Journal Website

Article history:
Received 28 September 2024
Revised 24 October 2024
Accepted 16 December 2024
Published online 25 December 2024

Dynamic Management and Business Analysis

Volume 3, Issue 4, pp 176-190

E-ISSN: 3041-8933

Design and Implementation of a Hybrid Deep Learning Algorithm for IoT Attack Detection Using Harmony Search for Hyperparameter Optimization and Feature Selection

Zahra Bakhshali[1], Alireza Poorebrahimi[2]*, Ahmad Ebrahimi[3], Nazanin Pilehvari[4]

[1] PhD student, Department of Information Technology Management, Science and Research Branch, Islamic Azad University, Tehran, Iran.
[2] Assistant Professor, Department of Industrial Management, Karaj Branch, Islamic Azad University, Alborz, Iran (Corresponding author).
[3] Assistant Professor, Department of Industrial Management and Technology, Science and Research Branch, Islamic Azad University, Tehran, Iran.
[4] Professor, Department of Industrial Management, West Tehran Branch, Islamic Azad University, Tehran, Iran.
*** Corresponding author email address**: poorebrahimi@gmail.com

A r t i c l e I n f o

Article type:
Original Research

How to cite this article:
Bakhshali Z, Poorebrahimi A, Ebrahimi A, Pilehvari N. (2024). Design and Implementation of a Hybrid Deep Learning Algorithm for IoT Attack Detection Using Harmony Search for Hyperparameter Optimization and Feature Selection. *Dynamic Management and Business Analysis*, *3*(4), 176-190.
https://doi.org/10.61838/

A B S T R A C T

Objective: The primary objective of this study is to design and implement a hybrid deep learning algorithm that integrates CNN and LSTM architectures for the proactive detection of attacks in IoT networks.

Methodology: This study develops a hybrid CNN-LSTM algorithm for IoT attack detection, utilizing Harmony Search for both hyperparameter optimization and feature selection. The Harmony Search algorithm is applied in two optimization stages: first for tuning hyperparameters, and second for selecting relevant features. The hybrid model is trained on IoT data and evaluated based on metrics such as accuracy, precision, recall, and F1 score.

Findings: The results indicate that the CNN-LSTM model optimized with Harmony Search demonstrates superior accuracy and efficiency in detecting IoT attacks compared to traditional methods, leading to improved key performance indicators and reduced computational overhead.

Conclusion: This approach can serve as a robust solution for proactive IoT attack detection and other security challenges.

Keywords: *Harmony Search algorithm, Neural Networks, CNN-LSTM model, feature selection*

EXTENDED ABSTRACT

Introduction

The rapid expansion of the Internet of Things (IoT) has revolutionized various industries, including healthcare, smart homes, smart cities, and industrial automation. However, this growth has significantly increased the vulnerability of IoT systems to cyberattacks, presenting critical security challenges. Traditional security methods often fail to address the dynamic and complex nature of IoT environments effectively (Yousefnezhad et al., 2020). This study introduces an innovative approach leveraging advanced deep learning techniques alongside metaheuristic optimization to enhance the detection of IoT network attacks.

In recent years, IoT security has made notable advancements, emphasizing early attack detection to prevent potential damages and ensure the reliability of IoT systems. Conventional approaches, such as signature-based and anomaly-based detection using statistical models, have limitations in scalability and adaptability. Advances in machine learning and deep learning suggest significant potential to improve detection accuracy and response times. While LSTMs excel in processing temporal data, CNNs demonstrate remarkable capabilities in spatial data analysis. Despite these advancements, challenges like hyperparameter optimization and feature selection remain critical, as they substantially impact model performance (Gautam et al., 2022; Khan, 2021; Khan et al., 2019).

This study aims to address these challenges by developing a hybrid deep learning model combining CNN and LSTM architectures, optimized using Harmony Search, a metaheuristic algorithm. The proposed model focuses on three primary objectives: optimizing hyperparameters for effective model training, selecting relevant features to enhance performance, and evaluating the model's efficiency using comprehensive IoT datasets. By tackling these goals, the research intends to provide a robust and efficient solution for IoT attack detection, addressing the limitations of current methods and contributing to the field with innovative optimization techniques and experimental validation.

Methodology

The proposed methodology for detecting intrusions in IoT networks comprises four main stages: data loading and preprocessing, data splitting, model tuning, and model evaluation. Initially, IoT network data is loaded and preprocessed, including handling missing values using appropriate imputation techniques, normalizing data to scale features uniformly, and encoding target variables for machine learning compatibility. Subsequently, data is divided into training and testing sets, ensuring both sets are normalized separately to prepare them for model training.

The model tuning stage incorporates weight balancing to mitigate data imbalance, hyperparameter tuning using custom-defined functions, and feature selection through Harmony Search optimization. This stage ensures that the model is trained with optimal hyperparameters and features, enhancing its accuracy and efficiency. A hybrid deep learning model, combining CNN, GRU, and LSTM layers, is designed to leverage both spatial and temporal data features. CNN layers extract spatial features, while GRU and LSTM layers focus on temporal relationships, with the model’s architecture optimized through iterative adjustments.

E-ISSN: 3041-8933

Model evaluation involves training the default and optimized models using the UNSW-NB15 dataset, a comprehensive IoT dataset containing both normal and attack traffic. Metrics such as accuracy, F1-score, precision, recall, AUC, and confusion matrix are used to assess the models' performance. Results indicate that the optimized model, which employs Harmony Search for hyperparameter and feature selection, significantly outperforms the default configuration, showcasing its efficacy for intrusion detection in IoT networks.

Findings

The findings demonstrate that the hybrid CNN-GRU-LSTM model, optimized using Harmony Search, outperforms existing models in detecting attacks on IoT networks. During evaluation on the UNSW-NB15 dataset, the model achieved an accuracy of 93.24%, precision of 89.00%, recall of 91.00%, and an F1 score of 90.00% on the test data. These metrics confirm the model’s ability to accurately distinguish between attack and normal traffic. Furthermore, the model achieved a ROC-AUC score of 93.24%, showcasing its superior capability in identifying true positive cases while minimizing false positives. Compared to individual models like CNN (accuracy: 90.50%, F1 score: 87.00%), GRU (accuracy: 91.20%, F1 score: 87.85%), and LSTM (accuracy: 91.50%, F1 score: 88.25%), the hybrid model consistently performed better across all evaluation metrics.

