

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

Hadi Tarazodar¹ , Karamollah Bagherifard^{2*}, Samad Nejatian³, Hamid Parvin⁴, Razieh Malekhosseini⁵

¹ Ph.D. Student, Department of computer Engineering ,Yas.C., Islamic Azad University ,Yasuj, Iran.

hadi.tarazodar@iau.ac.ir

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

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

⁴ Associate Professor, Department of computer Engineering , NoM.C., Islamic Azad University , Noorabad Mamasani, Iran. *Parvin@iaut.ac.ir*

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

ARTICLE INFO	ABSTRACT
Article history: Article Type: Research paper Receive: 09 October 2025 Revise: 24 November 2025 Accept: 06 December 2025 Available online: 28 December 2025 Keywords: Internet of Things Anomaly Detection Stacked Autoencoder Deep Autoencoder Ensemble Learning Dynamic Feature Selection Adaptive combination of models Cybersecurity	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. A Hybrid and Intelligent Model for Anomaly Detection in Internet of Things Using Ensemble Learning and Deep Autoencoders. Journal of Electronic and Cyber Defense. 2025; 13(4), 103- 123.

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



© The Author(s). retain the copyright and full publishing rights
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 monitoring. 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.

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

^۱دانشجوی دکتری، گروه مهندسی کامپیوتر، واحد یاسوج، دانشگاه آزاد اسلامی، یاسوج، ایران. hadi.tarazodar@iau.ac.ir

^۲دانشیار، گروه مهندسی کامپیوتر، واحد یاسوج، دانشگاه آزاد اسلامی، یاسوج، ایران (نویسنده مسئول: Ka.bagherifard@iau.ac.ir)

^۳دانشیار، گروه مهندسی برق، واحد یاسوج، دانشگاه آزاد اسلامی، یاسوج، ایران. Sa.nejatian@iau.ac.ir

^۴دانشیار، گروه مهندسی کامپیوتر، واحد نورآباد ممسنی، دانشگاه آزاد اسلامی، نورآباد ممسنی، ایران. Parvin@iaut.ac.ir

^۵استادیار، گروه مهندسی کامپیوتر، واحد یاسوج، دانشگاه آزاد اسلامی، یاسوج، ایران. Malekhoseini.r@iau.ac.ir

چکیده	مشخصات مقاله
اینترنت اشیا (IoT) با فراهم کردن 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 تحریک‌پذیری آن‌ها، تهدیدات امنیتی را نیز به‌طور قابل توجهی 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 به کار گرفته شده است. از نوآوری‌های این تحقیق می‌توان به طراحی سازوکار انتخاب پویای ویژگی در لایه رمزگذار و همچنین پیشنهاد طرح وزن دهی 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 مجموعه داده معتبر از جمله IoT-23، IoT-NI، BoT-IoT، NSL-KDD ارزیابی و نتایج نشان‌دهنده دقت بالای ۹۹.۳٪ و امتیاز F1 معادل ۹۹.۲٪ در مجموعه داده ترکیبی IoT-DS2 است. نرخ مثبت کاذب (FPR) در اغلب مجموعه داده‌ها 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.	تاریخچه مقاله: نوع مقاله: علمی - پژوهشی دریافت: 1404/07/17 بازنگری: 1404/09/03 پذیرش: 1404/09/15 ارائه آنلاین: 1404/10/07 کلیدواژه‌ها: اینترنت اشیا تشخیص ناهنجاری رمزگذار خودکار پشته‌ای رمزگذار عمیق یادگیری گروهی انتخاب پویای ویژگی ترکیب تطبیقی مدل‌ها امنیت سایبری

استاد: 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 و سایبری. ۱۴۰۴؛ ۱۳ (۴): ۱۰۱-۱۲۳.

<https://doi.org/10.47176/ECDJ.2025.1669>

© نویسنده(گان) حق نشر و حقوق کامل انتشار را برای خود محفوظ می‌دارند.

ناشر: دانشگاه جامع امام حسین (ع).



OPEN ACCESS

1-مقدمه

گسترش شتابان اینترنت، زمینه‌ساز توسعه فراگیر اینترنت اشیا (IoT)^۱ شده است. سهولت دسترسی، هزینه پایین، و نقش مؤثر این فناوری در زندگی روزمره انسان‌ها ازجمله عوامل کلیدی در توسعه آن به شمار 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 [1].

اینترنت اشیا شامل مجموعه‌ای گسترده از دستگاه‌های هوشمند است که توانایی حس کردن 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 [2]. بااین‌وجود، زیرساخت‌ها و خدمات IoT به دلیل محدودیت منابع، ناهمگونی دستگاه‌ها و استفاده از پروتکل‌های نوظهور، با چالش‌های امنیتی گسترده‌ای روبرو هستند [3].

ساختار اینترنت اشیا معمولاً بر اساس معماری‌های چندلایه طراحی می‌شود که شامل لایه‌های ادراک، شبکه، پردازش، کاربرد و کسب‌وکار است [4]. 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 اشیا صنعتی (IIoT)^۲ که داده‌ها حساس بوده و زمان پاسخ‌دهی از اهمیت بالایی برخوردار است، امنیت یکی از چالش‌های اساسی به شمار می‌آید [5].

یکی از راهکارهای متداول برای مقابله با تهدیدات امنیتی، استفاده از سامانه‌های تشخیص نفوذ (IDS)^۳ است این سامانه‌ها 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 [6].

در سال‌های اخیر، یادگیری ماشین^۴ و به‌ویژه یادگیری عمیق^۵، 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 [7، 8]؛ 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^۶ را کاهش می‌دهند از سوی دیگر، پژوهش‌های اخیر نشان داده‌اند که ترکیب چند مدل در قالب یادگیری گروهی^۷ می‌تواند به بهبود دقت و پایداری تشخیص کمک کند [9]. 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 باهدف 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 قابل‌بیان است:

1. استفاده هم‌زمان از دو نوع رمزگذار خودکار پشته‌ای (SAE)^۸ و عمیق (DAE)^۹ 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،
2. به‌کارگیری ترکیب تطبیقی وزنی خروجی چهار مدل یادگیری شامل درخت تصمیم (DT)^{۱۰}، پرسپترون چندلایه (MLP)^{۱۱}، شبکه عصبی احتمالی (PNN)^{۱۲} و نوع وزنی آن (WPNN)^{۱۳} باهدف کاهش نرخ هشدار کاذب و افزایش دقت در تشخیص حملات ناشناخته.

