Journal of Information and Communication Technology

Volume 18, Issue 68-69, Spring and Summer 2026, pp. 130-147

Intelligent Detection of DDoS Attacks in Internet of Things Devices Using a Hybrid Approach of CNN, LSTM, and FFNN Neural Networks

Mandana Rostami[1*], Pouya Derakhshan Barjouei[2], Elahe Moradi[3]

[1] Department of Computer Engineering and IT Engineering, SR.C., Islamic Azad University, Tehran, Iran
[2] Artificial Intelligence and Data Analysis Research Center, Department of Electrical Engineering, SR.C., Islamic Azad University, Tehran, Iran
[3] Department of Electrical Engineering, YI.C., Islamic Azad University, Tehran, Iran

Received: 16 September 2025, Revised: 04 May 2026, Accepted: 28 July 2026
Paper type: Research

Abstract

As the use of Internet of Things (IoT) devices expands, cyber-attacks, especially DDoS, have become more sophisticated, making their detection a fundamental challenge. Research shows that deep neural networks perform well due to their compatibility with large volumes of data. This study investigates and compares the performance of deep learning models for detecting cyber-attacks in distributed networks.Four deep learning models, including the CNN, LSTM, and FFNN neural networks, as well as their combination (CNN-FFNN and CNN-LSTM), were evaluated for analyzing network traffic data. The models were trained on the Bot-IoT dataset, and their performance was measured based on accuracy. The results show that the combination of CNN and LSTM, by leveraging both spatial features and temporal dependencies, achieves the highest accuracy in detecting complex attacks like DDoS.This model can extract hidden features from raw data and simulate the temporal relationships of attacks, which is crucial for identifying gradual and complex threats in IoT and Fog computing environments. The combination of CNN and FFNN also demonstrated a notable performance in detecting faster threats with less complexity. Ultimately, this research emphasizes the importance of combining deep learning models to improve the accuracy of cyber-attack detection systems and proposes solutions based on distributed architectures for the security of IoT and Fog networks.

Keywords: Convolutional Neural Network, Feed Forward Neural Network, Long Short-Term Memory, Internet of Things, Deep Learning.

[*] Corresponding Author's email: mandana.rostami@iau.ac.ir

دوفصلنامه
فناوری اطلاعات و ارتباطات ایران

سال هجدهم، شماره‌های ۶۸ و ۶۹ ، بهار و تابستان ۱۴۰۵، صفحه ۱۳۰ الی ۱۴۷

تشخیص هوشمند حملات DDoS در دستگاه‌های اینترنت اشیا با استفاده از رویکرد ترکیبی شبکه‌های عصبی CNN، LSTM و FFNN

ماندانا رستمی[1*]، پویا درخشان برجوئی[2]، الهه مرادی[3]

[1]گروه مهندسی کامپیوتر و مهندسی فناوری اطلاعات واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران.

[2]مرکز تحقیقات هوش مصنوعی و تجزیه و تحلیل داده، گروه مهندسی برق، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران.

[3]گروه مهندسی برق، واحد یادگار امام خمینی (ره) شهرری، دانشگاه آزاد اسلامی، تهران، ایران.

تاریخ دریافت: ۱۴۰۴/۰۶/۲۵ تاریخ بازبینی: ۱۴۰۵/۰۲/۱۴ تاریخ پذیرش: ۱۴۰۵/۰۵/۰۶

نوع مقاله: پژوهشی

چکیده

با گسترش استفاده از دستگاه‌های اینترنت اشیا، حملات سایبری، به‌ویژه حمله منع سرویس توزیع‌شده، پیچیده‌تر و تشخیص آن‌ها به چالشی اساسی تبدیل شده است. تحقیقات نشان می‌دهد شبکه‌های عصبی عمیق به دلیل سازگاری با داده‌های حجیم، عملکرد مطلوبی دارند. در این پژوهش، عملکرد مدل‌های یادگیری عمیق در تشخیص حملات سایبری در شبکه‌های توزیع‌شده بررسی و مقایسه شده است. چهار مدل یادگیری عمیق شامل شبکه عصبی کانولوشنی، حافظه طولانی کوتاه، شبکه عصبی پیش‌خور و ترکیب آن‌ها (CNN-FFNN و-CNN LSTM)برای تحلیل داده‌های ترافیک شبکه ارزیابی شدند. مدل‌ها با دیتاست Bot-IoT آموزش دیدند و عملکردشان بر اساس معیار دقت سنجیده شد. نتایج نشان می‌دهد ترکیب شبکه عصبی کانولوشنی و حافظه طولانی کوتاه‌مدت با بهره‌گیری از ویژگی‌های مکانی و وابستگی‌های زمانی، بالاترین دقت را در تشخیص حملات پیچیده؛ مانند حملات منع سرویس توزیع‌شده دارد. این مدل می‌تواند ویژگی‌های پنهان را از داده‌های خام استخراج و روابط زمانی حملات را شبیه‌سازی کند که در محیط‌های اینترنت اشیا و محاسبات رایانش مه برای شناسایی تهدیدات تدریجی و پیچیده حائز اهمیت است. همچنین ترکیب شبکه عصبی کانولوشنی و شبکه عصبی پیش‌خور نیز در تشخیص تهدیدات سریع‌تر و پیچیدگی کمتر، عملکرد قابل‌توجهی داشته است. در نهایت این پژوهش بر اهمیت ترکیب مدل‌های یادگیری عمیق در بهبود دقت سیستم‌های تشخیص حملات سایبری تأکید کرده و راهکارهایی مبتنی بر معماری‌های توزیع‌شده برای امنیت شبکه‌های اینترنت اشیا و رایانش مه پیشنهاد می‌دهد.

کلیدواژگان: شبکه عصبی کانولوشن، شبکه عصبی پیش‌خور، حافظه طولانی کوتاه‌مدت، اینترنت اشیا، یادگیری عمیق.

* رایانامهٔ نویسنده مسؤول: mandana.rostami@iau.ac.ir

۱- مقدمه

گسترش روزافزون اینترنت اشیا[۱] و افزایش کاربرد آن در حوزه‌های متنوعی همچون صنایع، سامانه‌های پزشکی متصل[۲]، سلامت، خانه‌های هوشمند، حمل‌ونقل هوشمند مبتنی بر ارتباطات بی‌درنگ، شبکه‌های انرژی هوشمند و سیستم‌های مدیریت مصرف، زیرساخت‌های شبکه‌ای و زندگی روزمره، منجر به تولید حجم عظیمی از داده شده و درعین‌حال سطح تهدیدات و حملات امنیتی را به طور قابل‌توجهی افزایش داده است. در نتیجه، امنیت شبکه‌های اینترنت اشیا به یکی از مهم‌ترین چالش‌های حوزه امنیت سایبری تبدیل شده است و توجه بسیاری از پژوهشگران و متخصصان امنیت شبکه را به خود جلب کرده است [۱], [۲]. ویژگی‌های خاص شبکه‌های اینترنت اشیا از جمله ناهمگونی، توزیع‌شدگی و مقیاس‌پذیری بالا اگرچه فرصت‌های جدیدی برای ارائه خدمات هوشمند فراهم می‌کنند، اما در عین حال آن‌ها را در معرض طیف گسترده‌ای از تهدیدات امنیتی قرار می‌دهند. از جمله مهم‌ترین تهدیدات در این محیط می‌توان به حملات سایبری متعددی مانند حمله منع سرویس[۳] و حمله منع سرویس توزیع‌شده[۴] اشاره کرد. این حملات با ارسال حجم بالایی از ترافیک مخرب، منابع شبکه و سرویس‌ها را مختل کرده و می‌توانند باعث کاهش کیفیت خدمات، ایجاد اختلال در عملکرد سیستم‌ها و حتی از کار افتادن کامل آن‌ها شوند [۳], [۱۵]. با افزایش چشمگیر تعداد دستگاه‌های متصل به اینترنت اشیا، بستر مناسبی برای اجرای گسترده حملات منع سرویس توزیع‌شده فراهم شده است که می‌تواند علاوه بر ایجاد اختلال در عملکرد شبکه، خسارات اقتصادی قابل‌توجهی مانند از دست رفتن خدمات و مصرف غیرمجاز منابع شبکه به همراه داشته باشند.

استفاده از مدل پیشنهادی مبتنی بر CNN-LSTM با دقت بالای تشخیص می‌تواند از طریق شناسایی زودهنگام حملات و جلوگیری از گسترش آن‌ها، به کاهش زمان اختلال در سرویس‌ها[۵] و هزینه‌های عملیاتی ناشی از حملات کمک کرده و در نتیجه صرفه‌جویی اقتصادی در مدیریت امنیت شبکه‌های اینترنت اشیا ایجاد کند. حملات منع سرویس توزیع‌شده به عنوان یکی از مخرب‌ترین تهدیدات سایبری هستند، زیرا با هدایت حجم زیادی از ترافیک، منابع شبکه و سرویس‌ها را مختل می‌کنند. پیچیدگی الگوهای ترافیک اینترنت اشیا، تنوع پروتکل‌ها و محدودیت منابع باعث شده روش‌های سنتی تشخیص نفوذ کارایی لازم را نداشته باشند. به دلیل تنوع روش‌های اجرا این حملات می‌توانند به شکل‌های مختلف از جمله حملات حجم محور، حملات مبتنی بر پروتکل و حملات در سطح برنامه، پیچیدگی بالایی برای تشخیص و مقابله ایجاد کنندکه هرکدام شیوه خاصی برای از کار انداختن سیستم‌های هدف دارند [۲], [۳]. روش‌های سنتی مقابله با تهدیدات نظیر دیواره‌های آتش و سامانه‌های تشخیص نفوذ[۶] مبتنی بر قواعد، به دلیل ماهیت ایستا و وابستگی به قوانین از پیش تعریف‌شده در مواجهه با پیچیدگی و پویایی بالای ترافیک در شبکه‌های اینترنت اشیا کارایی محدودی در شناسایی حملات پیشرفته دارند به همین دلیل، ضرورت استفاده از رویکردهای هوشمند مبتنی بر یادگیری ماشین و یادگیری عمیق در شناسایی و مقابله با این دسته از حملات بیش از پیش احساس می‌شود [۴] تا [۶].

در سال‌های اخیر، یادگیری ماشین[۷] و به‌ویژه مدل‌های یادگیری عمیق[۸] به عنوان ابزارهایی توانمند برای تحلیل داده‌های حجیم و شناسایی الگوهای پیچیده، جایگاه ویژه‌ای در حوزه امنیت سایبری و تشخیص نفوذ پیدا کرده‌اند [۷], [۱۰]. در میان این مدل‌ها، شبکه‌های عصبی کانولوشنی[۹] به دلیل توانایی بالا در استخراج ویژگی‌های مکانی و شناسایی الگوهای پنهان داده‌ها کاربرد گسترده‌ای در تحلیل داده‌های شبکه پیدا کرده‌اند [۱۳], [۲۴]. همچنین، شبکه‌های حافظه طولانی کوتاه‌مدت[۱۰] به دلیل توانایی درک وابستگی‌های زمانی در داده‌های ترتیبی، کارایی بالایی در تحلیل ترافیک شبکه و شناسایی حملات منع سرویس توزیع‌شده نشان داده‌اند و استفاده از این شبکه‌ها می‌تواند دقت تشخیص حملات منع سرویس توزیع‌شده را به میزان قابل توجهی افزایش دهد [۱۹], [۲۱]. ترکیب این دو معماری می‌تواند با بهره‌گیری از مزایای مکمل هر یک، امکان استخراج همزمان ویژگی‌های مکانی و زمانی را فراهم کرده و شناسایی دقیق‌تر و سریع‌تر حملات منع سرویس توزیع‌شده را در محیط‌های پویا و مقیاس‌پذیر اینترنت اشیا فراهم می‌سازد [۱۱],[۱۲], [۲۲]. با گسترش شبکه‌های نسل

---

۱ Internet of Things
۲ Healthcare IoT
۳ Denial of Service (DoS)
۴ Distributed Denial of Service (DDoS)
۵ Downtime
۶ Intrusion Detection System (IDS)
۷ Machine learning (ML)
۸ Deep Learning (DL)
۹ Convolutional Neural Network (CNN)
۱۰ Long short-term memory (LSTM)

پنجم[۱] و معماری‌های مبتنی بر رایانش لبه و مه نیاز به راهکارهای امنیتی با زمان پاسخ سریع و کارایی بالا بیش از گذشته احساس می‌شود. در این معماری‌ها، بخشی از پردازش داده‌ها در لایه‌های نزدیک به منبع داده انجام می‌شود که می‌تواند زمان تشخیص حملات را کاهش دهد. بنابراین، طراحی مدل‌های یادگیری عمیق که قابلیت استقرار در معماری‌های توزیع‌شده مانند رایانش مه را داشته باشند، از اهمیت بالایی برخوردار است.