In comparative analysis, the proposed hybrid model also surpassed other combination models, such as CNN-LSTM, which achieved an accuracy of 92.00% and an F1 score of 88.75%. The superior results of the CNN-GRU-LSTM model can be attributed to its ability to integrate spatial feature extraction (via CNN) with temporal dependencies (via GRU and LSTM), while optimized hyperparameters and feature selection ensured enhanced performance. These results highlight the robustness and effectiveness of the proposed approach in securing IoT environments, emphasizing its potential as a reliable solution for intrusion detection in complex IoT networks.

Discussion and Conclusion

This study aimed to design and implement a hybrid deep learning algorithm for IoT attack detection, leveraging Harmony Search for hyperparameter optimization and feature selection. The results demonstrated that the proposed CNN-GRU-LSTM model outperformed standalone models like CNN, GRU, LSTM, and hybrid models such as CNN-LSTM across all key performance metrics, including accuracy (93.24%), precision (89.00%), recall (91.00%), and F1 score (90.00%). These findings underscore the effectiveness of combining spatial and temporal feature extraction methods with metaheuristic optimization for improving the accuracy and efficiency of IoT intrusion detection systems.

The research highlights the importance of hybrid models and optimization techniques in enhancing IoT network security. While this study provides valuable insights into using neural network architectures and optimization algorithms, challenges remain, such as testing models under diverse conditions and optimizing computational efficiency. Future research could explore the impact of larger and more diverse datasets, implement alternative optimization techniques, and evaluate other model combinations. Additionally, real-world applications of these systems could further validate their potential, contributing to enhanced security in IoT environments and fostering trust in smart technologies and industrial systems.

شاپای الکترونیکی: ۸۹۳۳-۳۰۴۱

مدیریت پویا و تحلیل کسب و کار

دوره ۳، شماره ۴، صفحه ۱۷۶-۱۹۰

وبسایت مجله

تاریخچه مقاله
دریافت شده در تاریخ ۷ مهر ۱۴۰۳
اصلاح شده در تاریخ ۳ آبان ۱۴۰۳
پذیرفته شده در تاریخ ۲۶ آذر ۱۴۰۳
منتشر شده در تاریخ ۵ دی ۱۴۰۳

طراحی و پیاده‌سازی الگوریتم یادگیری عمیق ترکیبی برای تشخیص حملات در اینترنت اشیا با استفاده از جستجوی هارمونی برای بهینه‌سازی فراپارامتر و انتخاب ویژگی

زهرا بخشعلی[۱]، علیرضا پورابراهیمی[۲*]، احمد ابراهیمی[۳]، نازنین پیله وری[۴]

۱. دانشجوی دکتری ، گروه مدیریت فناوری اطلاعات، واحد علوم وتحقیقات، دانشگاه آزاد اسلامی،تهران،ایران.
۲. استادیار، گروه مدیریت صنعتی، واحد کرج، دانشگاه آزاد اسلامی، البرز، ایران (نویسنده مسئول).
۳. استادیار، گروه مدیریت صنعتی و تکنولوی ، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران.
۴. استاد، گروه مدیریت صنعتی، واحد تهران غرب، دانشگاه آزاد اسلامی،تهران، ایران.
*ایمیل نویسنده مسئول: poorebrahimi@gmail.com

اطلاعات مقاله

نوع مقاله
پژوهشی اصیل

نحوه استناد به این مقاله:
بخشعلی ز، پورابراهیمی ع، ابراهیمی ا، پیله وری ن .(۱۴۰۳). طراحی و پیاده‌سازی الگوریتم یادگیری عمیق ترکیبی برای تشخیص حملات در اینترنت اشیا با استفاده از جستجوی هارمونی برای بهینه‌سازی فراپارامتر و انتخاب ویژگی. *مدیریت پویا و تحلیل کسب و کار*، ۳(۴)، ۱۷۶-۱۹۰.

چکیده

هدف: هدف اصلی این مطالعه طراحی و پیاده‌سازی یک الگوریتم ترکیبی یادگیری عمیق می‌باشد که معماری‌های CNN و LSTM را در جهت شناسایی پیشگیرانه حملات در شبکه‌های IoT ادغام می‌کند. **روش‌شناسی:** این مطالعه یک الگوریتم ترکیبی از CNN و LSTM برای شناسایی حملات IoT توسعه داده است که از جستجوی هارمونی برای بهینه‌سازی هایپرپارامترها و انتخاب ویژگی‌ها استفاده می‌کند. جستجوی هارمونی در دو مرحله بهینه‌سازی انجام می‌شود: ابتدا برای تنظیم هایپرپارامترها و سپس برای انتخاب ویژگی‌های مرتبط. مدل ترکیبی روی داده‌های IoT آموزش داده شده و بر اساس معیارهایی مانند دقت، دقت مثبت، بازیابی و امتیاز F1 ارزیابی می‌شود. **یافته‌ها:** نتایج نشان می‌دهند که مدل CNN-LSTM بهینه‌شده با جستجوی هارمونی، دقت و کارایی بهتری در شناسایی حملات IoT نسبت به روش‌های سنتی دارد و منجر به بهبود معیارهای کلیدی عملکرد و کاهش سربار محاسباتی می‌شود. **نتیجه‌گیری:** این رویکرد می‌تواند به عنوان راه‌حل قوی برای شناسایی پیشگیرانه حملات IoT و دیگر چالش‌های امنیتی مورد استفاده قرار گیرد.

کلیدواژگان: *الگوریتم جستجوی هارمونی، شبکه‌های عصبی، مدل CNN-LSTM ، انتخاب ویژگی.*

مقدمه

توسعه روزافزون اینترنت اشیاء (IoT) صنایع گوناگونی مانند بهداشت و درمان، خانه‌های هوشمند، شهرهای هوشمند و اتوماسیون صنعتی را متحول نموده است. با این وجود، این گسترش به طور چشمگیری بر آسیب‌پذیری سیستم‌های IoT در برابر حملات سایبری افزوده و چالش‌های امنیتی مهمی را ایجاد کرده است. اطمینان از وجود مکانیزم‌های شناسایی پیشگیرانه و قوی در جهت حفاظت از این دستگاه‌های متصل امری حیاتی به نظر می‌رسد (Chataut et al., 2023). شیوه‌های امنیتی سنتی غالبا در مقابله با محیط‌های پویا و پیچیده IoT ناکام می‌مانند. این مطالعه رویکرد نوینی را معرفی خواهد کرد که از تکنیک‌های پیشرفته یادگیری عمیق همراه با بهینه‌سازی فراابتکاری برای بهبود شناسایی حملات در شبکه‌های IoT بهره می‌برد.