چارچوب پیشنهادی با درنظرگرفتن محدودیت‌های منابع در محیط‌های IoT، و تمرکز بر ویژگی‌های حیاتی ترافیک شبکه طراحی شده است. عملکرد مدل با استفاده از مجموعه داده‌های معتبر NSL-KDD، BoT-IoT، IoT-23، IoT-NI، MQTT، MQTTset و IoT-DS2 ارزیابی شده و نتایج حاکی از برتری قابل‌توجه آن نسبت به روش‌های مرجع موجود است. ازجمله مهم‌ترین حملاتی که در این مقاله موردبررسی قرارگرفته‌اند

^۶ Anomaly Detection

^۷ Ensemble Learning

^۸ Stacked autoencoder network

^۹ Deep autoencoder network

^{۱۰} Decision Trees

^{۱۱} Multilayer perceptron

^{۱۲} Probabilistic Neural Network

^{۱۳} weighted PNN

^۱ Internet of Things

^۲ Industrial Internet of Things

^۳ Intrusion Detection System

^۴ Machine Learning

^۵ Deep Learning

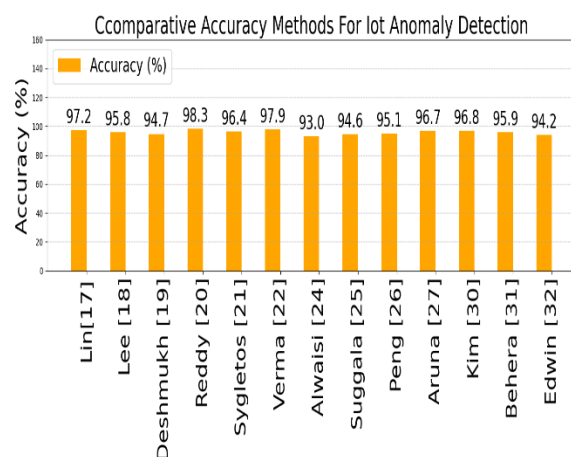
لجستیک (LR)^{۱۸} و k-نزدیک‌ترین همسایه (KNN)^{۱۹} به‌عنوان یادگیرنده پایه و LR به‌عنوان مدل نهایی تجمیع به‌کاررفته است.

گاد و همکاران [14] از الگوریتم XGBoost برای شناسایی ناهنجاری‌ها در شبکه‌های IoT استفاده کرده‌اند. این مطالعه با بهره‌گیری از سه زیرمجموعه از چهار نسخه مجموعه داده ToN_IoT و در دو سناریوی طبقه‌بندی باینری و چند کلاسه، عملکرد موفق‌تری را گزارش می‌دهد.

در مطالعه‌ای دیگر [15]، چندین الگوریتم یادگیری گروهی مانند XGBoost، Adaboost، Bagging، RF و Extra Trees برای تشخیص نفوذ در اینترنت اشیا صنعتی (IIoT) و با استفاده از مجموعه داده ToN_IoT Telemetry مورد بررسی قرار گرفته‌اند. بر اساس نتایج، XGBoost در هر دو نوع طبقه‌بندی، بهترین عملکرد را ارائه داده است.

در حوزه سیستم‌های کنترل صنعتی (SCADA)، مطالعه [16] چارچوبی مبتنی بر یادگیری گروهی با استفاده از مجموعه‌ای از شبکه‌های باور عمیق (DBN)^{۲۰} ارائه کرده که نتایج امیدبخشی را در تشخیص ناهنجاری‌ها نشان می‌دهد.

در شکل 1، 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.



شکل 1: 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 1 به بررسی

می‌توان به حملات DoS، DDoS، اسکن پورت (Port Scan)، نفوذ مبتنی بر پروتکل MQTT، حملات بات‌نت (مانند Mirai و Torii)، 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 مجموعه داده‌ها معرفی شده‌اند، بخش پنجم شامل تحلیل تجربی و نتایج آزمایش‌ها است، و نهایتاً بخش ششم به نتیجه‌گیری و پیشنهادها برای آتی اختصاص دارد.

2- کارهای مرتبط

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

مدلی بانام 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 (شامل AdaBoost، RUSBoost و Bagging) مورد ارزیابی قرار گرفته‌اند [10].

در مطالعه‌ای دیگر [11]، یک رویکرد گروهی مبتنی بر Stacking برای تشخیص ناهنجاری‌های شبکه‌های IoT پیشنهاد شده است. در این مدل، از ترکیب شبکه عصبی کانولوشنی (CNN)^{۱۴} و شبکه عصبی بازگشتی (RNN)^{۱۵} به‌عنوان یادگیرنده‌های پایه استفاده شده است. مزیت این روش، استفاده از داده‌های واقعی و ناهمگون است، که می‌تواند چالش‌های موجود در مجموعه داده‌های کوچک‌تر را کاهش دهد و بستر آموزشی مناسبی فراهم کند. خان و همکاران [12] 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 مجموعه داده ToN_IoT و در زمینه اینترنت اشیا پزشکی (IoMT)^{۱۶} به‌کار برده‌اند.

آلتایبی و الیاس [13] نیز رویکردی گروهی مبتنی بر stacking پیشنهاد کردند که در آن جنگل تصادفی (RF)^{۱۷}، DT، رگرسیون

¹⁸ Logistic Regression

¹⁹ k-Nearest Neighbors

²⁰ Deep Belief Networks

¹⁴ Convolutional Neural Network

¹⁵ Recurrent Neural Networks

¹⁶ Internet of Medical Things

¹⁷ Random Forest

این چارچوب شامل سه مرحله اصلی است: پیش‌پردازش داده‌های IoT، یادگیری مدل پایه، و ادغام آنالین 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 [40] یک مدل تشخیص نفوذ در حوزه اینترنت اشیا پزشکی (IoMT) ارائه دادند که مبتنی بر یادگیری گروهی چندمدلی و تمرکز بر شناسایی تهدیدات وب است. آن‌ها با استفاده از ویژگی‌هایی نظیر IP، اندازه بسته و نوع پروتکل، داده‌های ترافیک شبکه را تجزیه و تحلیل کرده و از طبقه‌بندهایی همچون XGBoost، KNN، درخت تصمیم، جنگل تصادفی و AdaBoost برای ترکیب و طبقه‌بندی بهره بردند.

نتایاگابیری و همکاران [41] یک رویکرد یادگیری گروهی جدید با نام OMIC معرفی 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 به کارگیری روش‌هایی مانند نمونه‌برداری تطبیقی، یادگیری حساس به هزینه، و پردازش تکه‌ای پویا، چالش‌های عدم تعادل کلاس و مقیاس‌پذیری را هدف قرار می‌دهد.

رحمان و همکاران [42] 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 [43] 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 طبقه‌بند LightGBM، XGBoost و 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 [44] یک مدل یادگیری گروهی ترکیبی برای تشخیص ناهنجاری در شبکه‌های بی‌سیم مبتنی بر

ساختار، مجموعه داده، دقت عملکرد و ویژگی‌های کلیدی 19 پژوهش اخیر طی سال‌های ۲۰۲۳ تا ۲۰۲۵ پرداخته است.