مدل پیشنهادی مبتنی بر CNN-LSTM، به دلیل پشتیبانی از پردازش توزیع‌شده، قابلیت استقرار در لایه‌های مختلف اکوسیستم نسل پنجم، لبه و ابر[۲] را دارد. این ویژگی امکان انجام استخراج ویژگی در لبه و تحلیل عمیق در هسته شبکه را فراهم کرده و با کاهش تأخیر تشخیص، برای محیط‌های پرسرعت و سرویس‌های حساس به تأخیر کاملاً سازگار است.

با وجود پیشرفت‌های قابل‌توجه در این حوزه، بسیاری از روش‌های موجود هنوز با محدودیت‌هایی مواجه هستند، برخی از مدل‌های مبتنی بر شبکه‌های عصبی کانولوشنی تنها بر استخراج ویژگی‌های فضایی تمرکز دارند و قادر به درک وابستگی‌های زمانی پیچیده نیستند. از سوی دیگر، مدل‌های مبتنی بر حافظه طولانی کوتاه منفرد به‌تنهایی در استخراج ویژگی‌های مکانی عملکرد مطلوبی ندارند. علاوه بر این، بسیاری از سامانه‌های موجود برای محیط‌های توزیع‌شده و مقیاس‌پذیر اینترنت اشیا بهینه‌سازی نشده‌اند و نمی‌توانند مدیریت کارآمد به‌روزرسانی مستمر مدل‌ها و اشتراک‌گذاری پارامترها در یک معماری توزیع‌شده را به شکل مؤثر انجام دهند.

این محدودیت‌ها نشان‌دهنده وجود یک شکاف پژوهشی آشکار در طراحی سامانه‌های تشخیص نفوذ کارآمد و مقیاس‌پذیر برای محیط‌های اینترنت اشیا و رایانش مه است.

در این راستا، پژوهش حاضر با هدف ارائه یک چارچوب هوشمند برای تشخیص حملات منع سرویس توزیع‌شده در شبکه‌های اینترنت اشیا انجام شده است. در این پژوهش یک مدل ترکیبی مبتنی بر شبکه‌های عصبی عمیق شامل شبکه عصبی کانولوشنی، شبکه حافظه طولانی کوتاه‌مدت و شبکه عصبی پیش‌خور[۳] پیشنهاد می‌شود. این چارچوب قادر است ویژگی‌های مکانی و وابستگی‌های زمانی ترافیک شبکه را به‌صورت هم‌زمان استخراج کرده و با بهره‌گیری از معماری توزیع‌شده مبتنی بر رایانش مه، فرایند تشخیص حملات را با تأخیر کمتر و دقت بالاتر انجام دهد.

برای ارزیابی عملکرد مدل پیشنهادی، چندین معماری مختلف شامل FFNN، LSTM، CNN-FFNN و CNN-LSTM طراحی و پیاده‌سازی شده و عملکرد آن‌ها با یکدیگر مقایسه شده است. آزمایش‌ها بر روی مجموعه‌داده‌های استاندارد اینترنت اشیا شامل CIC-IoT و Bot-IoT انجام شده‌اند. نتایج نشان می‌دهد که ترکیب ویژگی‌های مکانی و زمانی در مدل پیشنهادی موجب افزایش دقت تشخیص، کاهش نرخ خطا و بهبود عملکرد کلی سیستم در مقایسه با مدل‌های پایه و روش‌های پیشین شده است [۱۴]، [۲۵]، [۳۰].

نوآوری‌های این پژوهش عبارتند از:

- ارائه یک چارچوب ترکیبی مبتنی بر CNN–LSTM برای تشخیص حملات منع سرویس توزیع‌شده در محیط اینترنت اشیا.
- استفاده از معماری رایانش مه برای استقرار مدل به‌منظور کاهش تأخیر در تشخیص و افزایش مقیاس‌پذیری.
- ارزیابی جامع مدل پیشنهادی و مقایسه آن با چندین مدل پایه شامل شبکه‌های عصبی کانولوشنی، LSTM، شبکه عصبی پیش‌خور و مدل‌های ترکیبی.
- بررسی تأثیر معماری‌های مختلف شبکه‌های عصبی کانولوشنی بر عملکرد سیستم تشخیص نفوذ در محیط اینترنت اشیا.

انتظار می‌رود نتایج این پژوهش بتواند با افزایش دقت تشخیص، کاهش نرخ خطا و بهبود کارایی سامانه‌های تشخیص نفوذ، گامی مؤثر در ارتقای امنیت سامانه‌های مبتنی بر اینترنت اشیا بردارد.

این تحقیق یک چارچوب ترکیبی مبتنی بر CNN–LSTM–FFNN ارائه می‌دهد که هدف اصلی آن، ارائه و ارزیابی یک مدل ترکیبی مبتنی بر شبکه‌های عصبی عمیق CNN-LSTM به‌منظور استخراج هم‌زمان ویژگی‌های مکانی و زمانی از داده‌های ترافیک شبکه اینترنت اشیا و بهبود عملکرد تشخیص حملات منع سرویس توزیع‌شده است.

اهداف فرعی این تحقیق شامل موارد زیر است:

- طراحی و پیاده‌سازی معماری‌های مختلف شبکه عصبی پیش‌خور، حافظه طولانی کوتاه‌مدت، CNN-FFNN و CNN-LSTM و مقایسه عملکرد آن‌ها.
- ارزیابی تأثیر استخراج هم‌زمان ویژگی‌های مکانی و زمانی بر

[۱] 5G

[۲] 5G–Edge–Cloud

[۳] Feed Forward Neural Network

عملکرد تشخیص حملات با مقایسه مدل‌های مبتنی بر CNN، LSTM و مدل ترکیبی .CNN-LSTM

- طراحی و تحلیل سه معماری شبکه عصبی کانولوشنی با سطوح مختلف پیچیدگی؛ در زمینه تشخیص حملات اینترنت اشیا.
- بررسی مشکل بیش برازش در مدل‌های شبکه عصبی کانولوشنی و ارزیابی نقش استفاده از لایه‌های حافظه طولانی کوتاه‌مدت در بهبود تعمیم‌پذیری مدل برای تشخیص حملات.
- مقایسه عملکرد مدل پیشنهادی با روش‌های پیشین بر اساس معیارهای ارزیابی مانند دقت[۱]، صحت پیش‌بینی[۲] ، فراخوانی[۳] و امتیاز -F1 [۴] انجام می‌شود.

مسئله را می‌توان چنین بیان کرد: باتوجه به پیچیدگی روزافزون حمله منع سرویس توزیع‌شده و میزان داده عظیم تولیدشده توسط دستگاه‌های اینترنت اشیا، روش‌های مبتنی بر قوانین ثابت و امضا به‌شدت ناکارآمد شده‌اند. شبکه‌های اینترنت اشیا شامل دستگاه‌هایی باقدرت پردازشی محدود هستند که نمی‌توانند الگوریتم‌های سنگین پردازش مرکزی را تحمل کنند.

سؤالات تحقیق شامل موارد زیر است:

سؤال ۱: چگونه می‌توان یک روش هوشمند، دقیق، مقیاس‌پذیر و مناسب برای محیط‌های اینترنت اشیا و مه ارائه داد که قادر به تشخیص الگوهای پیچیده و چندبعدی حملات منع سرویس توزیع‌شده باشد؟

سؤال ۲: آیا استخراج هم‌زمان ویژگی‌های مکانی و زمانی از ترافیک شبکه می‌تواند توانایی مدل را در شناسایی الگوهای پیچیده و چندبعدی حملات منع سرویس توزیع‌شده بهبود بخشد؟

سؤال ۳: آیا استفاده از مدل یادگیری عمیق ترکیبی(CNN–LSTM–FFNN) نسبت به مدل‌های تک‌ساختی، عملکرد بهتری از نظر دقت، نرخ تشخیص و کاهش نرخ خطای مثبت کاذب ارائه می‌دهد؟

سؤال ۴: آیا پیاده‌سازی فرایند تشخیص در لایه مه می‌تواند تأخیر تشخیص[۵] را کاهش داده و امکان واکنش بلادرنگ در محیط‌های اینترنت اشیا را فراهم سازد؟

سؤال ۵: آیا روش پیشنهادی، پس از بهینه‌سازی مدل، قابلیت مقیاس‌پذیری و سازگاری با محدودیت منابع محاسباتی در محیط‌های اینترنت اشیا و مه را حفظ می‌کند؟

فرضیات تحقیق نیز در زیر فهرست شده‌اند:

فرضیه ۱: به‌کارگیری معماری سلسله‌مراتبی اینترنت اشیا – مه موجب افزایش معنادار دقت تشخیص حملات منع سرویس توزیع‌شده نسبت به معماری‌های متمرکز مبتنی بر ابر می‌شود.

فرضیه ۲: ترکیب ویژگی‌های مکانی و زمانی ترافیک شبکه، عملکرد مدل تشخیص حملات منع سرویس توزیع‌شده را از نظر معیارهای دقت[۶]، بازخوانی[۷] امتیاز - F1 و طور معناداری بهبود می‌دهد.

فرضیه ۳: مدل یادگیری عمیق ترکیبی CNN–LSTM در مقایسه با مدل‌های منفرد مانند CNN، LSTM و FFNN، توانایی بالاتری در تشخیص الگوهای پیچیده و تدریجی حملات منع سرویس توزیع‌شده دارد.

فرضیه ۴: انتقال فرایند استنتاج[۸] به لایه مه باعث کاهش تأخیر تشخیص و افزایش قابلیت تشخیص بلادرنگ حملات در شبکه‌های اینترنت اشیا می‌شود.

فرضیه ۵: روش پیشنهادی، پس از اعمال تکنیک‌های بهینه‌سازی مدل، بدون کاهش معنادار در دقت، قابلیت اجرا و مقیاس‌پذیری در محیط‌های دارای منابع محدود را خواهد داشت.

۲- پیشینه تحقیق

نتیجه مرور ادبیات نشان می‌دهد که امنیت در شبکه‌های اینترنت اشیا به دلیل ماهیت توزیع‌شده، منابع محدود دستگاه‌ها و حجم بالای داده‌های تولیدی، با چالش‌های متعددی روبه‌رو است. یکی از مهم‌ترین تهدیدات در این حوزه، حملات منع سرویس توزیع‌شده است که با استفاده از تعداد زیادی دستگاه آلوده به‌صورت هم‌زمان به یک هدف حمله کرده و منابع آن را اشباع می‌کند. در این نوع حملات، مهاجم ابتدا آسیب‌پذیری‌های موجود در دستگاه‌ها یا زیرساخت‌های شبکه را شناسایی کرده و سپس از آن‌ها برای ایجاد یک بات‌نت گسترده استفاده می‌کند. بات‌نت‌ها می‌توانند هزاران یا حتی میلیون‌ها دستگاه را در سراسر جهان درگیر کرده و به طور هماهنگ ترافیک مخرب را به سمت هدف ارسال کنند.

---

[۱] Accuracy
[۲] Precision
[۳] Recall
[۴] F1-score
[۵] Latency
[۶] Precision
[۷] Recall
[۸] Inference

در بسیاری از موارد، پروتکل‌هایی مانند سیستم نام دامنه[۱] به دلیل برخی ضعف‌های امنیتی به‌عنوان زیرساختی برای تقویت و گسترش این حملات مورد سوءاستفاده قرار می‌گیرند. در چنین حملاتی، مهاجم با ارسال درخواست‌های تقویتی حجم بسیار زیادی از ترافیک را به سمت قربانی هدایت می‌کند که می‌تواند موجب اختلال جدی در سرویس‌های اینترنتی شود. ازاین‌رو، شناخت دقیق ساختار و نحوه عملکرد حملات منع سرویس توزیع‌شده نقش مهمی در طراحی راهکارهای دفاعی مؤثر در شبکه‌های اینترنت اشیا دارد [۵].

با گسترش کاربرد اینترنت اشیا، مدل‌های سنتی امنیت سایبری دیگر پاسخگوی نیازهای این محیط پیچیده نیستند. در معماری‌های کلاسیک امنیت اطلاعات، اهداف اصلی شامل محرمانگی، یکپارچگی و دردسترس‌بودن[۲] داده‌ها است؛ بااین‌حال در محیط‌های اینترنت اشیا این اهداف به‌تنهایی کافی نیستند و الزامات دیگری نظیر پاسخگویی، قابلیت حسابرسی، حریم خصوصی و اعتمادپذیری نیز اهمیت پیدا می‌کنند [۶]. در بسیاری از سیستم‌های امنیتی سنتی، ابزارهایی مانند سیستم‌های تشخیص نفوذ احراز هویت کاربران، رمزنگاری داده‌ها، دیواره‌های آتش و نرم‌افزارهای ضدویروس برای محافظت از شبکه مورداستفاده قرار می‌گیرند. بااین‌وجود، همان‌طور که در پژوهش‌های پیشین نشان‌داده‌شده است، این روش‌ها در محیط‌های اینترنت اشیا که با داده‌های حجیم، پویا و ناهمگون مواجه هستند کارایی محدودی دارند [۷].