در سال‌های اخیر، حوزه امنیت IoT پیشرفت‌های قابل توجهی داشته است. شناسایی زودهنگام حملات به منظور ممانعت از آسیب‌های بالقوه و حصول اطمینان از قابل اعتماد بودن سیستم‌های IoT بسیار حائز اهمیت و حیاتی می‌باشد. روش‌های متعارف از جمله: شناسایی مبتنی بر امضا و شناسایی ناهنجاری با استفاده از مدل‌های آماری دارای محدودیت‌هایی در مقیاس‌پذیری و تطبیق‌پذیری هستند. پیشرفت‌های اخیر در یادگیری ماشین و یادگیری عمیق بر این مطلب اشاره دارند که می‌توان دقت شناسایی و پاسخگویی را بهبود داد (Nazir et al., 2023; Yousefnezhad et al., 2020).

برای مثال، در حالی که شبکه‌های حافظه بلند مدت کوتاه (LSTM) در پردازش توالی‌های زمانی موفق هستند، شبکه‌های عصبی کانولوشنی (CNN) نیز در پردازش داده‌های مکانی عملکرد فوق‌العاده‌ای نشان داده‌اند. با وجود این پیشرفت‌ها، بهینه‌سازی هایپرپارامترها و انتخاب ویژگی‌های مرتبط همچنان چالش‌های مهمی به شمار می‌آیند که به طور قابل توجهی روی عملکرد مدل اثر می‌گذارند. مطالعاتی نیز تکنیک‌های بهینه‌سازی مختلف را بررسی نموده‌اند، ولی یک راه‌حل جامع که به طور همزمان از ترکیب CNN و LSTM با تنظیم بهینه هایپرپارامترها و انتخاب ویژگی‌ها بهره‌برداری کند، هنوز به طور کامل محقق نشده است (Raeisi et al., 2024; Sun et al., 2020).

در سال‌های اخیر، استفاده از الگوریتم‌های یادگیری عمیق برای تشخیص حملات در شبکه‌های اینترنت اشیاء (IoT) به شدت رشد کرده است. مدل‌های ترکیبی مختلفی از شبکه‌های عصبی به منظور بهبود دقت تشخیص و کاهش نرخ مثبت کاذب ارائه شده است. به‌عنوان مثال، Emeç و Özcanhan (۲۰۲۲) مدل BLSTM-GRU را برای تشخیص حملات IoT معرفی کردند که با استفاده از دیتاست‌های CIC-IDS-2018 و BoT-IoT عملکرد بهتری نسبت به مدل‌های پیشین داشته است (Emeç & Özcanhan, 2022). همچنین، Gautam et al. (۲۰۲۲) مدلی ترکیبی از RNN، LSTM و GRU برای بهینه‌سازی ویژگی‌ها و تشخیص حملات پیشنهاد کردند که با استفاده از دیتاست CICIDS2017 نتایج بسیار مطلوبی ارائه داد (Gautam et al., 2022). در مقایسه با این مدل‌ها، Khan et al. (۲۰۱۹) سیستم Conv-LSTM را معرفی کردند که به‌طور خاص بر مقیاس‌پذیری و پردازش داده‌های بزرگ تمرکز دارد و عملکرد بهتری نسبت به روش‌های موجود بر روی دیتاست ISCX-UNB دارد (Khan et al., 2019). Aldallal (۲۰۲۲) نیز سیستم Cu-LSTMGRU را برای تشخیص حملات با استفاده از الگوریتم‌های همبستگی پیرسون توسعه داد که توانسته است عملکرد بهتری نسبت به مدل‌های قبلی از لحاظ دقت و نرخ مثبت کاذب ارائه دهد (Aldallal, 2022). در نهایت، Khan (۲۰۲۱) با معرفی سیستم HCRNNIDS که از ترکیب شبکه‌های عصبی کانولوشنی و بازگشتی استفاده می‌کند، به‌طور خاص به تشخیص و طبقه‌بندی حملات با دقت بالا و کاهش هشدارهای غلط پرداخته است (Khan, 2021). این مطالعات نشان می‌دهند که مدل‌های هیبریدی و ترکیبی به‌طور چشمگیری توانسته‌اند دقت تشخیص حملات را افزایش دهند، اما همچنان با چالش‌هایی نظیر نیاز به منابع سخت‌افزاری بالا و محدودیت‌های دیتاست‌های مورد استفاده مواجه هستند.

پژوهش‌های انجام شده کنونی در امنیت IoT فاقد رویکردی یکپارچه هستند که به طور موثر نقاط قوت CNN و LSTM را ترکیب کرده و به چالش‌های مهم بهینه‌سازی هایپرپارامترها و انتخاب ویژگی‌ها بپردازد. شیوه‌های موجود یا روی تنها یک جنبه تمرکز دارند و منجر به عملکرد کافی نمی‌شوند، یا از تکنیک‌های جستجوی فراگیر استفاده می‌کنند که از نظر محاسباتی هزینه‌بر و برای کاربردهای بلادرنگ غیر عملی می‌باشند. پژوهش پیش رو قصد دارد این شکاف را با توسعه یک مدل ترکیبی یادگیری عمیق که با بهره‌گیری از جستجوی هارمونی، یک الگوریتم بهینه‌سازی فراابتکاری، بهینه‌سازی شده است پر نماید.

هدف اصلی این مطالعه طراحی و پیاده‌سازی یک الگوریتم ترکیبی یادگیری عمیق می‌باشد که معماری‌های CNN و LSTM را در جهت شناسایی پیشگیرانه حملات در شبکه‌های IoT ادغام می‌کند. به طور مشخص، این پژوهش به دنبال:

۱. بهره‌گیری از جستجوی هارمونی به منظور انتخاب هایپرپارامترهای بهینه، به طوری که مدل با موثرترین پارامترها آموزش ببیند.