جدول ۱: مقایسه مدل‌های تشخیص ناهنجاری در اینترنت اشیا

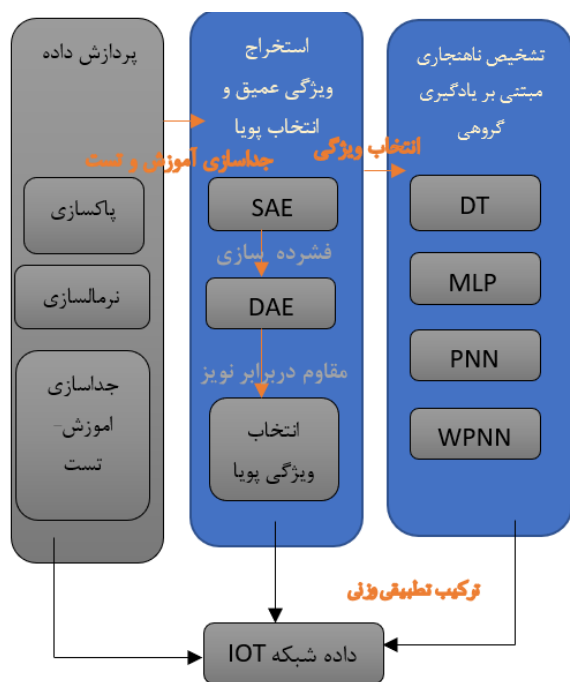
دقت (%)	نوع داده	مدل معماری	نویسنده (سال)
97.2	ICS	AE+ ML Ensemble	لین و همکاران (2025) [17]
95.8	IIoT	FL Lightweight	لی و همکاران (2025) [18]
94.7	IoT+Finance	Federated DL	دشموخ و همکاران (2025) [19]
98.3	IoT Wireless	Graph-ResNet + Hawk-Bee	ردی و همکاران (2025) [20]
96.4	IoT General	CNN Hybrid	سیگلنوس و همکاران (2025) [21]
97.9	IIoT	Ensemble + EO	ورما و همکاران (2025) [22]
91.7	IoT	DPS-DL	علی و همکاران (2025) [23]
93.0	6G-IoT	CNN Lite	الویسی (2025) [24]
94.6	SmartGrid	GANN + Blockchain	سوگولا و همکاران (2025) [25]
95.1	Industrial IoT	Adversarial CNN	پنگ و همکاران (2025) [26]
96.7	IoT Time Series	AE + LSTM+CNN	اوئرا (2025) [27]
97.5	BoT-IoT	Hybrid AE + Ensemble	ماشالی (2025) [28]
96.8	Industrial IoT	Masked AE	لی (2025) [29]
95.9	Smart Grid	MTD-AD (AE+Defense)	کیم (2025) [30]
94.2	Pumping IoT	AE+Classifier	بحارا (2025) [31]
98.1	BoT-IoT	AE + BiGRU+DBN+Walrus	ادوین (2025) [32]
97.6	IoT Malware	Autoencoder Ensemble	یان (2025) [33]
94.9	Smart City	Rule-extracted AE	فان (2025) [34]
95.2	Cross-layer IoT	Multilayer AE	سارانیا (2025) [35]
96.3	Smart Cities	DASVDD	نایت (2025) [36]
93.8	Finance IoT	Graph AE	کومار (2025) [37]
96.0	Healthcare IoT	Conv-AE + Blockchain	برزنجانی (2023) [38]

وو و همکاران [39] یک چارچوب تشخیص ناهنجاری تطبیقی به نام AEWAE^{۲۱} را معرفی کردند که از چهار الگوریتم یادگیری آنالین در قالب یک ساختار یادگیری گروهی ترکیبی بهره می‌برد.

²¹ Adaptive Exponentially Weighted Average Ensemble

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 قابل توجه 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 با دقت بالا تلفیق می‌کند. سوم، تجمیع رمزگذارهای خودکار عمیق و گروهی از یادگیرنده‌های 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 نمایش داده شده است.



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

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 [45]، [46]، [47] و [48] به این موضوع پرداخته شده است.

با وجود عملکرد قابل توجه 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 [17] AE+ML Ensemble یا [21] CNN Hybrid که 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. با این حال، 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 پویای ویژگی‌ها، 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. از این رو، نیاز به طراحی چارچوبی هوشمند، سازگار و دقیق که بتواند بر این محدودیت‌ها غلبه کند، به شدت احساس می‌شود. پژوهش حاضر باتکیه بر 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.

۳-۲- مدل پیشنهادی

مدل پیشنهادی این مقاله باهدف تشخیص ناهنجاری در شبکه‌های اینترنت اشیا، از یک چارچوب چندمرحله‌ای بهره می‌برد که بر پایه ترکیب رمزگذارهای عمیق و الگوریتم‌های یادگیری گروهی طراحی شده است. این چارچوب شامل سه جز اصلی است: (۱) پیش‌پردازش داده‌ها، (۲) استخراج و انتخاب

²³ Cleaning

²⁴ Normalization

²⁵ Missing Values

²⁶ Noise

²² Deep neural networks

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 در عین حال 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.

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 ناهنجار^{۲۸} جهت آموزش مدل تشخیص ناهنجاری استفاده می‌گردد.

فرض کنید مجموعه داده‌های ورودی به صورت $X_n = \{x_1, x_2, \dots, x_n\}$ ، $X_n \in \mathbb{R}^n$ باشد و همچنین بردار خروجی بازسازی شده به صورت $X'_n = \{x'_1, x'_2, \dots, x'_n\}$ 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 به صورت رابطه (1) 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. به طور مشابه، رمزگشا خروجی را از طریق رابطه (2) 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، به گونه‌ای بهینه‌سازی می‌شوند که خطای بازسازی بین ورودی و خروجی، حداقل شود. در این مقاله، دو نوع رمزگذار برای استخراج و نمایش ویژگی‌ها به کار گرفته شده است:

