attack Detection System Using Clustering Method and Active Learning Approach," Electron. Cyber Def., vol. 11, no. 3, pp. 101–118, 2023. (in Persian).dor: https://dor.isc.ac/dor/20.1001.1.23224347.1402.11.3.10.5

[48] M. Hesabi and M. De Pierre, "An Improved Method for Detecting Malware Attacks in Cloud Computing Using Crowd Learning," Electron. Cyber Def., vol. 10, no. 4, pp. 33–39, 2023. (in Persian).dor: https://dor.isc.ac/dor/20.1001.1.23224347.1401.10.4.4.4

[49] K. A. Alaghbari, H. S. Lim, M. H. M. Saad, and Y. S. Yong, "Deep Autoencoder-Based Integrated Model for Anomaly Detection and Efficient Feature Extraction in IoT Networks," IoT, vol. 4, no. 3, pp. 345–365, 2023

[50] K. N. Singh et al., "LSTM Based Stacked Autoencoder Approach for Time Series Forecasting," J. Indian Soc. Agric. Stat., vol. 77, pp. 71–78, 2023.

[51] E. Tsogbaatar et al., "DeL-IoT: A Deep Ensemble Learning Approach to Uncover Anomalies in IoT," Internet of Things, vol. 14, p. 100391, 2021.

[52] M. Kusy and P. A. Kowalski, "Weighted Probabilistic Neural Network," Information Sciences, vol. 430, pp. 65–76, 2018.

[53] I. Ullah and Q. H. Mahmoud, "A Technique for Generating a Botnet Dataset for Anomalous Activity Detection in IoT Networks," in Proc. IEEE Int. Conf. Systems, Man, and Cybernetics (SMC), Oct. 2020.

[54] I. Ullah and Q. H. Mahmoud, "A Scheme for Generating a Dataset for Anomalous Activity Detection in IoT Networks," in Advances in Artificial Intelligence (Lecture Notes in Computer Science), vol. 12109, C. Goutte and X. Zhu, Eds. Cham, Switzerland: Springer, 2020, pp. 508–520

[55] I. Ullah and Q. H. Mahmoud, "Design and Development of a Deep Learning-Based Model for Anomaly Detection in IoT Networks," IEEE Access, vol. 9, pp. 103906–103926, 2021.

[56] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A Detailed Analysis of the KDD CUP 99 Data Set," in Proc. IEEE Symp. Comput. Intell. Security Defense Applications, Jul. 2009.

[57] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the Development of Realistic Botnet Dataset in the Internet of Things for Network Forensic Analytics: Bot-IoT Dataset," Future Generation Computer Systems, vol. 100, pp. 779–796, Nov. 2019.

[58] H. Kang, D. H. Ahn, G. M. Lee, J. D. Yoo, K. H. Park, and H. K. Kim, "IoT Network Intrusion Dataset," IEEE Dataport, Tech. Rep.,2020.

[59] A. Parmisano, S. Garcia, and M. J. Erquiaga, "IoT-23: A Labeled Dataset with Malicious and Benign IoT Network Traffic," Stratosphere Laboratory, Praha, Czech Republic, Tech. Rep., 2020.

[60] H. Hindy, E. Bayne, M. Bures, R. Atkinson, C. Tachtatzis, and X. Bellekens, "Machine Learning Based IoT Intrusion Detection System: An MQTT Case Study (MQTT-IoT-IDS2020 Dataset)," in Proc. Int. Networking Conf., 2020, pp. 73–84

[61] I. Vaccari, G. Chiola, M. Aiello, M. Mongelli, and E. Cambiaso, "MQTTset: A New Dataset for Machine Learning Techniques on MQTT," Sensors, vol. 20, no. 22, p. 6578, Nov. 2020.