۲. استفاده از جستجوی هارمونی در جهت انتخاب ویژگی‌ها، برای شناسایی ویژگی‌های مرتبط از مجموعه داده‌ها به منظور بهبود عملکرد مدل.

۳. ارزیابی عملکرد مدل پیشنهادی با به کارگیری مجموعه داده‌های جامع IoT و مقایسه آن با روش‌های موجود.

از مسیر پرداختن به این اهداف، مطالعه در پی توسعه راه‌حلی قوی و کارآمد برای شناسایی حملات IoT است که محدودیت‌های روش‌های فعلی را برطرف نماید.

پژوهش حاضر چندین مشارکت مهم را به حوزه امنیت IoT ارائه می‌دهد:

۱. مدل ترکیبی نوین: ادغام شبکه‌های CNN و LSTM راه‌حل جامعی را فراهم می‌کند که از نقاط قوت هر دو معماری در جهت بهبود میزان دقت و ارتقای سطح کارایی شناسایی بهره می‌برد.

۲. تکنیک‌های بهینه‌سازی: کاربرد جستجوی هارمونی به منظور بهینه‌سازی هایپرپارامترها و انتخاب ویژگی‌ها رویکردی نوآورانه است که عملکرد مدل را بهبود بخشیده و سربار محاسباتی را کاهش می‌دهد.

۳. اعتبارسنجی تجربی: طیف وسیعی از آزمایش‌ها و مقایسه با روش‌های موجود بیانگر اثربخشی مدل پیشنهادی می‌باشد و داده‌های تجربی جدیدی برای پژوهش‌های آینده فراهم می‌نماید.

روش پژوهش

مدل پیشنهادی به منظور تشخیص نفوذ در شبکه‌های اینترنت اشیاء (IoT) مشتمل بر چهار مرحله اصلی می‌باشد که در فلوچارت نمایش داده شده است: بارگذاری و پیش‌پردازش داده‌ها، تقسیم داده‌ها، تنظیم مدل و ارزیابی مدل.

در مرحله بارگذاری و پیش‌پردازش داده‌ها، ابتدا داده‌های مربوط به شبکه IoT بارگذاری می‌شوند. پس از آن داده‌ها برای شناسایی مقادیر مفقود بررسی شده و مقادیر مفقود با استفاده از تکنیک‌های مناسب جایگذاری می‌شوند. سپس، داده‌ها مجدداً مورد بررسی قرار می‌گیرند تا اطمینان حاصل شود که هیچ مقدار مفقودی باقی نمانده است. در ادامه، متغیر هدف برای استفاده در مدل کدگذاری شده و داده‌ها نرمال‌سازی می‌شوند تا مقادیر در یک مقیاس واحد قرار گیرند.

در مرحله تقسیم داده‌ها، داده‌ها به مجموعه‌های آموزشی و آزمایشی تقسیم می‌گردند و سپس داده‌های آموزشی و آزمایشی به طور جداگانه نرمال‌سازی می‌شوند. این مرحله تضمین می‌کند که مدل در مراحل بعدی بر اساس داده‌های نرمال‌سازی شده آموزش داده شود.

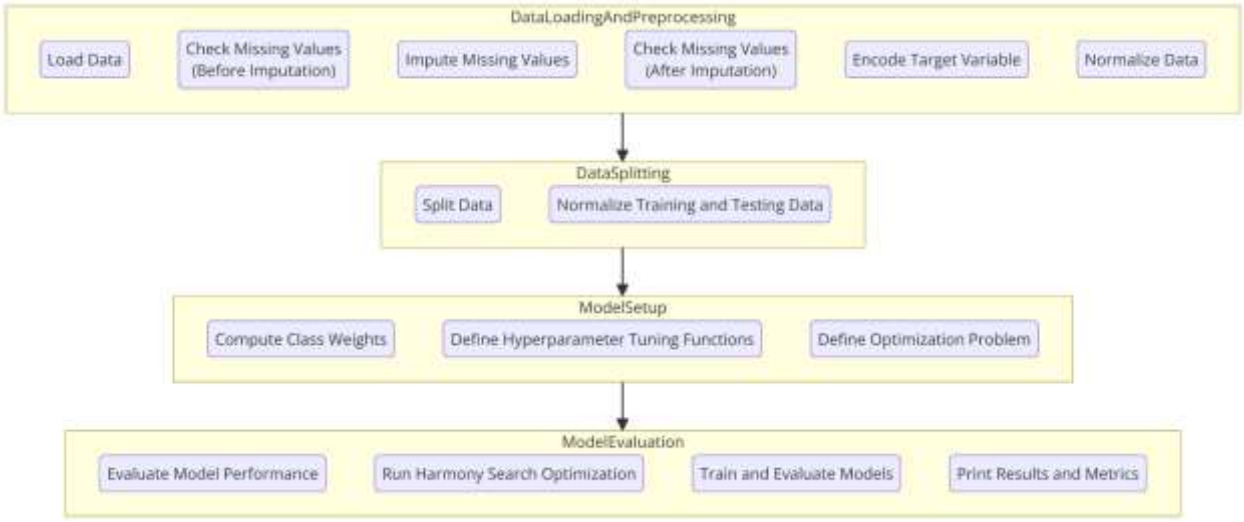
E-ISSN: 3041-8933

مرحله تنظیم مدل در بر دارنده سه بخش می‌باشد: ابتدا وزن کلاس‌ها محاسبه می‌شود تا تاثیر ناهماهنگی داده‌ها در کلاس‌های مختلف کاهش یابد. سپس توابعی برای تنظیم هایپرپارامترهای مدل تعریف می‌شوند و در نهایت، مسئله بهینه‌سازی برای یافتن بهترین هایپرپارامترها و ویژگی‌ها تعریف می‌گردد. این مرحله کمک می‌کند تا مدل با پارامترهای بهینه آموزش داده شود و دقت بالاتری داشته باشد.

در مرحله ارزیابی مدل، بهینه‌سازی هایپرپارامترها و انتخاب ویژگی‌ها با بهره‌گیری از الگوریتم جستجوی هارمونی انجام می‌پذیرد. سپس مدل‌های پیشنهادی آموزش داده شده و ارزیابی می‌شوند. در نهایت، نتایج و معیارهای ارزیابی مدل‌ها چاپ و تحلیل می‌گردند. این مرحله تضمین می‌کند که مدل‌های پیشنهادی بهینه شده و سطح بالایی از دقت در شناسایی حملات شبکه‌های IoT دارند.