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

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 ← LoadData(input_path)
3:   preprocessed_data ← Preprocess(raw_data)
4:
5:   # SAE for hierarchical feature extraction
6:   features_SAE ← SAE_Encoder(preprocessed_data)
7:
8:   # DAE for robust compressed representation
9:   features_DAE ← DAE_Encoder(features_SAE)
10:
11:  # Dynamic feature selection based on activation weights
12:  optimized_features ← 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 ← 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 ← 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 ← 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

```

²⁷ Legitimate

²⁸ Anomal

²⁹ Encoder

³⁰ Decoder

مکانیزم انتخاب پویای ویژگی مبتنی بر تحلیل ضرایب فعال سازی در لایه های میانی رمزگذار طراحی شده است. پس از استخراج بردار ویژگی فشرده شده از طریق رمزگذارهای SAE و DAE، میزان فعال سازی هر نرون (ویژگی) در طول کل داده های آموزشی محاسبه می شود. اگر میانگین فعال سازی یک ویژگی از آستانه مشخصی کمتر باشد، آن ویژگی به عنوان ویژگی کم اهمیت شناخته شده و حذف می گردد. این آستانه به صورت تجربی و با تحلیل توزیع فعال سازی ها تنظیم می شود.

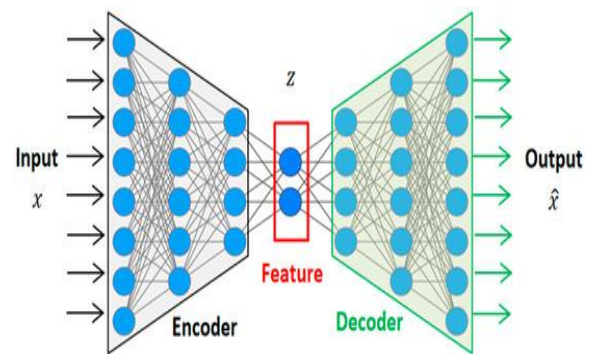
این فرایند به صورت کاملاً پویا و تطبیقی انجام می شود و در هر نوبت آموزش، ویژگی های مؤثر به صورت خودکار تقویت و ویژگی های کم اثر حذف می شوند. در نتیجه، این روش برخلاف روش های ایستا مانند تحلیل مؤلفه های اصلی (PCA)³²، اطلاعات متقابل (MI)³³ و الگوریتم های درخت تصمیم با ساختار شبکه عمیق کاملاً یکپارچه بوده و بدون نیاز به اجرای جداگانه عمل می کند. مقایسه روش پیشنهادی با روش های ذکر شده نشان داد که استفاده از انتخاب پویای ویژگی، باعث افزایش دقت شناسایی ناهنجاری، کاهش نرخ هشدارهای کاذب و بهبود پایداری مدل در مواجهه با داده های نویزی شده است. جدول 2 این مقایسه را نشان می دهد.

جدول 2: مقایسه روش پیشنهادی و روش های انتخاب ویژگی

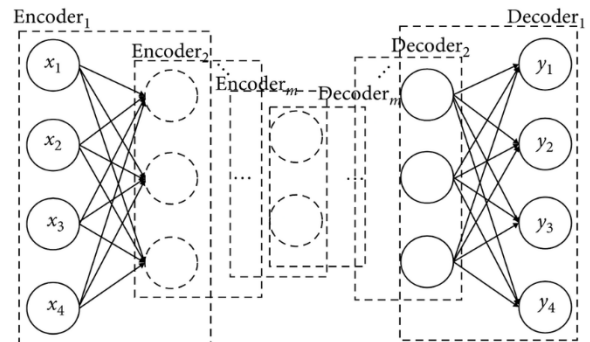
معیار مقایسه	روش پیشنهادی	PCA	اطلاعات متقابل (MI)	مبتنی بر درخت تصمیم
نوع روش	پویا، درون-مدلی، وابسته به شبکه	آماري، ایستا	آماري، ایستا	یادگیری محور، برون مدلی
تطبیق با داده	بله	خیر	خیر	محدود
جداسازی قبل از آموزش	ندارد	دارد	دارد	دارد
یکپارچگی با شبکه عصبی عمیق	کامل	ندارد	ندارد	ندارد
حذف ویژگی نویز و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

مزیت اصلی رمزگذارهای عمیق، توانایی در استخراج نمایش های سطح بالا و انتزاعی از داده ها است که در بهبود عملکرد مدل های تشخیص ناهنجاری نقش مهمی ایفا می کند.

همان طور که در شکل 3 نشان داده شده، ساختار رمزگذار خودکار عمیق شامل چندین لایه فشرده سازی و بازسازی است. همچنین در شکل 4 ساختار رمزگذار پشته ای ترسیم شده است که در آن هر لایه به صورت تدریجی ویژگی های ورودی را فشرده سازی کرده و به لایه بعد منتقل می کند. در این رمزگذارها، نوع کم کامل³¹ مورد استفاده قرار گرفته است؛ به طوری که تعداد نرون های لایه های پنهان کمتر از ورودی بوده و در نتیجه، شبکه مجبور به یادگیری نمایش های کلیدی تر از داده ها می شود.



شکل 3: رمزگذاری خودکار عمیق [49]



شکل 4: رمزگذاری خودکار پشته ای [50]

در این پژوهش، رمزگذارهای SAE و DAE برای استخراج ویژگی های کلیدی و کاهش ابعاد داده به کار گرفته شده اند. SAE با یادگیری سلسله مراتبی، الگوهای رفتاری شبکه را به خوبی مدل سازی می کند و DAE با حذف نویز، بازنمایی فشرده و مؤثری از داده ها ارائه می دهد. همچنین، با استفاده از سازوکار انتخاب پویای ویژگی، ویژگی های کم اهمیت حذف و ویژگی های مؤثر تقویت می شوند. این ترکیب باعث بهبود دقت، کاهش هشدارهای کاذب و افزایش توان شناسایی حملات ناشناخته در مدل تشخیص نفوذ می شود.

³² Principal Component Analysis

³³ Mutual Information

³¹ Undercomplete

3-3-3- 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 در نظر گرفتن 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 سه لایه پنهان، هر یک با ۱۰۰ نورون، استفاده شده است. در تمامی لایه‌ها، تابع فعال‌سازی ReLU به صورت $\sigma(z) = \max(0, z)$ به کار گرفته شده 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 مورد استفاده 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 کیفیت صورت می‌گیرد تا بهترین تفکیک ممکن حاصل شود. در این مقاله، معیار آنتروپی^{۳۷} به عنوان شاخص اصلی برای ارزیابی کیفیت تقسیم‌بندی انتخاب شده است. گره‌های میانی درخت، وظیفه انجام تصمیم‌گیری مرحله به مرحله و هدایت نمونه‌ها به سمت برجسب‌های 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 چهار لایه اصلی تشکیل شده است: لایه ورودی، لایه الگو، لایه جمع و لایه خروجی (مطابق با شکل ۳). این شبکه را می‌توان به عنوان 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 ورودی x ، نمونه آموزشی x_i و کلاس C_k مطابق رابطه (3) محاسبه می‌کند:

$$p(x | x_i, C_k) = \frac{1}{\sigma} \omega\left(\frac{x - x_i}{\sigma}\right) \quad (3)$$

که در آن x_i نمونه نام و x نمونه ورودی $\omega(\cdot)$ تابع وزن و σ پارامتر همواسازی 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 (4) تعریف شده است تخمین زده می‌شود.

$$\hat{f}_{C_k}(x) = \frac{1}{n_{C_k} \sigma} \sum_{i=1}^{n_{C_k}} \omega\left(\frac{x - x_i}{\sigma}\right) \quad (4)$$

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 همواسازی 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

³⁸ Feedforward Neural Network

³⁹ Linear Discriminant Analysis

⁴⁰ Kernel Discriminant Analysis

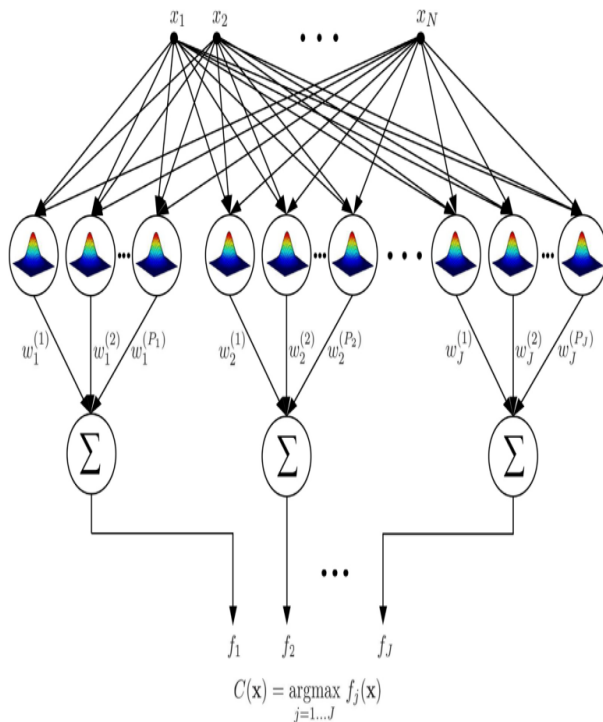
⁴¹ Radial Basis Function

³⁴ False Positive Rate

³⁵ FeedForward

³⁶ Backpropagation

³⁷ Entropy



شکل 6: معماری WPNN [52]

با استفاده از تخمین چگالی پنجره‌ای پارزن وزنی در رابطه (6)، می‌توان تابع چگالی احتمال کلاس C_k را به صورت چندبعدی و ماتریسی بیان کرد:

$$\hat{f}_{C_k}(x) = \frac{1}{\sum_{i=1}^{n_{C_k}} w_i \det(H)} \sum_{i=1}^{n_{C_k}} w_i \cdot \frac{1}{s_i^N} k\left(\frac{(x - x_i)^T H^{-1}}{s_i}\right) \quad (7)$$

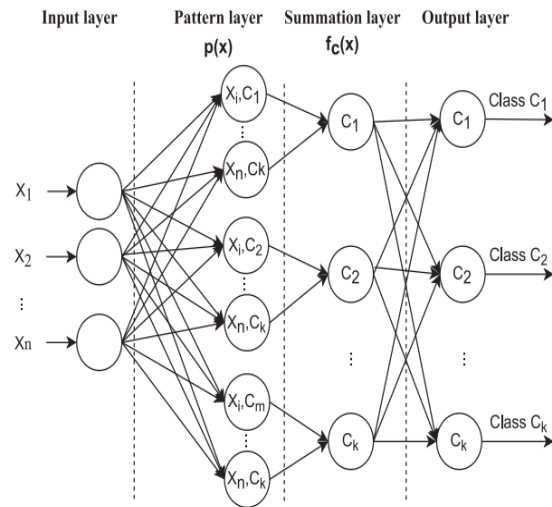
که در آن، (H) ماتریس هموارسازی قطری شامل پارامترهای h_j ، s_i ضریب اصلاح نمونه و $ik(\cdot)$ کرنل چندبعدی (مثلاً کرنل کوشی) می‌باشد. تصمیم‌گیری کلاس در رابطه (8) برای نمونه جدید x بر اساس قانون بیشینه احتمال است:

$$c(x) = \arg \max_k \hat{f}_{C_k}(x) \quad (8)$$

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

$$w_j = \frac{1}{\|a_j\|_n} a_j \cdot a_j = \left[\frac{1}{P_j} \sum_{p=1}^{P_j} \|\nabla \hat{f}_j^{(p,r)}\|_n^2 \right]^{1/2} \quad (9)$$

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 5 معماری شبکه عصبی احتمالی را نشان می‌دهد.



شکل 5: معماری شبکه عصبی احتمالی (PNN) [51]

۳-۳-۴- 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 به منظور افزایش دقت طبقه‌بندی و کاهش اثر داده‌های پرت یا نمونه‌های کم‌کیفیت انجام می‌گیرد. شکل 6 معماری شبکه عصبی احتمالی وزنی را نشان می‌دهد.

تابع چگالی احتمال شرطی در لایه الگو WPNN به صورت رابطه (5) اصلاح می‌شود:

$$p(x | x_i, C_k) = \frac{w_i}{\sigma} \omega\left(\frac{x - x_i}{\sigma}\right) \quad (5)$$

که در آن w_i وزن اختصاص‌یافته به نمونه 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 (6)، تجمع مقادیر را بر اساس وزن‌ها انجام می‌دهد:

$$\hat{f}_{C_k}(x) = \frac{1}{\sum_{i=1}^{n_{C_k}} w_i \sigma} \sum_{i=1}^{n_{C_k}} w_i \cdot \omega\left(\frac{x - x_i}{\sigma}\right) \quad (6)$$

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.

دقیق تر، هر یک از این مدل‌ها با تحلیل بردار ویژگی فشرده شده تولید شده توسط رمزگذارها، احتمال تعلق نمونه به کلاس ناهنجار را محاسبه کرده و خروجی نهایی از طریق یک سازوکار ترکیب تطبیقی وزنی حاصل می‌شود.

که، α_j بردار حساسیت‌های تجمع شده کلاس j ، P_j تعداد نمونه‌های کلاس j و $\nabla f_j^{(p,r)}$ گرادیان KDE نسبت به ورودی‌ها برای نمونه p است.

۵-۳-۳- چارچوب یادگیری گروهی عمیق

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

$$y = \arg \max_{c \in \mathcal{C}} \sum_{j=1}^4 \alpha_j \cdot p_j(c | x) \quad (10)$$

که در آن، α_j وزن یادگیرنده j -ام، $p_j(c | x)$ احتمال تخصیص داده شده به کلاس c توسط یادگیرنده j ، و $\mathcal{C}$ 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 x ، یک بردار احتمالاتی است:

$$p_j(x) = [p_j(c_1 | x), p_j(c_2 | x), \dots, p_j(c_K | x)] \quad (11)$$

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:

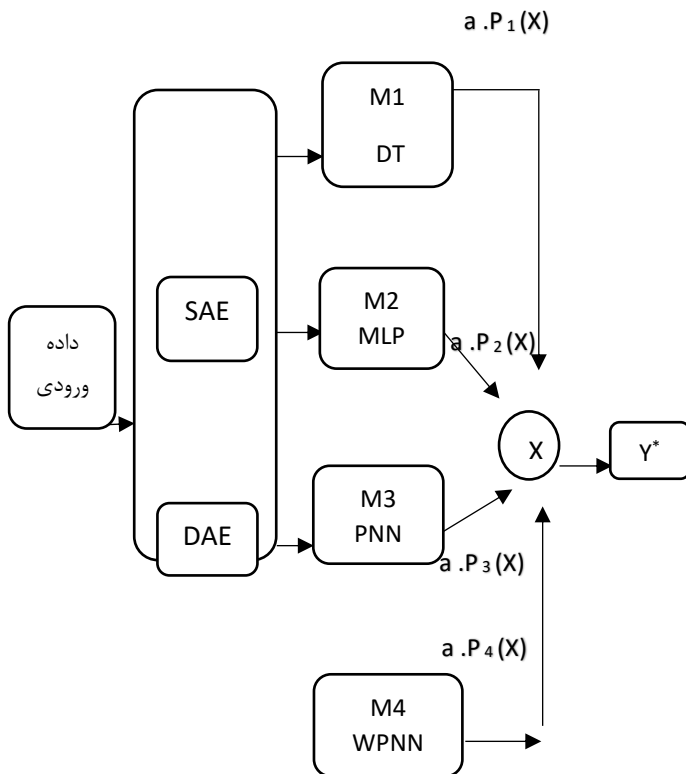
$$\sum_{j=1}^4 \alpha_j = 1, \alpha_j \geq 0 \quad (12)$$

خروجی نهایی طبقه‌بندی مدل گروهی $\mathcal{Y}^*$ به صورت رابطه (13) تعریف می‌شود:

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

نمودار بلوکی مدل یادگیری گروهی عمیق به صورت شکل 7 می‌باشد.

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. به عبارت



شکل 7: نمودار بلوکی مدل یادگیری گروهی عمیق

در معماری پیاده‌سازی پیشنهادی، تشخیص ناهنجاری‌ها توسط گره‌های لبه^{۴۲} یا گره‌های میان‌افزار^{۴۳} 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^{۴۴} 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.

4- مجموعه داده‌ها

مجموعه داده‌های BoT-IoT [53]، IoT-NI [54]، IoT-23 [55]، MQTT [56]، MQTTset [56] و NSL-KDD [57] برای ارزیابی مدل‌های پیشنهادی مورداستفاده قرار گرفتند. اولین مرحله شامل پردازش فایل‌های pcap مجموعه داده‌های BoT-IoT