در سال‌های اخیر، استفاده از روش‌های یادگیری ماشین برای تحلیل ترافیک شبکه و تشخیص فعالیت‌های مخرب موردتوجه قرار گرفته است. الگوریتم‌های کلاسیک یادگیری ماشین مانند درخت تصمیم، ماشین بردار پشتیبان و جنگل تصادفی در برخی مطالعات برای تشخیص حملات سایبری مورداستفاده قرار گرفته‌اند؛ بااین‌حال این روش‌ها وابستگی زیادی به مهندسی دستی ویژگی‌ها دارند و در مواجهه با داده‌های پیچیده و حملات جدید عملکرد مطلوبی ارائه نمی‌دهند [۸] – [۱۰]. یکی از محدودیت‌های مهم این رویکردها، ناتوانی در استخراج خودکار ویژگی‌های مؤثر از داده‌های خام شبکه است که می‌تواند موجب کاهش دقت در تشخیص حملات پیچیده یا جهش‌یافته شود. به همین دلیل، پژوهشگران به سمت استفاده از تکنیک‌های یادگیری عمیق برای بهبود عملکرد سیستم‌های تشخیص نفوذ حرکت کرده‌اند [۱۱]. در همین راستا، در یک مطالعه مروری جامع به بررسی کاربرد روش‌های یادگیری عمیق در سیستم‌های تشخیص نفوذ برای اینترنت اشیا پرداختند و معماری‌های مختلفی از جمله شبکه عصبی کانولوشنی، شبکه عصبی پیش‌خور، شبکه حافظه طولانی کوتاه‌مدت، خودرمزگذارها و مدل‌های ترکیبی را مورد ارزیابی قرار گرفتند. نتایج این پژوهش نشان داد که مدل‌های یادگیری عمیق نسبت به روش‌های سنتی یادگیری ماشین توانایی بیشتری در استخراج خودکار ویژگی‌ها و شناسایی الگوهای پیچیده ترافیک شبکه دارند. بااین‌حال، چالش‌هایی مانند نیاز به منابع محاسباتی بالا، دشواری استقرار در دستگاه‌های محدود منابع اینترنت اشیا و ضعف در تشخیص حملات جدید همچنان مطرح است.

این مطالعه تأکید می‌کند که استفاده از معماری‌های ترکیبی که بتوانند هم‌زمان ویژگی‌های مکانی و زمانی ترافیک شبکه را تحلیل کنند، می‌تواند عملکرد سیستم‌های تشخیص نفوذ در محیط‌های اینترنت اشیا را به طور قابل‌توجهی بهبود دهد [۲۴]. ازسوی‌دیگر، شباهت قابل‌توجهی میان الگوهای حملات سایبری و مسئله تشخیص تصویر وجود دارد. بسیاری از حملات جدید در واقع نسخه‌های جهش‌یافته‌ای از حملات شناخته‌شده قبلی هستند و تنها تغییرات جزئی در الگوی ترافیک شبکه ایجاد می‌کنند. این ویژگی مشابه تغییرات جزئی در پیکسل‌های تصاویر است که می‌تواند توسط مدل‌های یادگیری عمیق شناسایی شود. در این زمینه، شبکه‌های عصبی کانولوشنی به دلیل توانایی بالا در استخراج الگوهای مکانی از داده‌ها، برای تحلیل ترافیک شبکه و شناسایی فعالیت‌های غیرعادی مورداستفاده قرار گرفته‌اند [۱۲]، [۱۳]. بااین‌حال، ماهیت توزیع‌شده شبکه‌های اینترنت اشیا و محدودیت منابع محاسباتی در دستگاه‌های لبه، طراحی سیستم‌های تشخیص نفوذ کارآمد را با چالش‌های جدیدی مواجه کرده است [۱۴].

در بسیاری از پژوهش‌های حوزه تشخیص نفوذ، استفاده از مجموعه‌داده‌های استاندارد برای آموزش و ارزیابی مدل‌ها اهمیت زیادی دارد. یکی از مجموعه‌داده‌های مهم در این حوزه، مجموعه‌داده Bot-IoT است که شامل بیش از ۷۳ میلیون رکورد از ترافیک شبکه در یک محیط اینترنت اشیا شبیه‌سازی‌شده است [۱۵]. این مجموعه‌داده شامل ترافیک عادی و چندین نوع حمله سایبری از جمله حمله منع سرویس توزیع‌شده، حمله منع سرویس، سرقت اطلاعات و ثبت کلید[۳] است. حملات منع سرویس توزیع‌شده و حملات منع سرویس به تلاش‌های مخرب برای ایجاد اختلال در عملکرد سرویس‌ها از طریق ارسال حجم بالایی از ترافیک اشاره دارند، درحالی‌که حملات ثبت کلید برای جمع‌آوری اطلاعات ورودی

[۱] Domain Name System (DNS)

[۲] Confidentiality, Integrity, Availability (CIA)

[۳] Keylogging

کاربران و حملات سرقت اطلاعات برای استخراج داده‌های حساس مورداستفاده قرار می‌گیرند. داده‌های این مجموعه بر اساس فعالیت شبکه‌ای ۶۲ میزبان در محدوده آدرس 192.168.100.0/26 تولید شده است. از آنجا که تمامی حملات موجود در این مجموعه‌داده مبتنی بر روش سیل ترافیک[۱] هستند، ویژگی‌های مرتبط با نرخ ارسال داده، تعداد بسته‌ها و نوع پروتکل‌ها نقش مهمی در تحلیل و تشخیص حملات ایفا می‌کنند.

علاوه بر Bot-IoT، مجموعه‌داده NSL-KDD نیز یکی از مجموعه داده‌های پرکاربرد در پژوهش‌های تشخیص نفوذ است که به‌عنوان نسخه بهبودیافته مجموعه‌داده KDDCUP'99 معرفی شده است [۱۶]. این مجموعه شامل بیش از یک میلیون رکورد داده‌ای است که هر رکورد از ۴۱ ویژگی مختلف تشکیل شده و برای تشخیص ناهنجاری در ترافیک شبکه مورداستفاده قرار می‌گیرد [۱۷].

در میان مدل‌های یادگیری عمیق، شبکه‌های عصبی پیش‌خور یکی از ساختارهای پایه در شبکه‌های عصبی مصنوعی محسوب می‌شوند که در آن اطلاعات از لایه ورودی به سمت لایه خروجی و از طریق لایه‌های پنهان به‌صورت یک‌طرفه جریان پیدا می‌کنند [۱۸]. در این مدل، تعداد نورون‌های لایه ورودی و خروجی بر اساس تعداد متغیرهای ورودی و خروجی تعیین می‌شود، درحالی‌که تعداد نورون‌های لایه‌های پنهان معمولاً از طریق روش‌های تجربی یا آزمون‌وخطا مشخص می‌گردد. اتصال کامل میان لایه‌ها موجب می‌شود هر نورون یک لایه به‌تمامی نورون‌های لایه بعدی متصل باشد. ازسوی‌دیگر، شبکه‌های حافظه طولانی کوتاه‌مدت به‌عنوان نوعی از شبکه‌های عصبی بازگشتی برای تحلیل داده‌های ترتیبی طراحی شده‌اند [۱۹] همچنین این مدل‌ها قادرند وابستگی‌های بلندمدت در داده‌ها را یاد بگیرند و به همین دلیل در تحلیل ترافیک شبکه و تشخیص حملات سایبری کاربرد گسترده‌ای دارند. در این زمینه، یک مدل تشخیص نفوذ مبتنی بر یادگیری عمیق برای شبکه‌های (SDN-IoT) [۲] ارائه کردند که بر پایه معماری حافظه طولانی کوتاه‌مدت دوسویه[۳] طراحی شده است. در این روش از قابلیت یادگیری وابستگی‌های زمانی در داده‌های ترافیک شبکه برای شناسایی الگوهای حملات استفاده می‌شود. نتایج نشان داد که این مدل نسبت به برخی روش‌های سنتی یادگیری ماشین عملکرد بهتری در تشخیص حملات دارد، بااین‌حال تمرکز اصلی آن بر تحلیل توالی‌های زمانی بوده و از سازوکارهای استخراج ویژگی مکانی مانند شبکه‌های عصبی کانولوشنی استفاده نشده است [۳۸]. در پژوهش دیگری با بررسی چندین مدل یادگیری عمیق برای تشخیص نفوذ در شبکه‌سازی مبتنی بر نرم‌افزار نشان دادند که استفاده از این مدل‌ها می‌تواند دقت شناسایی حملات را نسبت به روش‌های کلاسیک به طور قابل‌توجهی افزایش دهند. بااین‌وجود، نتایج این مطالعه نشان داد که بسیاری از این مدل‌ها از نظر پیچیدگی محاسباتی سنگین بوده و استقرار آن‌ها در محیط‌های محدود منابع مانند شبکه‌های اینترنت اشیا همچنان وجود دارد و استفاده از مدل‌های ترکیبی و سبک‌وزن می‌تواند راهکاری مناسب برای بهبود عملکرد سامانه‌های تشخیص نفوذ در چنین محیط‌هایی باشد [۳۹]. همچنین استفاده از مجموعه‌داده‌های به‌روز مانند CIC-IoT2023 در برخی مطالعات اخیر نشان داده است که به‌کارگیری داده‌های متنوع و واقعی می‌تواند پایداری و تعمیم‌پذیری مدل‌های تشخیص نفوذ را بهبود دهد [۳۷].

۲-۱- جمع‌بندی پیشینه و شکاف تحقیقات

بررسی مطالعات پیشین نشان می‌دهد که روش‌های یادگیری عمیق به‌ویژه معماری‌هایی نظیر شبکه‌های عصبی کانولوشنی، حافظه طولانی کوتاه‌مدت و مدل‌های ترکیبی CNN-LSTM نقش مهمی در بهبود عملکرد سیستم‌های تشخیص نفوذ در شبکه‌های اینترنت اشیا ایفا کرده‌اند. بااین‌حال، بخش قابل‌توجهی از پژوهش‌ها تنها بر یک نوع معماری متمرکز بوده‌اند و در نتیجه قادر به مدل‌سازی هم‌زمان الگوهای مکانی و وابستگی‌های زمانی موجود در ترافیک شبکه نیستند. ازسوی‌دیگر، برخی مدل‌های عمیق پیشنهادی با وجود دستیابی به‌دقت بالا، به دلیل پیچیدگی محاسباتی و نیاز به منابع پردازشی قابل‌توجه، برای استقرار در محیط‌های محدود منابع مانند اینترنت اشیا چندان مناسب نیستند. در نتیجه طراحی معماری‌های ترکیبی سبک‌وزن که بتوانند هم‌زمان الگوهای مکانی و زمانی را استخراج کرده و در بسترهای محاسباتی توزیع‌شده مانند رایانش مه اجرا شوند، همچنان یک چالش پژوهشی مهم محسوب می‌شود.

باتوجه‌به مقایسه ارائه‌شده در جدول ۱، مشخص می‌شود که هر یک از رویکردهای یادگیری عمیق مورد استفاده در سیستم‌های تشخیص نفوذ دارای نقاط قوت و در عین حال محدودیت‌هایی هستند. مدل‌های مبتنی بر شبکه عصبی کانولوشنی در استخراج ویژگی‌های مکانی از داده‌های ترافیک شبکه عملکرد مناسبی دارند، در حالی که مدل‌های مبتنی بر حافظه طولانی کوتاه مدت قادر به

[۱] Flooding

[۲] Software-Defined Networking – Internet of Things

[۳] Bi-LSTM

تحلیل وابستگی‌های زمانی در جریان‌های ترافیکی هستند. با این حال، استفاده مستقل از هر یک از این روش‌ها نمی‌تواند تمامی ابعاد پیچیده داده‌های شبکه در محیط‌های اینترنت اشیا را به طور کامل مدل‌سازی کند. از این رو، استفاده از یک معماری ترکیبی که بتواند به طور هم‌زمان ویژگی‌های مکانی و زمانی را استخراج کند، می‌تواند به بهبود دقت و کارایی سیستم‌های تشخیص نفوذ منجر شود.