شکل ۱

فلوچارت روش پیشنهادی



در ابتدا کتابخانه‌های لازم برای دستکاری داده‌ها، پیش‌پردازش، مدل‌سازی و بهینه‌سازی وارد می‌شوند.

به منظور رفع مشکلات احتمالی با داده‌های گم‌شده، تابعی به نام `check_missing` تعریف می‌شود تا مقادیر گم‌شده در مجموعه داده را شناسایی و چاپ کند. این تابع هر ستون را برای مقادیر گم‌شده مورد بررسی قرار می‌دهد و لیستی حاوی اطلاعات مربوط به ستون‌هایی که دارای مقادیر گم‌شده هستند، از قبیل تعداد مقادیر گم‌شده و نوع داده‌های آن‌ها، بازمی‌گرداند. این عملیات اطمینان حاصل می‌کند که مجموعه داده‌ها قبل از ادامه تحلیل به‌درستی تمیز شده‌اند.

سپس فرآیند جایگذاری (ایمپیوتر) برای مدیریت مقادیر گم‌شده اعمال می‌شود. ستون‌های عددی و دسته‌بندی به‌طور جداگانه شناسایی می‌شوند و `SimpleImputer` برای پر کردن مقادیر گم‌شده به کار می‌رود: ستون‌های عددی با میانگین هر ستون جایگذاری می‌شوند و ستون‌های دسته‌بندی نیز با بیشترین مقدار تکراری جایگذاری می‌گردند. پس از جایگذاری، مجموعه داده‌ها مجدداً برای هر گونه مقادیر گم‌شده مورد بررسی قرار می‌گیرند تا تأیید شود که فرآیند جایگذاری موفق بوده است.

در ادامه ، متغیر هدف نیاز به تبدیل به یک فرمت عددی دارد. این کار با استفاده از `LabelEncoder` انجام می‌گیرد که برچسب‌های دسته‌بندی را به مقادیر عددی تبدیل می‌کند. این مرحله برای اطمینان از اینکه الگوریتم‌های یادگیری ماشین می‌توانند متغیر هدف را به درستی پردازش کنند، ضروری می‌باشد.

در مراحل بعدی داده‌ها به دو بخش آموزش و آزمایش تقسیم شدند. این تقسیم‌بندی به مدل اجازه می‌دهد تا با داده‌های آموزشی یاد بگیرد و سپس با استفاده از داده‌های آزمایشی عملکرد خود را ارزیابی کند. در اینجا، ۸۰ درصد از داده‌ها به عنوان مجموعه آموزشی (`TRAIN_SPLIT`) و ۲۰ درصد باقی‌مانده به عنوان مجموعه آزمایشی در نظر گرفته شدند. این مرحله یکی از اصول مهم در یادگیری ماشین است که به مدل اجازه می‌دهد تا توانایی تعمیم‌پذیری خود را بر روی داده‌های نادیده بررسی نماید.

سپس تابع `multivariate_data` برای ایجاد داده‌های چندمتغیره استفاده شد. این تابع داده‌ها را به صورت توالی‌هایی از مشاهدات تاریخی برای هر نقطه زمانی آماده می‌کند. به طور خاص، این تابع با استفاده از پارامترهای `history_size` و `target_size`، مجموعه‌ای از داده‌های تاریخی و برچسب‌های مربوط به آن‌ها را ایجاد می‌نماید. در این مورد، `history_size` برابر با ۳۶ (تعداد مشاهدات گذشته) و `target_size` برابر با ۱ (تعداد مشاهدات آینده) تنظیم شده است. این داده‌های ورودی به دو بخش `X_train` و `y_train` در جهت آموزش و `X_test` و `y_test` برای آزمایش تقسیم شدند.

به منظور بهبود سطح عملکرد مدل، داده‌ها نرمال‌سازی شدند. نرمال‌سازی به این معنی است که مقادیر ویژگی‌ها به محدوده‌ای ثابت (معمولاً بین ۰ و ۱) مقیاس‌بندی شدند. این کار با استفاده از `MinMaxScaler` صورت گرفت. هر ویژگی به طور جداگانه نرمال‌سازی گردید تا تأثیر مقیاس‌های مختلف ویژگی‌ها کاهش یابد. همچنین، وزن‌های کلاس‌ها با بهره‌گیری از `class_weight` محاسبه گردیدند. این وزن‌ها به مدل در تشخیص بهتر کلاس‌های کم‌تعداد کمک می‌نمایند. وزن‌های کلاس‌ها به صورت دیکشنری ذخیره شده و در حین آموزش مدل مورد استفاده قرار می‌گیرند تا مدل بتواند تعادل بهتری بین کلاس‌های مختلف برقرار کند.

در ادامه تابع `get_hyperparameters` به منظور استخراج هایپرپارامترهای مدل شبکه عصبی از بردار ورودی `x` طراحی شده است. این تابع برای سه لایه شبکه عصبی تعداد نورون‌ها و نوع تابع فعال‌سازی را تعیین می‌کند. تعداد نورون‌های هر لایه با استفاده از مقادیر موجود در بردار ورودی و یک مقیاس خطی بین ۱۰ و ۵۰ محاسبه می‌گردد. همچنین، نوع تابع فعال‌سازی هر لایه از بین سه تابع ``relu`، `tanh`` و `sigmoid` انتخاب می‌شود. این تابع در نهایت دیکشنری‌ای شامل تعداد نورون‌ها و نوع توابع فعال‌سازی برای هر لایه را بازمی‌گرداند که در جهت پیکربندی مدل به کار می‌رود.

مدل شبکه عصبی `CNN_GRU_LSTM` مدلی ترکیبی است که شامل لایه‌های کانولوشنی، GRU و LSTM می‌باشد. این مدل ابتدا با به کارگیری یک لایه کانولوشن ۱ بعدی (`D۱Conv`) ویژگی‌های مکانی داده‌ها را استخراج می‌نماید. این لایه از تعدادی فیلتر با اندازه هسته ۳ و تابع فعال‌سازی انتخابی استفاده می‌کند. سپس یک لایه `D۱MaxPooling` برای کاهش ابعاد داده‌ها و حفظ ویژگی‌های مهم به کار می‌رود.