⁴² Edge Nodes

⁴³ Fog Nodes

⁴⁴ Gateways

ویژگی‌های غیرعددی به مقادیر عددی تبدیل شده و نمونه‌های تکراری در فایل‌های CSV حذف شدند. سپس داده‌ها در بازه (-1.1) تا (1.1) نرمال شدند تا مقادیر پرت کاهش یافته و سرعت پردازش افزایش یابد. داده‌های ناقص با مقدار میانگین جایگزین شده‌اند. جدول 3 خلاصه‌ای از کلاس‌ها و تعداد نمونه‌های هر مجموعه داده را، با در نظر گرفتن حذف و حفظ نمونه‌های افزوده، ارائه می‌کند.

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، DoS، DDoS، Scan و Data Theft است. کلاس DoS و DDoS با هم ترکیب شده‌اند.
 - IoT-NI: شامل حملات DoS، MITM، Mirai و Scan است. داده‌ها از ترافیک شبکه بی‌سیم جمع‌آوری شده‌اند.
 - IoT-23 توسعه‌یافته در آزمایشگاه Stratosphere دانشگاه CTU، 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 مجموعه داده‌ها IoT-DS2:

برای ایجاد مجموعه داده جامع‌تر، مجموعه‌های BoT-IoT، IoT-NI، IoT-23، MQTT و MQTTset ترکیب شده‌اند و مجموعه داده جدیدی به نام IoT-DS2 تشکیل شده است. این مجموعه داده شامل ۱۸ کلاس حمله و یک کلاس عادی است. نمونه‌های داده در IoT-DS2 به شرح جدول 4 تقسیم‌بندی شده‌اند. 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 به کار گرفته شد. برای مجموعه داده NSLKDD از روش انتخاب ویژگی استفاده نشد و همه ویژگی‌ها در مدل‌ها لحاظ شدند.

از میان مجموعه داده‌های 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

[58]، [59] Network Intrusion IoT، [60] IoT-23، MQTT-IDS2020 [61] و MQTTset [62] بود.

در مرحله اول، فایل‌های pcap این مجموعه داده‌ها استخراج و پردازش شدند تا ۸۰ ویژگی به صورت فایل CSV تولید گردد. برچسب‌گذاری نمونه‌ها بر اساس معیارهای از پیش تعریف شده برای هر مجموعه داده انجام شده است. نمونه‌هایی که شامل شناسه جریان، IP منبع، پورت مبدأ، IP مقصد و مهر زمانی برای مشخص کردن ارتباطات در شبکه IoT بودند، از تمامی مجموعه‌ها حذف گردیدند.

جدول 3: کلاس‌ها و نمونه‌های مجموعه داده‌های BoT-IoT، IoT-

IoT-23، NI 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	

$$Accuracy = \frac{(TP + TN)}{(TP + FP + TN + FN)} \quad (14)$$

$$Precision = \frac{TP}{(TP + FP)} \quad (15)$$

$$Recall = Sensitivity = \frac{TP}{(TP + FN)} \quad (16)$$

$$F1 \text{ score} = 2 \times \frac{(Precision \times Recall)}{(Precision + Recall)} \quad (17)$$

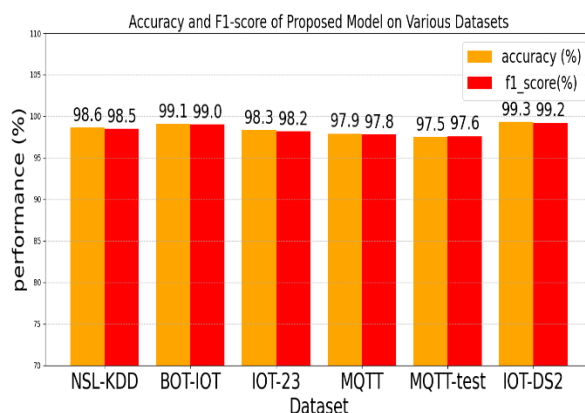
$$FPR = \frac{FP}{(FP + TN)} \quad (18)$$

$$FNR = \frac{FN}{(FN + TP)} \quad (19)$$

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

5-1- تحلیل معیار دقت و امتیاز F1

در شکل 8 و جدول 5، عملکرد مدل پیشنهادی در دو معیار دقت و امتیاز F1 بر روی چند مجموعه داده معتبر نشان داده شده است. دقت‌ها همگی بالای 97 درصد هستند که نشان‌دهنده قابلیت اطمینان بالای مدل برای تشخیص ناهنجاری‌ها است. بیشترین دقت در مجموعه داده BoT-IoT با 99.1٪ و کمترین دقت در MQTtset با 97.5٪ ثبت شده است. امتیاز F1 نیز به طور مشابه بین 97.6٪ تا 99.0٪ قرار دارد که تعادل خوبی بین فراخوانی و دقت مدل را نشان می‌دهد.



شکل 8: عملکرد مدل پیشنهادی در معیار دقت و F1

مدل پیشنهادی روی مجموعه داده NSL-KDD موفق به کسب دقت 98.6٪ و امتیاز F1 برابر با 98.5٪ 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،

پوشش داده شود. ترکیب این مجموعه‌ها امکان ارزیابی جامع مدل در شرایط گوناگون و افزایش اعتبار نتایج را فراهم می‌کند.

جدول 4: کلاس‌ها و نمونه‌های مجموعه داده IoT-DS2 و

زیرمجموعه‌های آن

دسته	BoT-IoT	IoT-NI	IoT-23	MQ TT	MQT Tset	IoT-DS2
Normal	-	-	4253 672	-	-	2000 000
DDoS	1742 0085	-	-	-	-	5000 00
DoS	-	593 91	-	-	-	5939 1
MITM ARP Spoonfin g	-	329 09	-	-	-	3290 9
Mirai	-	366 971	-	-	-	3669 71
MQTT Brutefo rce	-	-	-	2001 972	-	5000 00
Sparta	-	-	-	1217 198	-	5000 00
Theft	4457 99	-	-	-	-	4457 99
Attack	-	-	1699 608	-	-	5000 00
C&C	-	-	2061 2	-	-	2061 2
File Downl oad	-	-	7707	-	-	7707
Heartbe at	-	-	1264 8	-	-	1264 8
Okiru	-	-	1290 8506	-	-	5000 00
OS Scan	9462 68	-	-	-	-	5000 00
Port Scan	-	-	2999 999	-	-	5000 00
Torii	-	-	2449 2	-	-	2449 2
MQTT Flood	-	-	-	-	7775 6	7775 6
Malfor med	-	-	-	-	3535	3535
SlowIT e	-	-	-	-	3044	3044

5- 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 14 تا 19 ارائه شده است و ROC اعتبارسنجی شدند.

⁴⁵ False Negative Rate

طراحی رمزگذارهای خودکار عمیق و به کارگیری الگوریتم ترکیب تطبیقی وزن دهی در چارچوب یادگیری گروهی نسبت داد.

5-2- تحلیل معیار نرخ مثبت کاذب و نرخ منفی کاذب

معیارهای نرخ مثبت کاذب (FPR) و نرخ منفی کاذب (FNR) از مهم ترین شاخص ها در ارزیابی کارایی سیستم های تشخیص ناهنجاری به ویژه در زمینه اینترنت اشیا هستند.