جدول ۱. مقایسه پژوهش‌های مرتبط پیشین

روش پیشین	مزایا	محدودیت‌ها	ارتباط با این پژوهش
تنها CNN	استخراج مؤثر ویژگی‌های مکانی از ترافیک شبکه؛ توانایی تشخیص الگوهای پیچیده و ناهنجاری‌ها	ناتوانی در مدل‌سازی وابستگی‌های زمانی؛ کاهش دقت در تحلیل جریان‌های ترتیبی	استفاده به‌عنوان ماژول استخراج ویژگی مکانی در مدل پیشنهادی
تنها LSTM	مدل‌سازی وابستگی‌های زمانی بلندمدت؛ عملکرد مناسب در تحلیل داده‌های ترتیبی شبکه	ضعف در استخراج ویژگی‌های مکانی از داده‌های خام؛ وابستگی به کیفیت ویژگی‌های ورودی	به‌کارگیری برای تحلیل توالی زمانی ترافیک در معماری پیشنهادی
خودرمزگذار (Autoencoder)	کاهش ابعاد داده‌ها؛ یادگیری بدون ناظر و تشخیص ناهنجاری‌ها	حساسیت بالا به نویز؛ افت دقت در سناریوهای حملات پیچیده و چندمرحله‌ای	استفاده به‌عنوان روش مقایسه‌ای برای ارزیابی عملکرد مدل پیشنهادی
مدل‌های یادگیری عمیق مستقل (بر اساس مرور Ferrag et al., 2024)	دقت تشخیص بالا نسبت به روش‌های کلاسیک؛ استخراج خودکار ویژگی‌ها	پیچیدگی محاسباتی بالا؛ دشواری استقرار در محیط‌های محدود منابع IoT	انگیزه اصلی برای طراحی مدل ترکیبی کارآمد و قابل‌استقرار
Bi-LSTM (Alhussein et al., 2024)	تحلیل وابستگی‌های زمانی دوطرفه؛ بهبود دقت تشخیص در محیط SDN-IoT	عدم بهره‌گیری از استخراج ویژگی مکانی؛ تمرکز صرف بر بُعد زمانی	تکمیل محدودیت‌ها با افزودن لایه CNN در مدل پیشنهادی
مدل‌های DL در SDN (Alshammari et al., 2024)	افزایش دقت تشخیص حملات در شبکه‌های SDN؛ انعطاف‌پذیری بالا	سربار محاسباتی زیاد؛ چالش در پیاده‌سازی در IoT	استفاده از نتایج برای طراحی معماری سبک‌تر مبتنی بر Fog
مدل ترکیبی CNN–LSTM	مدل‌سازی هم‌زمان ویژگی‌های مکانی و زمانی؛ دقت تشخیص بالاتر	افزایش پیچیدگی محاسباتی در پیاده‌سازی مستقیم	توسعه‌یافته و بهینه‌سازی‌شده در چارچوب پیشنهادی مبتنی بر Fog

در سال‌های اخیر، معماری‌های ترکیبی یادگیری عمیق، به‌ویژه معماری‌های CNN–LSTM، به طور گسترده برای تشخیص نفوذ در شبکه‌های اینترنت اشیا مورداستفاده قرار گرفته‌اند. همان‌گونه که در جدول ۲ نشان داده شده است، در پژوهشی یک مدل CNN–LSTM برای تشخیص حملات در محیط‌های شبکه‌ای با دقت ۹۷٫۲٪ ارائه شده است؛ با این حال، این روش در یک معماری متمرکز مبتنی بر رایانش ابری پیاده‌سازی شده و قابلیت استقرار در محیط‌های مه و اینترنت اشیا را در نظر نمی‌گیرد [۲۹]. همچنین در پژوهش دیگری یک مدل RNN پیشرفته با دقت ۹۸٫۵٪ معرفی شده است که تمرکز اصلی آن بر کاهش زمان تشخیص حملات است، اما از ترکیب صریح ویژگی‌های مکانی و زمانی در یک معماری ترکیبی بهره نمی‌برد [۳۰].

در مقایسه با این مطالعات، پژوهش حاضر یک معماری ترکیبی CNN–LSTM مبتنی بر رایانش مه برای محیط‌های اینترنت اشیا ارائه می‌دهد که امکان تشخیص توزیع‌شده حملات را فراهم کرده و با ترکیب استخراج ویژگی‌های مکانی شبکه عصبی کانولوشنی و تحلیل وابستگی‌های زمانی حافظه طولانی کوتاه‌مدت عملکرد رقابتی و بهبود قابل‌توجهی در دقت تشخیص ارائه می‌دهد. نتایج آزمایش‌ها نشان می‌دهد که روش پیشنهادی با دستیابی به‌دقت ۹۹٫۹٪ عملکرد رقابتی و بهبود قابل‌توجهی در تشخیص حملات نسبت به روش‌های پیشین ارائه می‌دهد.

جدول ۲. مقایسه رویکردهای یادگیری عمیق و معماری‌های ترکیبی CNN–LSTM برای تشخیص نفوذ در محیط‌های اینترنت اشیا

مقاله	مدل یادگیری عمیق	محیط اجرا	دقت	نقاط قوت	محدودیت‌ها
2019 [29]	CNN-LSTM	متمرکز (Cloud)	97.2%	استفاده از مدل ترکیبی به‌عنوان baseline	عدم پشتیبانی از استقرار توزیع‌شده در Fog/IoT
2024 [30]	Advanced RNN	IoT	98.5%	بهینه‌سازی زمان تشخیص	تمرکز بر یک بعد مسئله، عدم ترکیب صریح ویژگی‌های مکانی–زمانی
این مقاله	CNN-LSTM	Fog Computing–based IoT	99.9%	تشخیص توزیع‌شده، بهره‌گیری دوبعدی از ویژگی‌ها (spatial-temporal)، انطباق با محدودیت منابع	پیچیدگی محاسباتی بالاتر نسبت به مدل‌های ساده‌تر

در مجموع، همان‌طور که جدول ۲ نشان می‌دهد، بسیاری از روش‌های موجود یا بر معماری‌های یادگیری عمیق منفرد تمرکز دارند یا در محیط‌های متمرکز پیاده‌سازی شده‌اند ولی این پژوهش با ارائه یک مدل ترکیبی CNN–LSTM مبتنی بر رایانش مه، تحلیل همزمان ویژگی‌های مکانی و زمانی در ترافیک شبکه و تشخیص توزیع‌شده حملات در محیط‌های اینترنت اشیا را فراهم می‌کند.

۳- روش پیشنهادی

در این بخش، معماری و الگوریتم پیشنهادی برای تشخیص بلادرنگ و فعال حملات سایبری در محیط‌های اینترنت اشیا و محاسبات مه به‌تفصیل تشریح شده است. رویکرد اصلی، استفاده از یک مدل ترکیبی شبکه عصبی کانولوشنی و حافظه طولانی کوتاه‌مدت است که در یک معماری یادگیری توزیع‌شده[۱] پیاده‌سازی می‌شود تا از مزایای پردازش محلی در رایانش مه و تجمیع دانش جهانی در رایانش ابری بهره ببرد.

۳-۱- جزئیات معماری مدل‌ها

در این تحقیق، مدل پایه و ترکیبی مورد ارزیابی قرار گرفتند. همچنین، جزئیات سه معماری مختلف شبکه عصبی کانولوشنی برای بررسی تأثیر پیچیدگی مدل ارائه شده است:

- مدل CNN1: یک شبکه عصبی کانولوشنی یک‌بعدی (CNN 1D)با ۱۰ لایه، شامل یک لایه کانولوشن، سه لایه Leaky_ReLU، یک لایه ماکس - پولینگ، یک لایه دراپ‌اوت[۲] (با نرخ ۲۰٪)، و دو لایه متراکم نهایی.
- مدل CNN2: یک ساختار ترتیبی با ۱۴ لایه و دو لایه کانولوشن، که پیچیدگی بیشتری نسبت به CNN1 دارد. نرخ دراپ‌اوت در این مدل 30% است.
- مدل CNN3: ساختار پیشرفته‌تر با ۱۸ لایه، شامل سه لایه کانولوشن و پنج لایه Leaky_ReLU با هدف استخراج ویژگی‌های پیچیده‌تر.
- مدل‌های ترکیبی(CNN-LSTM) : هر سه مدل CNN1، CNN2 و CNN3، قبل از لایه‌های خروجی نهایی، با یک لایه حافظه طولانی کوتاه‌مدت ادغام شدند. در این معماری، لایه شبکه عصبی کانولوشنی وظیفه استخراج ویژگی‌های مکانی را بر عهده دارد و خروجی آن به لایه حافظه طولانی کوتاه‌مدت داده می‌شود تا وابستگی‌های زمانی بین ویژگی‌های استخراج‌شده را مدل‌سازی کند.

CNN-FFNN مشابه معماری CNN-LSTM، اما لایه حافظه طولانی کوتاه‌مدت با یک لایه پیش‌خور کاملاً متصل[۳] جایگزین شده است.

۳-۲- معماری و فرایند مدل ترکیبی CNN - LSTM

معماری پیشنهادی شامل سه لایه اصلی است: لایهٔ لبه/اینترنت اشیا[۴]، لایه مه و لایه ابری.

در لایه لبه، دستگاه‌های اینترنت اشیا مانند سنسورها، دوربین‌ها، محرک‌ها، جریان پیوسته داده‌های خام شبکه، ترافیکی، یا محیطی را تولید می‌کنند، این داده‌ها به‌صورت محلی و سریع پیش‌پردازش اولیه می‌شوند. سپس به نزدیک‌ترین گره مه ارسال می‌شوند.

۳-۳- مراحل پیش‌پردازش داده‌ها

به‌منظور آماده‌سازی داده‌های خام تولیدشده توسط دستگاه‌های اینترنت اشیا برای استفاده در مدل‌های یادگیری عمیق، مجموعه‌ای از مراحل پیش‌پردازش بر روی داده‌ها اعمال شد. این مراحل با هدف کاهش نویز، یکنواخت‌سازی مقیاس ویژگی‌ها و بهبود عملکرد مدل انجام شدند و شامل موارد زیر هستند:

- نرمال‌سازی داده‌ها: ازآنجاکه ویژگی‌های عددی مجموعه‌داده‌ها دارای بازه‌های متفاوتی بودند، به‌منظور یکنواخت‌سازی مقیاس ویژگی‌ها، کاهش تأثیر تفاوت مقیاس میان آن‌ها و بهبود فرایند یادگیری مدل، تمامی ویژگی‌های عددی با استفاده از روش حداقل- حداکثر[۵] به بازه [0,1] نرمال‌سازی شدند.
- مدیریت داده‌های نامتعادل: در مجموعه‌داده‌های تشخیص نفوذ، معمولاً توزیع نمونه‌ها بین کلاس‌های عادی و انواع حملات نامتوازن است. این عدم توازن می‌تواند باعث سوگیری مدل به سمت کلاس اکثریت شود. به‌منظور کاهش این مشکل، از تکنیک‌های متوازن‌سازی داده‌ها استفاده شد تا تعداد نمونه‌های کلاس‌های مختلف متعادل‌تر گردد و مدل توانایی بهتری در شناسایی انواع حملات داشته باشد.
- برچسب‌گذاری متغیرهای دسته‌بندی: متغیرهای دسته‌بندی با استفاده از روش کدگذاری تک داغ[۶] به مقادیر عددی دودویی تبدیل شدند تا امکان استفاده از آن‌ها در مدل فراهم شود. این

---

۱ Distributed Learning
۲ Drop out
۳ FFNN (Dense)
۴ Edge/IoT
۵ Min–Max
۶ One-Hot Encoding

روش از ایجاد رابطه رتبه‌ای نادرست میان مقادیر کیفی جلوگیری کرده و نمایش مناسبی از ویژگی‌های غیرعددی ارائه می‌دهد.

- تقسیم‌بندی داده‌ها: پس از انجام مراحل پیش‌پردازش، مجموعه‌داده‌ها به دو بخش آموزش و آزمون تقسیم شدند؛ به‌طوری که ۸۰ درصد داده‌ها برای آموزش مدل و ۲۰ درصد برای ارزیابی عملکرد آن مورداستفاده قرار گرفتند، که در این مرحله آماده استفاده برای مدل یادگیری عمیق می‌شوند.

شبکه عصبی کانولوشنی در گره‌های مه برای استخراج ویژگی‌های پیچیده از داده‌های پیش‌پردازش شده استفاده می‌شود. این ویژگی‌ها می‌توانند شامل الگوهای غیرعادی یا مشکوک در داده‌های ترافیکی یا فعالیت‌های شبکه باشند. پس از استخراج ویژگی‌ها، داده‌ها به حافظه طولانی کوتاه‌مدت منتقل می‌شوند تا وابستگی‌های زمانی و متوالی حملات شبیه‌سازی شوند. حافظه طولانی کوتاه‌مدت قادر است تغییرات تدریجی و پیچیده در زمان را درک کند و در تشخیص حملات زمان‌بندی‌شده یا تدریجی کمک کند. گره‌های مه مدل‌های یادگیری عمیق خود را از لایه ابری دریافت می‌کنند که مدل جهانی[۱] در آن قرار دارد. این مدل جهانی شامل وزن‌های به‌روز شده است که از گره‌های مه به طور مداوم به‌روزرسانی می‌شود، گره اصلی[۲] در لایه ابری وظیفه مدیریت اعتبارسنجی، بهینه‌سازی، و تبادل پارامترهای مدل را انجام می‌دهد. پس از بهینه‌سازی وزن‌ها، پارامترهای به‌روز شده به گره‌های مه برای ادامه آموزش توزیع‌شده ارسال می‌شود. شبکه عصبی کانولوشنی در گره‌های مه به صورت محلی ویژگی‌ها را استخراج کرده و به مدل حافظه طولانی کوتاه‌مدت ارسال می‌کند. حافظه طولانی کوتاه‌مدت وابستگی‌های زمانی را شبیه‌سازی می‌کند و پس از هر به‌روزرسانی، وزن‌های مدل به سرور ابری مدل جهانی ارسال می‌شود، گره اصلی در لایه ابری مدل‌های به‌روز شده را اعتبارسنجی کرده و به‌روزرسانی‌ها را به گره‌های مه منتقل می‌کند. باتوجه‌به اشتراک‌گذاری وزن‌های به‌روزرسانی شده در سطح جهانی، مدل در لایه ابری به‌روزرسانی می‌شود و به گره‌های مه ارسال می‌شود، این فرایند به طور مداوم انجام می‌شود و باعث به‌روزرسانی مدل‌ها با داده‌ها و ویژگی‌های جدید از هر گره مه می‌شود.