پس از لایه‌های کانولوشنی و ماکس‌پولینگ، لایه‌های GRU و LSTM به ترتیب به مدل اضافه می‌شوند. لایه GRU (Gated Recurrent Unit) با تعداد نورون‌ها و تابع فعال‌سازی مشخص شده، به مدل اجازه می‌دهد تا روابط زمانی در داده‌ها را بیاموزد. این لایه دارای `return_sequences=True` است که خروجی‌های توالی زمانی را به لایه بعدی ارسال می‌کند. سپس، لایه LSTM (Long Short-Term Memory) با تعداد نورون‌ها و تابع فعال‌سازی مشخص شده به مدل اضافه می‌شود که به آن امکان می‌دهد ویژگی‌های ترکیبی و پیچیده‌تر را استخراج کند. در انتها، لایه Flatten برای تبدیل داده‌های چندبعدی به یک بعدی و لایه Dense با تابع فعال‌سازی `sigmoid` در خصوص تولید خروجی نهایی مدل استفاده می‌شود.

E-ISSN: 3041-8933

کلاس `NeuralNetworkOptimization` که از کلاس `Problem` در کتابخانه `niapy` ارث‌بری می‌کند، به منظور بهینه‌سازی هایپرپارامترهای مدل شبکه عصبی طراحی شده و در این کلاس، تعداد بعدهای مسئله به تعداد هایپرپارامترهای شبکه عصبی به علاوه تعداد ویژگی‌های داده‌های ورودی تنظیم گردیده‌است. متغیرهای `X_train` و `y_train` داده‌های آموزشی را نگه می‌دارند.

تابع `evaluate_` مسئول ارزیابی یک بردار ورودی `x` است که هایپرپارامترها و ویژگی‌های انتخاب شده را نشان می‌دهد. ابتدا ویژگی‌های انتخابی با استفاده از مقادیر موجود در بردار `x` مشخص می‌شوند. سپس، هایپرپارامترهای شبکه عصبی از بردار `x` استخراج می‌گردند و مدل `CNN_GRU_LSTM` با این هایپرپارامترها ساخته و آموزش داده می‌شود. مدل با استفاده از وزن‌های کلاس‌ها و داده‌های آموزشی به مدت یک دوره آموزش داده شده و دقت آن ارزیابی می‌شود. تابع در نهایت مقدار منفی امتیاز مدل را بازمی‌گرداند، زیرا هدف بهینه‌سازی ماکسیمم کردن دقت مدل است.

در راستای اجرای بهینه‌سازی، یک شیء از کلاس `NeuralNetworkOptimization` ساخته شده و در شیء `Task` که پارامترهای مسئله و شرایط بهینه‌سازی را تعیین می‌کند، قرار می‌گیرد. سپس الگوریتم `HarmonySearch` با جمعیت اولیه ۱۰۰ اجرا می‌شود. الگوریتم با اجرای ۱۰۰ تکرار، بهترین مقادیر هایپرپارامترها و ویژگی‌های انتخاب شده را پیدا می‌نماید. پس از اجرای الگوریتم، بهترین هایپرپارامترها و ویژگی‌های انتخاب شده به معرض نمایش قرار می‌گیرند.

مدل پیش‌فرض و مدل بهینه‌سازی شده با داده‌های تست ارزیابی می‌گردند. مدل پیش‌فرض با تعدادی هایپرپارامترهای ثابت ساخته شده و با داده‌های آموزشی آموزش داده می‌شود. مدل بهینه‌سازی شده با استفاده از بهترین هایپرپارامترها و ویژگی‌های انتخاب شده ساخته و آموزش داده می‌شود. عملکرد هر دو مدل با به کارگیری معیارهای گوناگون از قبیل میزان دقت، امتیاز F۱، دقت کلاس، AUC بازیابی و ماتریس اغتشاش مورد ارزیابی خواهد بود. نتایج ارزیابی‌ها بیانگر آن است که مدل بهینه‌سازی شده عملکرد بهتری نسبت به مدل پیش‌فرض دارد.

در این تحقیق، از مجموعه داده UNSW-NB15 برای شبیه‌سازی و ارزیابی مدل‌های یادگیری ماشین استفاده شده است. این مجموعه داده به منظور ایجاد ترکیبی از فعالیت‌های عادی مدرن و رفتارهای حمله مصنوعی معاصر طراحی گردیده و در بر دارنده بسته‌های شبکه خام می‌باشد. مجموعه داده UNSW-NB1۵ توسط ابزار IXIA PerfectStorm در آزمایشگاه Cyber Range در UNSW Canberra تولید شده و هدف اصلی از ایجاد این مجموعه داده، فراهم‌سازی بستری برای ارزیابی و توسعه الگوریتم‌های تشخیص نفوذ و تحلیل ترافیک شبکه می‌باشد. این مجموعه داده به عنوان یکی از معتبرترین منابع برای بررسی رفتارهای عادی و حمله‌های گوناگون در شبکه‌های کامپیوتری به شمار می‌رود.

یافته‌ها

در این بخش، به بررسی و تحلیل نتایج حاصل از شبیه‌سازی‌ها و آزمایشات انجام شده با استفاده از مدل‌های یادگیری ماشین پرداخته می‌شود. هدف اصلی این تحلیل، ارزیابی کارایی و میزان دقت مدل‌های توسعه یافته در تشخیص حملات و تحلیل ترافیک شبکه با استفاده از مجموعه داده UNSW-NB۱۵ است. در ابتدا، عملکرد مدل‌ها بر اساس معیارهای مختلف ارزیابی شده و سپس با مدل‌های LSTM,GRU,CNN,CNN_LSTM مقایسه می‌شوند. این ارزیابی‌ها به منظور شناسایی نقاط قوت و ضعف هر مدل و ارائه پیشنهاداتی برای بهبود و ارتقاء آن‌ها صورت می‌گیرد. یافته‌های این تحقیق می‌تواند به توسعه ابزارهای کارآمدتر و دقیق‌تر برای تشخیص نفوذ و امنیت شبکه کمک کند. در ادامه، نتایج حاصل از آزمایشات به صورت جداول و نمودارهای مختلف ارائه شده و تحلیل‌های مربوطه به تفصیل بیان می‌شود.