- (FPR) میزان نمونه های قانونی است که به اشتباه به عنوان ناهنجاری شناسایی شده اند. این مقدار پایین بودن آن نشان دهنده کاهش هشدارهای کاذب است.
- (FNR) میزان نمونه های ناهنجار است که به اشتباه به عنوان قانونی طبقه بندی شده اند. کاهش این نرخ اهمیت بسیار زیادی در شناسایی دقیق تهدیدات دارد.

جدول 6: نرخ مثبت کاذب و منفی کاذب برای مجموعه داده ها

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 6 و نمودار مربوطه (شکل ۹) می توان مشاهده کرد که مدل پیشنهادی توانسته است نرخ مثبت کاذب را در سطح پایینی حفظ کند، به ویژه در مجموعه داده هایی مانند NSL-KDD و BoT-IoT که به ترتیب کمترین مقادیر FPR برابر با ۱.۰٪ و ۱.۲٪ را نشان می دهند. این موضوع بیانگر کاهش هشدارهای نادرست و بهبود کارایی عملیاتی سیستم است. نرخ منفی کاذب نیز در تمامی مجموعه داده ها کمتر از ۲٪ گزارش شده که نشان دهنده دقت بالای مدل در شناسایی واقعی ناهنجاری ها و تهدیدات است. این ویژگی، در سناریوهای امنیتی حساس که شناسایی نشدن حملات می تواند پیامدهای جدی به دنبال داشته باشد، از اهمیت ویژه ای برخوردار است. بالاترین FPR و FNR مربوط به مجموعه داده MQTTset است که ممکن است به دلیل پیچیدگی های 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 و FNR، قابلیت اطمینان بالایی در تشخیص ناهنجاری ها ارائه می دهد.

نشان می دهد که مدل توانسته است بین نرخ شناسایی حملات و کاهش هشدارهای کاذب تعادل مناسبی برقرار کند.

جدول 5: عملکرد مدل پیشنهادی در معیار دقت و امتیاز FI

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

در مجموعه داده BoT-IoT، مدل دقت ۹۹.۱٪ و F1-score برابر با ۹۹ را ثبت کرده است. این میزان دقت بسیار بالا نشان می دهد که مدل پیشنهادی توانسته است به خوبی با پیچیدگی و حجم بالای داده های مربوط به ترافیک بات نت های 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 مجموعه داده IoT-23 به دقت ۹۸.۳٪ و F1-score معادل ۹۸.۲٪ دست یافته است. این نتایج نشان دهنده قدرت مدل در شناسایی تهدیدات در محیط های واقعی تر و متنوع تر اینترنت اشیا است، جایی که انواع مختلف حملات و داده های پیچیده تر وجود دارد. حفظ دقت بالا در این مجموعه بیانگر انعطاف پذیری و سازگاری مدل در محیط های پر تغییر و چند کلاسه است.

مدل پیشنهادی برای داده های MQTT موفق به کسب دقت ۹۷.۹٪ و F1-score برابر ۹۷.۸٪ شده است. با توجه به خصوصیات پروتکل MQTT که مختص اینترنت اشیا و انتقال پیام های سبک است، این دقت نشان می دهد که مدل قادر است الگوهای حملات و ناهنجاری های مختص این پروتکل را به خوبی تشخیص دهد. این امر برای امنیت در لایه انتقال داده های اینترنت اشیا بسیار حیاتی است.

نتایج به دست آمده از مجموعه داده MQTTset شامل دقت ۹۷.۵٪ و F1-score معادل ۹۷.۶٪ است. این ارقام، مدل پیشنهادی را در دسته بندی دقیق انواع حملات و رفتارهای غیرعادی شبکه های IoT با استفاده از پروتکل MQTT قرار می دهد. عملکرد پایدار مدل روی این مجموعه داده نشان می دهد که استراتژی انتخاب ویژگی و یادگیری گروهی اثرگذار بوده و قابلیت تعمیم مدل را بهبود بخشیده است.

در مجموعه داده ترکیبی IoT-DS2 که از ادغام چند مجموعه داده مختلف تشکیل شده و شامل هجده کلاس حمله و یک کلاس نرمال است، مدل پیشنهادی به دقت ۹۹.۳٪ و F1-score معادل ۹۹.۲٪ دست یافته است. این عملکرد عالی نشان دهنده توانایی برجسته مدل در مقابله با پیچیدگی های ترکیب داده های متعدد و تشخیص دقیق انواع مختلف تهدیدات است. بهبود عملکرد مدل در این مجموعه داده نسبت به سایر مجموعه ها را می توان به

استاندارد بودن این مجموعه داده قابل انتظار است. عملکرد مدل روی مجموعه داده‌های پیچیده‌تر مانند MQTTset نیز بسیار قابل قبول بوده و توانسته است حفظ دقت و شناسایی بالا را تضمین کند.

4-5- تحلیل نمودار ROC⁴⁶

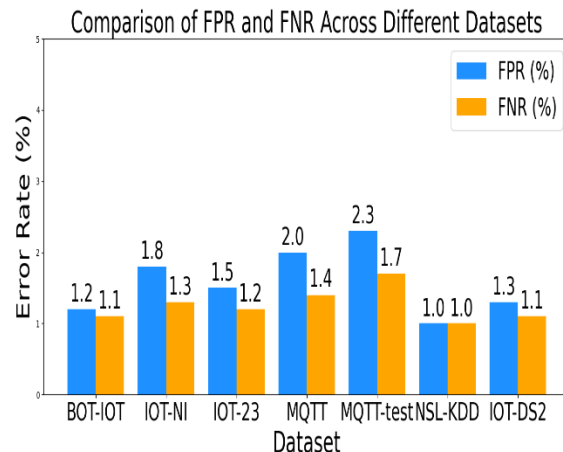
نمودار ROC یکی از مهم‌ترین ابزارها برای ارزیابی عملکرد مدل‌های تشخیص ناهنجاری است. این نمودار رابطه بین نرخ مثبت کاذب و حساسیت را در آستانه‌های مختلف نمایش می‌دهد. معیار کلیدی در این تحلیل، مقدار AUC⁴⁷ است که نشان‌دهنده توانایی مدل در تمایز قائل شدن بین کلاس‌های مثبت و منفی است.

- مقدار AUC بین 0.5 تا 1 تغییر می‌کند، به طوری که مقدار نزدیک به 1 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.

جدول 7: 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 مجموعه داده‌ها نزدیک به عدد 1 است، که نشان‌دهنده توانایی بالا در تشخیص دقیق نمونه‌های ناهنجار از نمونه‌های قانونی است. بالاترین مقدار AUC مربوط به مجموعه داده NSLKDD با عدد 0.987 می‌باشد که بیانگر تشخیص تقریباً بی‌نقص در این مجموعه داده است. کمترین مقدار AUC در میان مجموعه داده‌ها مربوط به BoT-IoT با 0.865 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.

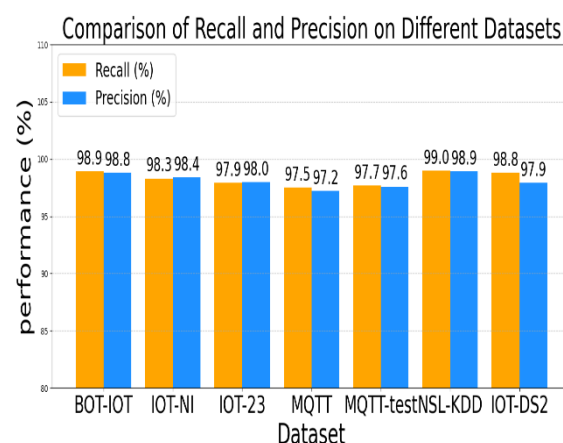


شکل 9: نمودار مقایسه FNR و FPR در مدل پیشنهادی روی مجموعه داده‌های مختلف