۳-۴- الگوریتم تشخیص حمله توزیع‌شده مبتنی بر CNN و LSTM

این الگوریتم، که شبیه به یک فرایند یادگیری فدرال است، نحوه هماهنگی آموزش و به‌روزرسانی مدل را بین لایه‌های مه و ابری تعریف می‌کند.

ورودی‌های الگوریتم:

- RDx : داده‌های خام از دستگاه‌های IoT در لایه لبه.
- PDx : داده‌های پیش‌پردازش شده از دستگاه‌های اینترنت اشیا
- Mw : مدل جهانی در لایه ابری.
- ΔWx: وزن‌های شیب ارسال‌شده به سرور ابری از گره‌های مه

مراحل الگوریتم:

- **مرحله پیش‌پردازش داده‌ها:** داده‌های خام توسط دستگاه‌های اینترنت اشیا در لایه لبه پیش‌پردازش شده و به گره‌های مه ارسال می‌شوند.
- **دریافت مدل جهانی:** گره‌های مه آخرین‌مدل جهانی وزن‌های بهینه شده را از سرور ابری دریافت می‌کنند.
- **آموزش محلی**: آموزش با استفاده از داده‌های پیش‌پردازش شده محلی هر گره انجام می‌شود. مدل ترکیبی CNN-LSTM به‌صورت زیر عمل می‌کند:
- **استخراج ویژگی با CNN:** شبکه عصبی کانولوشنی به‌عنوان استخراج‌کننده ویژگی فضایی/محلی عمل می‌کند. شبکه عصبی کانولوشنی با اعمال فیلترها، الگوهای آماری و ارتباطات پنهان (مانند امضاهای بسته یا ناهنجاری‌های لحظه‌ای) را از داده‌های ورودی استخراج می‌کند.
- **مدل‌سازی وابستگی‌های زمانی با LSTM**: ویژگی‌های استخراج شده توسط شبکه عصبی کانولوشنی به شبکه حافظه طولانی کوتاه‌مدت ارسال می‌شوند. حافظه طولانی کوتاه‌مدت به‌عنوان مدل‌ساز وابستگی زمانی عمل کرده و قادر است تغییرات تدریجی، حملات مرحله‌ای، و ناهنجاری‌های طولانی‌مدت در توالی داده‌ها را تشخیص دهد.
- **به‌روزرسانی و ارسال وزن‌ها:** گره‌های مه، گرادیان‌های وزن‌های به‌روز شده یا خود وزن‌های به‌روز شده را به سرور ابری ارسال می‌کنند.
- **اعتبارسنجی و به‌روزرسانی مدل جهانی:** سرور وظیفه اعتبارسنجی، تجمیع پارامترها مانند الگوریتم میانگین‌گیری فدرال در یادگیری فدرال و بهینه‌سازی مدل جهانی را برعهده دارد و از طریق ماژول مرکزی اعتبارسنجی و به‌روزرسانی می‌کند، سپس پارامترهای به‌روزرسانی شده به گره‌های مه بازگردانده می‌شود تا چرخه آموزش توزیع‌شده ادامه یابد. این

[۱] Mw

[۲] Master

فرایند یادگیری مداوم و به‌اشتراک‌گذاری دانش جهانی را تضمین می‌کند.

- **آموزش و حفاظت مداوم:** فرایند آموزش به طور مداوم انجام می‌شود، به‌طوری که هر گره مه مدل‌های به‌روز شده خود را با داده‌های جدید آموزش می‌دهد و به سرور ابری ارسال می‌کند. هنگامی که دستگاه‌های جدید به شبکه متصل می‌شوند، می‌توانند با استفاده از مدل به‌روز شده در لایه ابری از حملات عمومی محافظت شوند.

این الگوریتم ترکیبی از شبکه عصبی کانولوشنی و حافظه طولانی کوتاه‌مدت در یک معماری توزیع‌شده مبتنی بر یادگیری عمیق برای تشخیص حملات در محیط‌های اینترنت اشیا و مه طراحی شده است. استفاده از شبکه عصبی کانولوشنی برای استخراج ویژگی‌ها و حافظه طولانی کوتاه‌مدت برای پردازش وابستگی‌های زمانی باعث می‌شود که این مدل قادر به شناسایی حملات پیچیده و تدریجی بادقت بالا باشد. سیستم به‌روزرسانی مداوم مدل در لایه ابری و به‌اشتراک‌گذاری وزن‌ها در گره‌های مه باعث می‌شود که امنیت و عملکرد کلی سیستم بهبود یابد و انعطاف‌پذیری در مقابل تهدیدات مختلف افزایش یابد.

شبکه‌های عصبی متمرکز CNN–FFNN و CNN–LSTM، برای شبیه‌سازی شبکه‌های عصبی متمرکز CNN–FFNN و CNN–LSTM، این مراحل رو طی می‌کنیم. برای ایجاد مدل‌ها، مدل CNN–FFNN از چندین لایه کانولوشنی و سپس لایه‌های تمام متصل استفاده می‌کنیم. در مدل CNN–LSTM، از ترکیب لایه‌های CNN و LSTM استفاده می‌کنیم و داده‌های شبیه‌سازی‌شده، دیتاست Bot-IoT را بارگذاری و پیش‌پردازش می‌کنیم. برای کامپایل و آموزش مدل‌ها، هر دو مدل با بهینه‌ساز اَدَم[1]، تابع زیان آنتروپی متقاطع دوتایی[2] و متریک دقت آموزش داده شده‌اند.

برای مقایسه عملکرد، علاوه بر رویکرد توزیع‌شده، باید مدل‌های متمرکز متداول را نیز با همان داده‌ها و معیارها شبیه‌سازی کرد.

آماده‌سازی مجموعه‌داده: دیتاست Bot-IoT یا هر مجموعه‌داده معتبر دیگر در حوزه حملات اینترنت اشیا شبکه بارگذاری، پاک‌سازی و پیش‌پردازش کامل می‌شود. این شامل انتخاب ویژگی‌های مرتبط، نرمال‌سازی مقیاس بزرگ، و تبدیل داده‌های توالی به فرمت‌های مناسب برای شبکه عصبی کانولوشنی (آرایه‌های چندبعدی) است.

مدل‌های متمرکز مقایسه‌ای:

- شبکه عصبی کانولوشن و شبکه عصبی پیش‌خور: این مدل از لایه‌های کانولوشنی برای استخراج ویژگی‌های فضایی و سپس از لایه‌های تمام متصل کاملاً متصل شبکه عصبی پیش‌خور برای طبقه‌بندی نهایی استفاده می‌کند. شبکه عصبی پیش‌خور توانایی مدل‌سازی وابستگی‌های زمانی را ندارد و به‌عنوان یک معیار پایه برای مقایسه عملکرد حافظه طولانی کوتاه‌مدت استفاده می‌شود.
- شبکه عصبی کانولوشنی و حافظه طولانی کوتاه‌مدت متمرکز: این مدل ساختار مشابهی با مدل پیشنهادی دارد؛ اما آموزش آن به‌صورت متمرکز بر روی کل داده‌ها انجام می‌شود نه به‌صورت توزیع‌شده بین مه و ابر.
- کامپایل و آموزش: هر دو مدل متمرکز و همچنین هر دور آموزش در گره‌های مه در مدل پیشنهادی، با تنظیمات یکسان کامپایل می‌شوند:
- بهینه‌ساز: بهینه‌ساز اَدَم با نرخ یادگیری مشخص.
- تابع هزینه: برای تشخیص دوتایی حمله عادی یا برای تشخیص چندکلاسی انواع حمله.
- سنجش ارزیابی: دقت فراخوانی برای ارزیابی عملکرد تشخیص حمله.

برای تضمین تکرارپذیری تحقیق، پارامترهای کلیدی آموزش مدل‌ها در جدول ۳ گزارش شده است.

جدول ۳. جزئیات پیاده‌سازی و پارامترهای آموزش

پارامتر	مقدار	توضیح
بهینه‌ساز (Optimizer)	Adam	برای محاسبه و به‌روزرسانی وزن‌ها
نرخ یادگیری (Learning Rate)	۰.۰۰۱	نرخ یادگیری بهینه برای بهینه‌ساز Adam.
تابع هزینه (Loss Function)	Binary Cross-Entropy	متناسب با مسئله طبقه‌بندی دوتایی (حمله/عادی)
اندازه دسته (Batch Size)	64	حجم داده پردازشی در هر گام آموزش
تعداد دوره‌های آموزش (Number of Epochs)	100	تعداد دوره‌های کامل آموزش بر روی دیتاست
تقسیم‌بندی مجموعه‌داده (Dataset Split)	۸۰٪ آموزش / ۲۰٪ آزمون	تست تقسیم‌بندی داده‌های Bot-IoT
پیاده‌سازی مدل (Implementation Environment)	Python 3.9, Keras/TensorFlow	کتابخانه‌های اصلی مورداستفاده
سخت‌افزار (Hardware)	NVIDIA GPU	برای تسریع آموزش مدل‌های عمیق

[1] Adam Optimizer

[2] Binary Cross-Entropy Loss

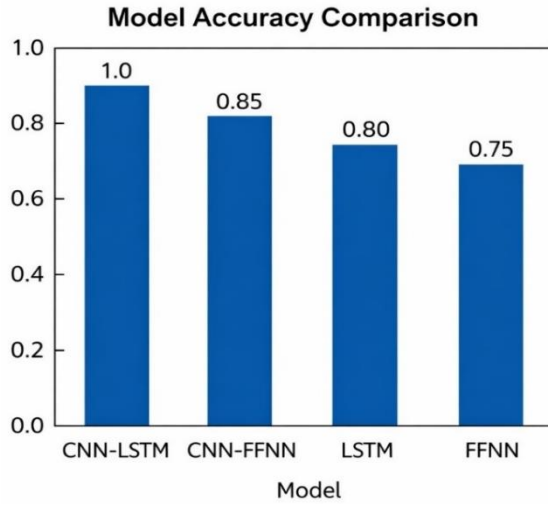
۴- نتایج و بحث

در این بخش، نتایج حاصل از ارزیابی مدل‌های پیشنهادی برای تشخیص حملات منع سرویس توزیع‌شده در شبکه‌های اینترنت اشیا ارائه و تحلیل می‌شوند. پژوهش حاضر به مقایسه عملکرد چهار مدل مختلف یادگیری عمیق شامل CNN-LSTM، CNN-FFNN، LSTM و FFNN بر روی دیتاست‌های Bot-IoT و CIC-IoT-Dataset2023 می‌پردازد. علاوه بر این، در این بخش، عملکرد مدل‌های پیشنهادی و مدل‌های پایه شامل CNN1، CNN2، CNN3 و نسخه‌های ترکیبی آن‌ها با LSTM مورد ارزیابی قرار گرفته است. هدف اصلی این تحلیل، بررسی تأثیر پیچیدگی معماری شبکه عصبی کانولوشنی و افزودن حافظه طولانی کوتاه‌مدت بر دقت و تعمیم‌پذیری مدل‌ها در تشخیص حملات در شبکه‌های اینترنت اشیا است.

ویژگی‌هایی که شبکه عصبی کانولوشنی استخراج می‌کند، به شبکه عصبی پیش‌خور داده می‌شود که یک شبکه عصبی پیش‌خور ساده است و مسئول طبقه‌بندی یا پیش‌بینی بر اساس آن ویژگی‌ها است. در دیتاست شبکه Bot-IoT، ویژگی‌های اساسی رفتار خاص بسته‌های شبکه و الگوهای ساده را شناسایی می‌کند. شبکه عصبی پیش‌خور معماری ساده‌تری نسبت به حافظه طولانی کوتاه‌مدت دارد و زمان محاسبات کمتری نیاز دارد. CNN–FFNN نمی‌تواند توالی‌های زمانی یا الگوهای دینامیکی در داده‌ها (مانند رفتار حملات شبکه در طول زمان) را مدل‌سازی کند. در روش ارائه شده با ترکیب دو روش CNN–FFNN و پیاده‌سازی آن با پایتون، در Bot-IoT که داده‌ها معمولاً حاوی توالی‌های زمانی و وابستگی‌های طولانی‌مدت هستند، عملکرد شبکه عصبی پیش‌خور محدود است و دقت کمتری (ACC = 83%) دارد.