به منظور ارزیابی عملکرد الگوریتم ترکیبی پیشنهادی، آن را با چند الگوریتم مقایسه کرده‌ایم. مقایسه‌ی این الگوریتم‌ها بر اساس پنج معیار اصلی ارزیابی صورت گرفته است:

۱. دقت (Accuracy Score):

- میزان صحت در تشخیص حملات و عدم حملات توسط الگوریتم‌ها مورد بررسی قرار گرفته است (Aribisala et al., 2022).

$$\text{Accuracy} = \frac{\text{True Positive} + \text{True Negative}}{\text{True Positive} + \text{True Negative} + \text{False Positive} + \text{False Negative}}$$

۲. دقت پیش‌بینی مثبت (Precision Score):

- توانایی الگوریتم‌ها در اعلام حمله در مواقعی که واقعاً حمله رخ داده است (Lin et al., 2020).

$$\text{Precision} = \frac{\text{True Positive}}{\text{True Positive} + \text{False Positive}}$$

۳. حساسیت (Recall Score):

- میزان تشخیص حملات توسط الگوریتم در مقابل کل حملات واقعی (Chattopadhyay, 2015).

$$\text{Recall} = \frac{\text{True Positive}}{\text{True Positive} + \text{False Negative}}$$

۴. امتیاز F1:

- ترکیبی از دقت پیش‌بینی مثبت و حساسیت، که نمایانگر توازن بین دو این معیار است (Chattopadhyay, 2015).

$$\text{F1 Score} = \frac{2\times \text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$

۵. مساحت زیر منحنی مشخصه عملگری (ROC-AUC Score):

- ارزیابی توانایی الگوریتم‌ها در تفکیک بین کلاس‌ها با در نظر گرفتن تجزیه‌وتحلیل مشخصه عملگری.

$$\text{ROC-AUC} = \frac{1}{2} \times (\text{ Sensitivity} + \text{Specificity})$$

در زیر پارامتر و هایپرپارامترهای که برای بهینه سازی به الگوریتم هارمونی استفاده شد را در یک جدول قرار می‌دهیم:

جدول ۱

هایپرپارامترهای که در مدل استفاده شده

E-ISSN: 3041-8933

Activation Function	RELU, tanh, sigmoid
Neurons per Layer	۱۰-۵۰

Activation Function توابع فعال‌سازی برای تعیین خروجی هر نورون در لایه‌های مخفی استفاده می‌شوند. انتخاب تابع فعال‌سازی مناسب می‌تواند بر عملکرد مدل تأثیر بسزایی داشته باشد. در این مدل، سه نوع تابع فعال‌سازی به کار گرفته شده‌اند:

- RELU (Rectified Linear Unit): یک تابع فعال‌سازی غیرخطی که مقدار ورودی را اگر مثبت باشد حفظ می‌کند و در غیر این صورت آن را به صفر تبدیل می‌نماید. این تابع به دلیل سادگی و کارایی بالا به طور گسترده‌ای در شبکه‌های عصبی استفاده می‌شود.
- tanh (Hyperbolic Tangent): این تابع، مقدار ورودی را به یک محدوده بین -۱ و ۱ نگاشت می‌کند. استفاده از این تابع به طور معمول به همگرایی سریع‌تر در برخی از شبکه‌های عصبی منجر می‌شود.
- sigmoid: یک تابع فعال‌سازی که مقدار ورودی را به یک محدوده بین ۰ و ۱ نگاشت می‌کند. این تابع بیشتر در لایه‌های خروجی برای مشکلات دسته‌بندی دودویی به کار می‌رود.

Neurons per Layer تعداد نورون‌ها در هر لایه از شبکه عصبی، که می‌تواند بین ۱۰ تا ۵۰ باشد. افزایش تعداد نورون‌ها معمولاً به افزایش ظرفیت یادگیری مدل منجر می‌شود، اما می‌تواند منجر به افزایش پیچیدگی و نیاز به محاسبات بیشتر گردد. انتخاب تعداد مناسب نورون‌ها به تعادل بین دقت مدل و کارایی آن کمک می‌کند.

این هایپرپارامترها بر اساس نیازهای مدل و ویژگی‌های داده‌ها تنظیم می‌شوند تا بهترین عملکرد ممکن به دست آید. تنظیم دقیق این پارامترها می‌تواند به بهبود دقت و کارایی مدل در پیش‌بینی نتایج یاری رساند.

جدول زیر پارامترهای کلیدی استفاده شده در الگوریتم جستجوی هارمونی به منظور بهینه‌سازی هایپرپارامترها و انتخاب ویژگی‌ها در مدل شبکه عصبی را نشان می‌دهد. این پارامترها شامل اندازه جمعیت، نوع بهینه‌سازی، حداکثر تعداد تکرارها و مقدار اولیه برای تولید اعداد تصادفی می‌باشند.

جدول ۲

پارامترهای جستجوی هارمونی

نام پارامتر	توضیحات	مقدار
population_size	تعداد نمونه‌های جمعیت اولیه	۱۰
max_iters	حداکثر تعداد تکرارها برای الگوریتم بهینه‌سازی	۵۰
optimization_type	نوع بهینه‌سازی (حداکثر یا حداقل‌سازی)	OptimizationType.MAXIMIZATION
Seed	مقدار اولیه برای تولید اعداد تصادفی (برای بازتولیدپذیری)	۱۲۳۴

این پارامترها با دقت انتخاب شده‌اند تا الگوریتم جستجوی هارمونی به طور مؤثری هایپرپارامترهای مدل را بهینه‌سازی کند و ویژگی‌های مناسب را انتخاب نماید. تنظیم دقیق این پارامترها می‌تواند به بهبود عملکرد و کارایی مدل کمک کند.

در این بخش، به تجزیه و تحلیل نتایج حاصل از فازهای آموزش و آزمایش مدل می‌پردازیم که با بهره‌گیری از آمار عملکردی نمایش داده شده است. این آمار به ما نشان می‌دهد که مدل ترکیبی CNN-GRU-LSTM چگونه توانسته با استفاده از الگوریتم‌های بهینه‌سازی پیشرفته و یادگیری عمیق، دقت بالایی در شناسایی حملات در شبکه‌های اینترنت اشیا (IoT) به دست آورد. نتایج به‌دست‌آمده از داده‌های آموزشی و آزمایشی به تفصیل در جدول زیر آورده شده تا میزان موفقیت مدل در هر دو فاز را به خوبی نشان دهد.