3-5- 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 10 بیانگر عملکرد بسیار مطلوب مدل پیشنهادی در شناسایی نمونه‌های ناهنجار است، به گونه‌ای که حساسیت همه مجموعه داده‌ها بالاتر از 97.4 درصد می‌باشد. این موضوع نشان‌دهنده توانایی بالا در کشف حملات و ناهنجاری‌های مختلف در محیط‌های اینترنت اشیا است.



شکل 10: نمودار حساسیت و صحت مدل پیشنهادی روی مجموعه داده‌های مختلف

صحت مدل در تمامی مجموعه داده‌ها 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

⁴⁶ Receiver Operating Characteristic

⁴⁷ Area Under the Curve

5-5- مقایسه با سایر روش‌های مشابه

در شکل 11، 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 98٪ است که از بیشتر مدل‌های دیگر، مانند ML Ensemble [17] با 97.2٪ و CNN Lite [24] با 93.0٪ پیشی گرفته است. در حوزه‌های خاص مانند Industrial IoT و Smart Grid، مدل‌های تخصصی همچون Graph-ResNet + Hawk-Bee [20] و MTD-AD [29] دقت بالا اما کمتر یا نزدیک به مدل پیشنهادی ما دارند.

پژوهش [17] روش که از ترکیب چندین مدل یادگیری ماشین استفاده کرده، به دقت 97.2٪ دست یافته است. این تفاوت نشان‌دهنده تأثیر بهینه‌سازهای انجام شده در معماری پیشنهادی است. این مدل فاقد سازوکار انتخاب پویای ویژگی است که در روش پیشنهادی اعمال شده و منجر به دقت 99.3٪ شده است.

در [18] 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 [20] با معماری ترکیبی Graph-ResNet و الگوریتم Hawk-Bee به دقت 98.3٪ دست یافته‌اند.

پژوهش [22] با به کارگیری چارچوب گروهی و بهینه‌ساز تعادل به دقت 97.9٪ رسیده که مجدداً عملکرد پایین‌تری نسبت به روش حاضر دارد.

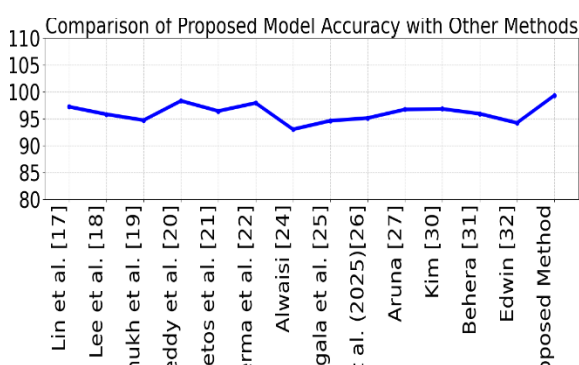
روش‌هایی مثل [24] که با هدف کاهش هزینه محاسباتی و سبک‌سازی طراحی شده‌اند، هرچند زمان آموزش و استنتاج کمتری دارند، اما به دلیل ضعف در لایه‌های استخراج ویژگی عمیق و عدم مدیریت مناسب داده‌های نامتوازن، دقت پایین‌تری نسبت به روش پیشنهادی کسب کرده‌اند.

روش [19] با یادگیری عمیق مشارکتی دقت 94.7٪ را کسب کرده و در حفظ حریم خصوصی مؤثر است، اما در تشخیص ناهنجاری‌های پیچیده نسبت به روش پیشنهادی ضعف دارد. روش [23] با معماری سبک DPS-DL و دقت 91.7٪ در تحلیل داده‌های پیچیده و غیرخطی نسبت به روش پیشنهادی دقت پایینی دارد.

روش [25] با ترکیب GANN و بلاکچین به دقت 94.6٪ رسیده اما در برابر حملات نوین IoT با افت دقت روبروست. روش [26] با AE+LSTM+CNN دقت 96.7٪ کسب کرده و در تحلیل

داده‌های زمانی قوی است، اما در داده‌های نامتوازن نسبت به روش پیشنهادی ضعف دارد. روش [29] با Masked AE دقت 96.8٪ 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 [30] با MTD-AD دقت 95.9٪ 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 [32] با ترکیب چندین شبکه پیچیده و الگوریتم Walrus به دقت 98.1٪ دست یافته‌اند، پیچیدگی بالای معماری آن‌ها باعث افزایش هزینه محاسباتی شده است. که باعث شده دقت کمتری نسبت به روش پیشنهادی داشته باشد.



شکل 11: 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 16 گیگابایت RAM انجام شده‌اند. زمان آموزش کامل مدل پیشنهادی برای مجموعه داده IoT-DS2 حدود ۲۷ دقیقه و زمان تست برای ۱۰۰۰۰ نمونه جدید حدود ۱.۳ ثانیه گزارش شده است. پیچیدگی زمانی بخش رمزگذار خودکار با تعداد لایه‌های L و ابعاد ویژگی d، به صورت 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 $O(M \times n \times d)$ خواهد بود.

اگرچه این مدل پیشنهادی به دلیل 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. به علاوه، با توجه به اجرای مدل در گره‌های لبه یا سرور، مصرف منابع در گره‌های حسگر نهایی نخواهد بود.

[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. Krzyszoń, 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. Elsis, 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

6- 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 استفاده از الگوریتم‌های متنوعی همچون PNN و 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 مجموعه داده معتبر از جمله NSL-KDD، IoT-23 و BoT-IoT نشان داد که چارچوب ارائه شده 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 داده‌های IoT، 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.

7- مراجع

[1] A. Čolaković, B. Karahodža, and A. H. Džbur, "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.

- 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. Benteleb, J. Ndikumagege, 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](https://dor.isc.ac/dor/20.1001.1.23224347.1403.12.22.2).
- 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. Bakhiet, 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

- [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. Tavallaei, 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.
- [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.