CNN+LSTM در داده‌های Bot-IoT دقت 99.9% را نشان داده است، که نشان‌دهنده توانایی این معماری در شناسایی دقیق نفوذها است. این مدل پیچیدگی بیشتری نسبت به CNN–FFNN دارد و نیازمند زمان بیشتری برای آموزش است. جدول ۱ (بخش پیشینه تحقیق) نشان می‌دهد که روش‌های مختلف یادگیری عمیق با استفاده از مدل‌های مختلف و داده‌های مختلف برای تشخیص نفوذ در شبکه مورد استفاده قرار گرفته‌اند. با توجه به جدول، مدل‌هایی مانند خودرمزگذار واریاسیونی شرطی[۱] و خودرمزگذار پشته‌ای[۲] روی داده‌های NSL-KDD دقت بالاتری (تا 95%) دارند. حتی دقت مدل‌های شبکه عصبی کانولوشنی و خودرمزگذار حذف نویز[۳] روی داده‌های Bot-IoT بین 97% تا 83% است، ولی CNN+LSTM (Bot-IoT) عملکرد بسیار بهتری با دقت 99.9%، نسبت به مدل CNN–FFNN دارد و همچنین دقت آن از تمام مقادیر ذکر شده در جدول ۱ (بخش پیشینه تحقیق) بالاتر است. CNN+ LSTM همچنین بهتر از مدل‌های خودرمزگذار حذف نویز پشته‌ای[۴] و خودرمزگذار پشته‌ای است که روی داده‌های NSL-KDD استفاده شده‌اند.

در این قسمت، هدف مقایسه، دقت چهار مدل مختلف یادگیری عمیق برای تشخیص حمله عبارت‌اند از CNN-LSTM، CNN–FFNN، FFNN و LSTM. نتایج نهایی شبیه‌سازی به‌صورت نمودار نمایش داده شده و عملکرد هر مدل به تفصیل تحلیل شده است.



نمودار ۱. مقایسه دقت تشخیص حمله در اینترنت اشیا برای چهار مدل

مدلCNN-LSTM بالاترین دقت را در بین مدل‌های مقایسه شده به دست آورد. این برتری را می‌توان به ترکیب قابلیت استخراج ویژگی‌های محلی توسط CNN و مدل‌سازی روابط زمانی توسط LSTM نسبت داد که امکان یادگیری الگوهای پیچیده در داده‌های ترافیک اینترنت اشیا را فراهم می‌کند.

مدل CNN–FFNN به‌عنوان مدل دوم از نظر دقت عملکرد بسیار نزدیکی به CNN–LSTM داشت. این مدل از توانایی بالای شبکه عصبی کانولوشنی در استخراج ویژگی‌های مکانی بهره برده و با استفاده از شبکه عصبی پیش‌خور، این ویژگی‌ها را به طور موثر پردازش کرده است. هرچند دقت این مدل اندکی کمتر از CNN–LSTM است، اما به دلیل سادگی و سرعت بیشتر در پردازش،

[۱] Conditional Variational Autoencoder (CVAE)
[۲] Stacked AE (SAE)
[۳] Denoising Autoencoder (DAE)
[۴] Stacked NDAE

همچنان گزینه مناسبی برای بسیاری از کاربردها است.

مدل LSTM در رتبه سوم قرار گرفت. این مدل توانایی بالایی در شناسایی الگوهای ترتیبی دارد، اما عدم توانایی آن در استخراج مستقیم ویژگی‌های مکانی باعث کاهش دقت آن نسبت به CNN-LSTM وCNN–FFNN شده است. بااین‌حال، LSTM همچنان گزینه‌ای مناسب برای داده‌هایی است که عمدتاً الگوهای ترتیبی پیچیده دارند.

مدل FFNN پایین‌ترین دقت را در بین مدل‌های مورد بررسی داشت. این مدل به دلیل عدم توانایی در استخراج ویژگی‌های مکانی و ترتیبی پیچیده، تنها به وابستگی‌های سطحی میان داده‌ها متکی است؛ بنابراین، در داده‌هایی که نیازمند پردازش ویژگی‌های عمیق هستند، عملکرد ضعیف‌تری دارد.

افزودن LSTM دقت را ۱٫۵ تا ۲٪ افزایش داده است. اختلاف میان دقت آموزش و آزمایش کاهش‌یافته که نشانه کاهش بیش برازش[1] است. مدل CNN3+LSTM بهترین عملکرد را در میان مدل‌های آزمایش‌شده در دیتاست CIC-IoT دارد.

نتایج شبیه‌سازی‌های انجام‌شده در نمودار ۱ نشان می‌دهند که مدل‌های CNN–LSTM و CNN–FFNN به وضوح عملکرد بهتری نسبت به LSTM و FFNN دارند.

۴-۱- ارزیابی مدل‌های CNN1، CNN2 و CNN3

برای بررسی عمیق‌تر سه معماری مختلف CNN با تعداد لایه‌ها، فیلترها، ساختارها و پیچیدگی‌های متفاوت (CNN1, CNN2, CNN3) طراحی و پیاده‌سازی شدند تا تأثیر پیچیدگی معماری بر عملکرد مدل بررسی شود.

نتایج نشان می‌دهند که مدل‌های CNN1، CNN2 و CNN3، (نمودارهای ۲، ۳ و ۴) در داده‌های آموزشی دقت بسیار بالا دارند در بازه ۹۵-۱۰۰، اما دقت آن‌ها در داده‌های آزمایشی به شدت کاهش می‌یابد (در حدود ۷۵%) که این اختلاف قابل‌توجه بیانگر وقوع بیش‌برازش در مدل‌های CNN است که در آن مدل به جای یادگیری الگوهای عمومی، جزئیات داده‌های آموزشی را حفظ می‌کند و قادر به عملکرد مناسب روی داده جدید نیست. هرچند که افزایش پیچیدگی مدل بیشتر باشد، مانند CNN3، که تنها به بهبود بسیار جزئی (حدود 0.3%) در دقت آزمایش منجر شده است و همچنان بیش‌برازش مشهود است.

۴-۱- ارزیابی مدل‌های ترکیبی CNN+LSTM

همان‌طور که در نمودارها و جدول ۴ مشخص است، مدل‌های ترکیبیCNN+LSTM (نمودارهای ۵، ۶، و ۷) به ویژه در CNN2+LSTM و CNN3+LSTM دقت بسیار بهتری در داده‌های آزمایشی دارند و به دقت داده‌های آموزشی نزدیک‌تر است.

روش پیشنهادی در این مقاله با روش‌های بررسی شده در تحقیقات پیشین بررسی شده و نتایج آن در جدول ۵ ارائه شده است.

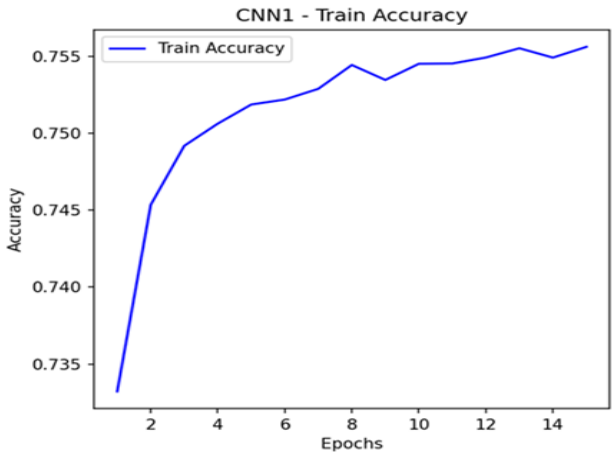
جدول ۴. نتیجه خروجی دقت مدل‌های CNN1، CNN2 ، CNN3 ، LSTM+CNN1 ، LSTM+CNN2 ،LSTM+CNN3

مدل	درصد آموزش	درصد آزمایش	دقت	توضیح
CNN1 [31-33]	**80%**	**20%**	**75,67%**	مدل پایه با ساختار ساده‌تر
CNN2 [31-33]	**80%**	**20%**	**75,81%**	مدل پایه با بهبود معماری کانولوشن
CNN3 [31-33]	**80%**	**20%**	**75,98%**	بهترین مدل پایه **CNN**
CNN1+LSTM*	**80%**	**20%**	**77,17%**	مدل ترکیبی با بهبود وابستگی‌های زمانی
CNN2+LSTM*	**80%**	**20%**	**77,51%**	مدل ترکیبی بهینه‌تر از**CNN2**
CNN3+LSTM*	**80%**	**20%**	**77,58%**	بهترین مدل کلی با بالاترین دقت

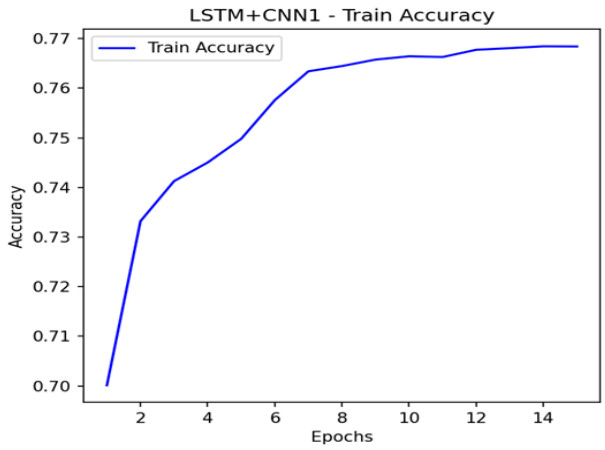
جدول ۵. روش‌های مختلف یادگیری عمیق با استفاده از مدل‌های مختلف و داده‌های مختلف برای تشخیص نفوذ در شبکه

Metrics	Datasets	DL models	Year	Ref.
ACC(% 97.5)	NSL-KDD	DBN	2015	[20]
ACC(% 98.8)	KDD Cup 99	LSTM to RNN	2016	[21]
ACC(% 98)	KDD Cup 99	Stacked NDAE	2018	[22]
	NSL-KDD	--	--	--
ACC(%90)	NSL-KDD	MLP	2019	[23]
ACC(% 98-97)	Bot-IoT	CNN, DAE	2020	[24]
	CSE-CIC-IDS2018	--	--	--
ACC(% 99.5)	Custom	SAE	2016	[25]
ACC(% 99)	NSL-KDD	CVAE	2017	[26]
TPR (> % 80) FPR (> %38)	CICIDS	AE	2018	[27]
ACC (%99-96)	NSL-KDD	Stacked AE	2018	[28]
ACC (%97.2)	CICIDS	CNN and LSTM	2019	[29]
ACC (%83)	Bot-IoT	CNN and FFNN	--	Our*
ACC(%99.9)	Bot-IoT	CNN and LSTM	--	Our*
ACC(%99.9)	Bot-IoT	CNN and LSTM	--	Our*

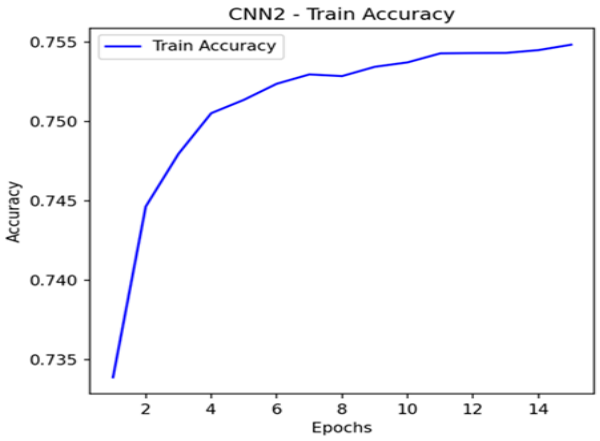
[1] Overfitting



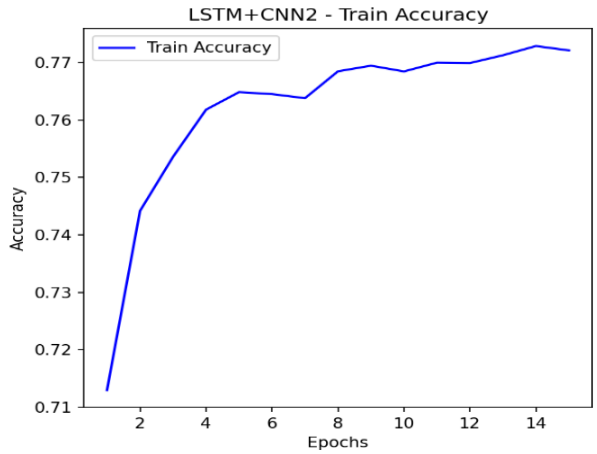
نمودار ۲. دقت مدل CNN1



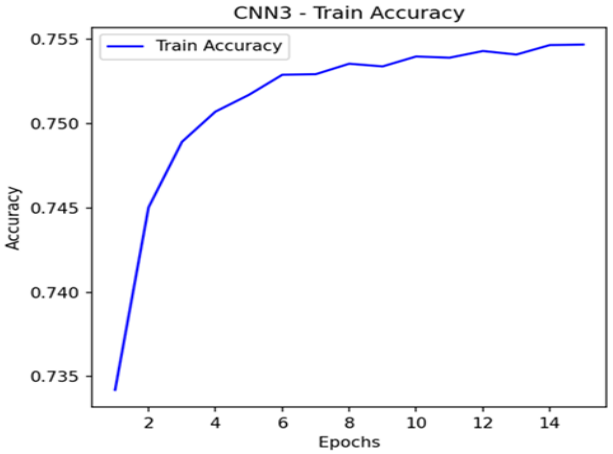
نمودار ۵. دقت مدل LSTM+ CNN1



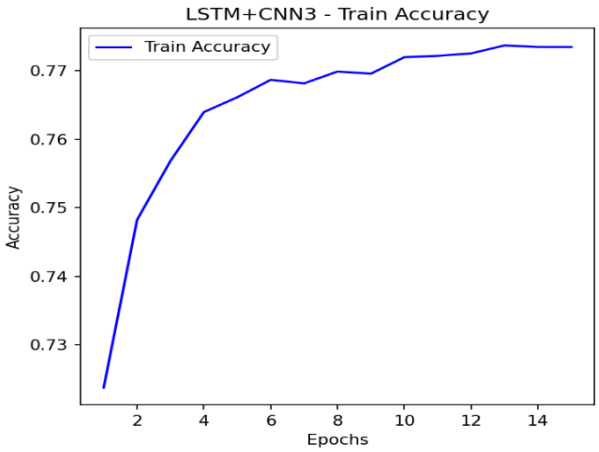
نمودار ۳. دقت مدل CNN2



نمودار ۶. دقت مدل LSTM+ CNN2



نمودار۴. دقت مدل CNN3



نمودار ۷. دقت مدل LSTM+CNN3

درحالی‌که مدل‌های قبلی روی دیتاست‌های مختلف (مانند NSL-KDD و CICIDS) نتایج قابل‌قبولی داشته‌اند، رویکرد پیشنهادی ما (CNN-LSTM) بر روی دیتاست Bot-IoT به‌دقت ۹۹,۹٪ دست یافته است. که این دقت در مقایسه با سایر روش‌های گزارش شده روی Bot-IoT (مانند شبکه عصبی کانولوشنی و خودرمزگذار حذف نویز با ۹۷ تا ۹۸ درصد و حتی برخی از بهترین نتایج روی سایر دیتاست‌ها (با در نظر گرفتن تفاوت در ماهیت دیتاست‌ها) چشمگیر است.

جدول ۵ نشان می‌دهد که روش‌های مختلف یادگیری عمیق با استفاده از مدل‌های مختلف و داده‌های مختلف برای تشخیص نفوذ در شبکه مورد استفاده قرار گرفته‌اند. با توجه به جدول، مدل‌های پیشرفته مانند خودرمزگذار وارياسیونی شرطی و خودرمزگذار پشته‌ای روی داده‌های NSL-KDD دقت بالاتری (99.5%) دارند. حتی دقت مدل‌های شبکه عصبی کانولوشنی و خودرمزگذار حذف نویز روی داده‌های Bot-IoT بین 97 تا 98 درصد است. اما مدل پیشنهادی این پژوهش (CNN-LSTM) روی دیتاست Bot-IoT عملکرد بسیار بهتری با دقت 99.9%، نسبت به مدل CNN-FFNN دارد و همچنین دقت آن از تمام مقادیر ذکر شده در جدول ۵ بالاتر است.

CNN-LSTM همچنین بهتر از مدل‌های خودرمزگذار حذف‌نویز پشته‌ای و خودرمزگذار حذف نویز است که روی داده‌های NSL-KDD استفاده شده اند. این نتایج نشان‌دهنده عملکرد بسیار مؤثر مدل در تشخیص حملات منع سرویس توزیع‌شده در محیط اینترنت اشیا است. این دقت بالای CNN-LSTM ، برتری مدل پیشنهادی این تحقیق را نسبت به نتایج گزارش شده در پژوهش‌های پیشین تأیید می‌کند. برای ارزیابی دقیق‌تر عملکرد مدل پیشنهادی، از ماتریس درهم‌ریختگی[1] استفاده شد. این ماتریس امکان بررسی جزئی‌تر نتایج طبقه‌بندی و تحلیل میزان پیش‌بینی صحیح و خطاهای مدل را فراهم می‌کند. ماتریس درهم‌ریختگی مدل CNN-LSTM بر اساس نتایج به‌دست‌آمده از مجموعه آزمون محاسبه شده است. مجموعه آزمون شامل ۹۰۰ نمونه از داده‌های ترافیک شبکه اینترنت اشیا بوده که از این میان ۴۳۰ نمونه مربوط به ترافیک عادی و ۴۷۰ نمونه مربوط به حملات است. نتایج ماتریس درهم‌ریختگی برای مدل CNN-LSTM در جدول ۶ ارائه شده است.

همان‌طور که در جدول ۶ مشاهده می‌شود، مدل توانسته است ۴۳۰ نمونه عادی و ۴۶۹ نمونه حمله را به درستی طبقه‌بندی کند، در حالی که تنها یک نمونه از حملات به اشتباه به عنوان ترافیک عادی شناسایی شده است. همچنین هیچ نمونه عادی به اشتباه به عنوان حمله پیش‌بینی نشده است که نشان‌دهنده نرخ بسیار پایین خطای مثبت کاذب است. این نتایج نشان می‌دهد که مدل پیشنهادی توانایی بالایی در تفکیک ترافیک عادی از ترافیک مخرب دارد. تعداد بسیار کم خطاها نیز بیانگر قدرت تفکیک بالا و پایداری مناسب مدل CNN-LSTMدر مسئله تشخیص نفوذ است.

نتایج در جدول ۷ نشان می‌دهد که مدل CNN-LSTM به‌طور معناداری از مدل‌های پایه بهتر عمل کرده است. این بهبود ناشی از توانایی مدل در استخراج همزمان الگوهای مکانی و وابستگی‌های زمانی ترافیک شبکه است. همچنین، افزایش فراخوانی بیانگر کاهش قابل توجه نرخ خطای منفی کاذب است که در کاربردهای امنیتی اهمیت حیاتی دارد[38-34].

جدول ۶. ماتریس درهم‌ریختگی مدل CNN-LSTM برای تشخیص حملات در شبکه‌های IoT

Predicted Attack	Predicted Normal	Actual Class
False Positive (FP) = 0	True Negative (TN) = 430	Normal
True Positive (TP) = 469	False Negative (FN) = 1	Attack

جدول ۷. مقایسه عملکرد مدل‌های پیشنهادی

مدل	دقت (%)	صحت (%)	فراخوانی (%)	امتیاز – F1 (%)
FFNN	83.0	80.1	78.3	79.2
LSTM	92.0	90.4	88.1	89.2
CNN-FFNN	97.0	96.2	95.0	95.5
CNN-LSTM	99.9	99.2	99.5	99.3

۵- نتیجه‌گیری و تحقیقات آتی

در این پژوهش، یک مدل هیبریدی تشخیص نفوذ مبتنی بر ترکیب شبکه عصبی کانولوشنی و شبکه حافظه طولانی کوتاه‌مدت برای شناسایی حملات منع سرویس توزیع‌شده در محیط‌های اینترنت اشیا و رایانش مه ارائه شد. مدل پیشنهادی روی دو مجموعه‌داده معتبر ترافیک شبکه ارزیابی گردید و عملکرد آن از نظر معیارهای دقت، صحت، فراخوانی و امتیاز-F1 با مدل‌های رایج موجود مقایسه شد. نتایج آزمایش‌ها نشان داد که مدل ترکیبی CNN–LSTM توزیع‌شده قادر است ویژگی‌های مکانی و زمانی ترافیک شبکه را به طور هم‌زمان استخراج کرده و عملکرد سیستم تشخیص نفوذ را در

[1] Confusion Matrix

مقایسه با مدل‌های منفرد بهبود دهد.

با توجه به رشد و پیچیدگی حملات سایبری در شبکه‌های اینترنت اشیا، روش‌های نوین تشخیص نفوذ مبتنی بر یادگیری عمیق، به‌ویژه مدل‌های شبکه عصبی کانولوشنی و حافظه طولانی کوتاه‌مدت، نقش مهمی در بهبود امنیت این شبکه‌ها ایفا می‌کنند. در این پژوهش، با استفاده از ترکیب شبکه عصبی کانولوشنی و حافظه طولانی کوتاه‌مدت برای تشخیص حملات توزیع‌شده در شبکه‌های اینترنت اشیا و محاسبات مه نشان داده شد که این مدل قادر به شناسایی حملات پیچیده و زمان‌بندی‌شده بادقت بالا است. نتایج حاکی از آن است که معماری ترکیبی شبکه عصبی کانولوشنی، حافظه طولانی کوتاه‌مدت و شبکه عصبی پیش‌خور برای تشخیص حملات منع سرویس توزیع‌شده در شبکه‌های اینترنت اشیا ارائه شده و عملکرد قابل‌توجهی در شناسایی الگوهای پیچیده ترافیک شبکه دارد.

نتایج تجربی روی دو مجموعه‌داده معتبر نشان داد که مدل‌های شبکه عصبی کانولوشنی منفرد علی‌رغم دقت بالا در مرحله آموزش، دچار بیش‌برازش شده و در داده‌های آزمون عملکرد محدودی دارند. در مقابل، ترکیب شبکه عصبی کانولوشنی با حافظه طولانی کوتاه‌مدت موجب افزایش تعمیم‌پذیری مدل و بهبود دقت آزمون تا حدود 2% شد. مدل پیشنهادی در مجموعه‌داده Bot-IoT به دقت 99.9% دست یافت که عملکرد برتری نسبت به تمامی روش‌های پیشین گزارش‌شده نشان می‌دهد. این نتایج نشان می‌دهد که ادغام ویژگی‌های مکانی–زمانی در سیستم‌های تشخیص نفوذ اینترنت اشیا ضروری بوده و می‌تواند عملکرد آن‌ها را به‌طور قابل‌توجهی ارتقا دهد.

در مقایسه با روش‌های سنتی مانند شبکه عصبی کانولوشنی و شبکه عصبی پیش‌خور، مدل پیشنهادی عملکرد به‌مراتب بهتری در شبیه‌سازی حملات و شناسایی الگوهای وابسته به زمان دارد. ازآنجاکه داده‌های ترافیک شبکه معمولاً دارای وابستگی‌های زمانی هستند، مدل حافظه طولانی کوتاه‌مدت قادر است این وابستگی‌ها را به طور مؤثر پردازش کرده و دقت شناسایی حملات را افزایش دهد. علاوه بر این، استفاده از الگوریتم‌های یادگیری عمیق در محیط‌های توزیع‌شده مانند محاسبات مه امکان به‌روزرسانی مستمر مدل‌ها و به‌اشتراک‌گذاری وزن‌ها میان‌گره‌های مه را فراهم کرده و امنیت شبکه‌ها را در برابر تهدیدات مختلف تقویت می‌کند.

پژوهش حاضر علاوه بر ارزیابی مدل‌ها، یک چارچوب توزیع‌شده برای تشخیص حملات در محیط‌های اینترنت اشیا و محاسبات مه ارائه می‌دهد. در این معماری، از شبکه عصبی کانولوشنی در گره‌های مه برای استخراج ویژگی‌های محلی و از حافظه طولانی کوتاه‌مدت برای تحلیل وابستگی‌های زمانی استفاده می‌شود. این رویکرد به مدل‌ها اجازه می‌دهد تا به‌صورت محلی در گره‌های مه آموزش ببینند و وزن‌های بهینه‌شده به‌صورت مداوم به یک سرور مرکزی در لایه ابری منتقل و به اشتراک گذاشته شوند. این فرایند یادگیری مداوم و توزیع‌شده، امنیت سیستم را در برابر تهدیدات جدید افزایش داده و امکان سازگاری مدل با داده‌های در حال تغییر را فراهم می‌کند.

باوجود نتایج امیدوارکننده، پیچیدگی محاسباتی مدل یکی از محدودیت‌های اصلی آن محسوب می‌شود. بااین‌حال، ترکیب حافظه طولانی کوتاه‌مدت با شبکه عصبی کانولوشنی باعث بهبود دقت اعتبارسنجی، کاهش بیش برازش و استخراج مؤثر ویژگی‌های فضایی و زمانی از داده‌های پیچیده ترافیک شبکه می‌شود. این مدل‌ها به طور مؤثری ویژگی‌های فضایی و زمانی را استخراج کرده و برای داده‌هایی که پیچیدگی بیشتری دارند مناسب‌تر هستند.

۵-۱- نوآوری‌های این پژوهش به صورت خلاصه

- ارائه یک معماری هیبریدی تشخیص نفوذ مبتنی بر ترکیب شبکه عصبی کانولوشنی و شبکه حافظه طولانی کوتاه‌مدت به‌صورت توزیع‌شده در لایه مه برای شناسایی حملات منع سرویس توزیع‌شده در شبکه‌های اینترنت اشیا.
- نشان‌دادن این‌که استفاده از مدل‌های منفرد مانند شبکه عصبی کانولوشنی یا حافظه طولانی کوتاه‌مدت در مقایسه با معماری هیبریدی پیشنهادی دچار بیش‌برازش شده و تعمیم‌پذیری پایین‌تری در داده‌های آزمون دارند.
- دستیابی به بهبود قابل‌توجه در عملکرد تشخیص نفوذ، به‌طوری که مدل پیشنهادی بر روی مجموعه‌داده Bot-IoT به‌دقت ۹۹,۹٪ و بهبود حدود۲% در دقت آزمون نسبت به روش‌های پیشین دست یافته است.
- نشان‌دادن اهمیت ادغام هم‌زمان ویژگی‌های مکانی و زمانی ترافیک شبکه در طراحی سیستم‌های تشخیص نفوذ برای محیط‌های اینترنت اشیا و رایانش مه.
- ارائه شواهد تجربی از برتری مدل ترکیبی CNN–LSTM در مقایسه با مدل‌های پایه مانند FFNN ، LSTM و CNN–FFNN بر روی مجموعه‌داده معتبر Bot-IoT .
- ارائه یک چارچوب تشخیص حمله توزیع‌شده مبتنی بر CNN–LSTM که امکان استقرار در معماری مه/ ابر و به‌روزرسانی مداوم مدل برای مقابله با تهدیدات جدید را فراهم می‌سازد.

۵-۲- پیشنهاد برای تحقیقات آتی

باتوجه‌به نتایج موفقیت‌آمیز حاصل از این تحقیق، می‌توان جهت بهبود و گسترش روش‌های ارائه‌شده و بررسی دقت و کارایی مدل‌های یادگیری عمیق در شناسایی حملات و تحلیل داده‌های پیچیده، مسیرهای زیر را در تحقیقات آینده دنبال کرد:

- **ارتقا معماری‌های هیبریدی**: توسعه و ارزیابی معماری‌های هیبریدی پیشرفته‌تر، نظیر ترکیب CNN–LSTM با مکانیزم‌های توجه[۱] و شبکه‌های گراف عصبی کانولوشنی، به‌منظور بهبود دقت تشخیص و کاهش نرخ مثبت‌های کاذب در سناریوهای واقعی حملات منع سرویس توزیع‌شده در اینترنت اشیا.
- **بررسی مقاومت مدل**: تحلیل مقاومت مدل‌های پیشنهادی در برابر حملات تهاجمی[۲] و توسعه تکنیک‌های دفاعی مناسب برای افزایش قابلیت اعتمادپذیری در محیط‌های خصمانه واقعی.
- **استفاده از داده‌های چندوجهی و بزرگ‌تر**: بررسی کارایی مدل‌های هیبریدی CNN–LSTM بر روی مجموعه‌داده‌های چندوجهی (مانند ترکیب ترافیک شبکه، لاگ‌های سیستمی و داده‌های حسگرها) برای ارتقای توانایی سیستم در تشخیص حملات پیچیده و چندمرحله‌ای در محیط‌های اینترنت اشیا.
- **بهینه‌سازی برای منابع محدود**: توسعه نسخه‌های بهینه‌سازی شده از مدل CNN-LSTM با پیچیدگی محاسباتی کمتر برای استقرار مستقیم بر روی دستگاه‌های رایانش لبه/ اینترنت اشیا با منابع بسیار محدود.

مراجع

[1] Alieyan, K., Kadhum, M. M., Anbar, M., Rehman, S. U., & Alajmi, N. K. (2016). An overview of DDoS attacks based on DNS. In Proceedings of the International Conference on Information and Communication Technology Convergence (ICTC) (pp. 276–280). IEEE. https://doi.org/10.1109/ICTC.2016.7763313

[2] Tyagi, H., & Kumar, R. (2021). Attack and anomaly detection in IoT networks using supervised machine learning approaches. Revue d'Intelligence Artificielle, 35(1), 11–21.

[3] Li, J., Xue, Z., Li, C., & Liu, M. (2021). RTED-SD: A real-time edge detection scheme for Sybil DDoS on the Internet of Vehicles. IEEE Access, 9, 11296–11305.

[4] Gupta, R. K., Mishra, A., & Gupta, B. (2021). Enhanced identity-based encryption for secure key generation in large-scale cloud computing. *IEEE Access, 9*, 165259–165272. https://doi.org/10.1109/ACCESS.2021.3138503

[5] Inuwa, M. M., & Das, R. (2024). A comparative analysis of various machine learning methods for anomaly detection in cyber attacks on IoT networks. Internet of Things, 26, 101162. https://doi.org/10.1016/j.iot.2023.101162

[6] Cherdantseva, Y., & Hilton, J. (2013). A reference model of information assurance security. In Proceedings of the International Conference on Availability, Reliability and Security (ARES) (pp. 546–555). IEEE. https://doi.org/10.1109/ARES.2013.72

[7] Kwon, D., Kim, H., Kim, J., Suh, S., Kim, I., & Kim, J. (2019). A survey of deep learning-based network anomaly detection. *Cluster Computing, 22*(5), 949–961.

[8] Anderson, J., Carbonell, J., Mitchell, T., Michalski, R., Amarel, S., Tecuci, T., & Kodratoff, Y. (1983). *Machine learning: An artificial intelligence approach.* Morgan Kaufmann.

[9] Kilincer, I., Ertam, F., & Sengur, A. (2021). Machine learning methods for cyber security intrusion detection: Datasets and comparative study. *Computer Networks, 188*, 107840.

[10] Fadlullah, Z. M., Tang, F., Mao, B., Kato, N., Akashi, O., Inoue, T., & Mizutani, K. (2017). State-of-the-art deep learning: Evolving machine intelligence toward tomorrow's intelligent network traffic control systems. *IEEE Communications Surveys & Tutorials, 19*(4), 2432–2455.

[11] Tsimenidis, S., Lagkas, T., & Rantos, K. (2022). Deep learning in IoT intrusion detection. Journal of Network and Systems Management, 30(3), 58. https://doi.org/10.1007/s10922-022-09666-x

[12] Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. Future Generation Computer Systems, 82, 761–768. https://doi.org/10.1016/j.future.2017.10.045

[13] Roopak, M., Tian, G. Y., & Chambers, J. (2019). Deep learning models for cyber security in IoT networks. In Proceedings of the IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 452–457). IEEE. https://doi.org/10.1109/CCWC.2019.8666590

[14] Shalaka, M., Pawar, P. M., & Muthalagu, R. (2023). Efficient intelligent intrusion detection system for heterogeneous Internet of Things (HetIoT). Journal of Network and Systems Management, 31(4), 87. https://doi.org/10.1007/s10922-023-09748-7

[15] Mahjabin, T., Xiao, Y., Sun, G., & Jiang, W. (2017). A survey of distributed denial-of-service attack, prevention, and mitigation techniques. International Journal of Distributed Sensor Networks, 13(12), 1–20.

[16] University of California, Irvine. (1999). *KDD Cup 1999 data* [Data set]. UCI Machine Learning Repository. https://archive.ics.uci.edu/ml/datasets/kdd+cup+1999+data

[17] Canadian Institute for Cybersecurity. (n.d.). *NSL-KDD dataset* [Data set]. University of New Brunswick. https://www.unb.ca/cic/datasets/nsl.html

[18] Ramchoun, H., Idrissi, M. J., Ghanou, Y., & Ettaouil, M. (2016). Multilayer perceptron: Architecture optimization and training. *International Journal of Interactive Multimedia and Artificial Intelligence, 4*(1), 26–30.

[19] Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. Neural Computation, 9(8), 1735–1780. https://doi.org/10.1162/neco.1997.9.8.1735

[20] Alom, M. Z., Bontupalli, V., & Taha, T. M. (2015). Intrusion detection using deep belief networks. In Proceedings of the IEEE National Aerospace and Electronics Conference (NAECON) (pp. 339–344). IEEE. https://doi.org/10.1109/NAECON.2015.7443094

[21] Kim, J., Kim, J., Thi Thu, H. L., & Kim, H. (2016). Long short-term memory recurrent neural network classifier for intrusion detection. In Proceedings of the International

[۱] Attention Mechanisms

[۲] Adversarial Attacks

[30] Abbas, S., Alsubai, S., Ojo, S., Sampedro, G. A., Almadhor, A., Al Hejaili, A., & Bouazzi, I. (2024). An efficient deep recurrent neural network for detection of cyberattacks in realistic IoT environment. *The Journal of Supercomputing*, *80*(10), 13557–13575.

[31] Patel, D., Pillai, S., & Kumar, V. (2023). *Deep reinforcement learning based anomaly detection for securing IoT edge networks*. Neural Computing and Applications, 35(23), 17159–17175. https://doi.org/10.1007/s00521-023-08672-x

[32] Rajabzadeh,M., Derakhshan-Barjoei,P. (2022). An Efficient Proxy-Based Message Authentication Framework in Vehicular Ad-hoc Networks. *Journal of Communication Engineering*, *11*(1), 111-136. doi: 10.22070/jce.2024.18230.1255

[33] Rajabzadeh Asaar, M., Derakhshan Barjoei, P. (2023). A New Protocol for Lightweight Anonymous Authentication with Leading Security in Wireless Sensor Networks Based on IoT. Intelligent Multimedia Processing and Communication Systems (IMPCS), vol. 4, no. 3, 2023, pp. 1-13. 10.71856/impcs.2023.903612

[34] Kumar, P., Gupta, G. P. (2024). Hybrid deep learning-based threat intelligence framework for securing Internet of Things. *IEEE Transactions on Information Forensics and Security*, *19*, 882–895. https://doi.org/10.1109/TIFS.2023.3321500

[35] Shahpar, Z., Badragheh, M. (2026). Presenting a Hybrid Model on Machine Learning and Principal Component Analysis for Action Detection in the Internet of Things. Journal of Information and Communication Technology, vol. 17, no. 66.

[36] davami, F. , Derakhshan-Barjoei, P. and Shaviklou, N. (2026). Detecting abnormal nodes in IoT security using neural networks and graph theory. *Tabriz Journal of Electrical Engineering*, doi: 10.22034/tjee.2026.69361.5088

[37] zeraatkarmoghaddam, m., ghayori, m. (2023). Improvement of intrusion detection system on Industrial Internet of Things based on deep learning using metaheuristic algorithms. Journal of Information and Communication Technology, vol. 15, no. 57, pp. 165-190.

[38] Abdi, A., Salimi-Badr, A., Souzani, A.(2026). A Self-supervised Sensors' Anomaly Detection Scheme in Industrial Control Systems based on Ensemble Deep Learning . Journal of Information and Communication Technology, vol. 17, no. 66.

Conference on Platform Technology and Service (PlatCon) (pp. 1–5). IEEE.

[22] Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. *IEEE Transactions on Emerging Topics in Computational Intelligence*, *2*(1), 41–50.

[23] Rahman, M. M., Al-Faraj, A., & Alshamrani, A. (2023). Transformer-CNN hybrid architecture for real-time DDoS attack detection in IoT networks. Computer Networks, 228, 109280. https://doi.org/10.1016/j.comnet.2023.109280

[24] Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. Journal of Information Security and Applications, 50, 102419. https://doi.org/10.1016/j.jisa.2019.102419

[25] Yadav, S., & Subramanian, S. (2016). Detection of application layer DDoS attack by feature learning using stacked autoencoder. In Proceedings of the International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT) (pp. 361–366). IEEE.

[26] Lopez-Martin, M., Carro, B., Sanchez-Esguevillas, A., & Lloret, J. (2017). Conditional variational autoencoder for prediction and feature recovery applied to intrusion detection in IoT.Sensors (Basel, Switzerland), 17(9), 1967. https://doi.org/10.3390/s17091967

[27] Luo, T., & Nagarajan, S. G. (2018). Distributed anomaly detection using autoencoder neural networks in WSN for IoT. In Proceedings of the IEEE International Conference on Communications (ICC) (pp. 1–6). IEEE.

[28] Chen, C., Zhao, L., Wang, J., & Li, Y. (2024). Graph neural network-based intrusion detection in software defined networking environments. Scientific Reports, 14, 65321. https://doi.org/10.1038/s41598-024-65321-7

[29] Yaseen, Z. M., Hameed, A., & Karim, A. F. (2024). Hybrid autoencoder and convolutional neural network for intrusion detection in fog-enabled IoT systems. IEEE Access, 12, 87102–87118. https://doi.org/10.1109/ACCESS.2024.3456712