جدول ۳

جدول نتایج عملکرد مدل در داده‌های آموزشی و آزمایشی

معیار	داده‌های آموزشی	داده‌های آزمایشی
دقت(Accuracy)	۹۳.۸٪	۹۳.۲۴٪
دقت مثبت(Precision)	۹۰.۳٪	۸۹.۰۰٪
بازیابی(Recall)	۹۲.۲٪	۹۱.۰۰٪
نمره F۱ (F۱ Score)	۹۱.۵٪	۹۰.۰۰٪
منطقه زیر منحنی ROC (ROC AUC)	۹۴.۱۵٪	۹۳.۲۴٪

نتایج فوق نشان‌دهنده عملکرد مدل ترکیبی CNN-GRU-LSTM در تشخیص حملات در شبکه‌های اینترنت اشیا هستند. در هر دو فاز آموزش و آزمایش، مدل توانسته است دقت بالایی را به دست آورد که بیانگر توانایی مدل در شناسایی حملات است.

- دقت (Accuracy): میزان درستی پیش‌بینی‌های مدل را نشان می‌دهد. مدل در داده‌های آموزشی دقت ۹۳.۸٪ و در داده‌های آزمایشی دقت ۹۳.۲۴٪ را به دست آورده است.
- دقت مثبت (Precision): نشان‌دهنده تعداد نمونه‌های مثبت واقعی است که به درستی شناسایی شده‌اند. دقت مثبت مدل در داده‌های آموزشی ۹۰.۳٪ و در داده‌های آزمایشی ۸۹.۰۰٪ است.
- بازیابی (Recall): بیانگر تعداد نمونه‌های مثبت واقعی می‌باشد که توسط مدل شناسایی شده‌اند. بازیابی مدل در داده‌های آموزشی ۹۲.۲٪ و در داده‌های آزمایشی ۹۱.۰۰٪ است.
- نمره F1 (F1 Score): میانگین هماهنگ دقت و بازیابی را نشان می‌دهد. نمره F1 مدل در داده‌های آموزشی ۹۱.۵٪ و در داده‌های آزمایشی ۹۰.۰۰٪ است.
- منطقه زیر منحنی ROC (ROC AUC): نشان‌دهنده توانایی مدل در تمایز بین کلاس‌های مثبت و منفی است. مدل در داده‌های آموزشی ROC AUC برابر با ۹۴.۱۵٪ و در داده‌های آزمایشی ۹۳.۲۴٪ را به دست آورده است.

این نتایج نشان می‌دهد که مدل ترکیبی CNN-GRU-LSTM با استفاده از جستجوی هارمونی برای بهینه‌سازی فراپارامترها و انتخاب ویژگی‌ها، توانسته است به دقت و کارایی بالایی در شناسایی حملات در شبکه‌های اینترنت اشیا دست یابد. این امر بیانگر موفقیت رویکرد پیشنهادی در بهبود میزان امنیت و شناسایی حملات در محیط‌های پیچیده IoT می‌باشد.

E-ISSN: 3041-8933

جدول زیر نتایج عملکرد مدل پیشنهادی (CNN-GRU-LSTM) را با چهار الگوریتم دیگر مقایسه می‌کند: CNN، CNN-LSTM، GRU، و LSTM. معیارهای مورد استفاده برای مقایسه شامل دقت (Accuracy)، دقت مثبت (Precision)، بازیابی (Recall)، و نمره F1 (F1 Score) می‌باشند.

جدول ۴

نتایج مدل پیشنهادی و سایر الگوریتم‌ها

الگوریتم	دقت(Accuracy)	دقت مثبت(Precision)	بازیابی(Recall)	نمره(F۱ Score) F۱
مدل پیشنهادی	٪۹۳.۲۴	٪۸۹.۰۰	٪۹۱.۰۰	٪۹۰.۰۰
CNN	٪۹۰.۵۰	٪۸۶.۰۰	٪۸۸.۰۰	٪۸۷.۰۰
CNN-LSTM	٪۹۲.۰۰	٪۸۸.۰۰	٪۸۹.۵۰	٪۸۸.۷۵
GRU	٪۹۱.۲۰	٪۸۷.۰۰	٪۸۸.۷۰	٪۸۷.۸۵
LSTM	٪۹۱.۵۰	٪۸۷.۵۰	٪۸۹.۰۰	٪۸۸.۲۵

مدل پیشنهادی (CNN-GRU-LSTM): مدل ترکیبی پیشنهادی پژوهش حاضر با استفاده از شبکه‌های عصبی کانولوشنی (CNN)، واحدهای بازگشتی دروازه‌دار (GRU)، و شبکه‌های حافظه کوتاه‌مدت بلند (LSTM)، توانسته است در همه معیارها عملکرد بهتری نسبت به مدل‌های دیگر به دست آورد. این مدل دقت 93.24% (Accuracy)، دقت مثبت 89.00% (Precision)، بازیابی 91.00% (Recall) و نمره F1 (F1 Score) 90.00% را به دست آورده است.

CNN مدل شبکه عصبی کانولوشنی با میزان دقت ٪۹۰.۵۰، دقت مثبت ٪۸۶.۰۰، بازیابی ٪۸۸.۰۰ و نمره F1 برابر با ٪۸۷.۰۰ عملکرد نسبتاً خوبی داشته است، اما نسبت به مدل پیشنهادی کمترین دقت و نمره F1 را دارد.

CNN-LSTM این مدل ترکیبی از شبکه عصبی کانولوشنی و شبکه حافظه کوتاه‌مدت بلند بوده و سطح دقت ٪۹۲.۰۰، دقت مثبت ٪۸۸.۰۰، بازیابی ٪۸۹.۵۰ و نمره F1 برابر با ٪۸۸.۷۵ را به دست آورده است که عملکرد نسبتاً خوبی داشته اما همچنان کمتر از مدل پیشنهادی می‌باشد.

GRU مدل با واحدهای بازگشتی دروازه‌دار (GRU) میزان دقت ٪۹۱.۲۰، دقت مثبت ٪۸۷.۰۰، بازیابی ٪۸۸.۷۰ و نمره F1 برابر با ٪۸۷.۸۵ را به دست آورده است. این مدل نیز عملکرد خوبی داشته اما در مقایسه با مدل پیشنهادی همچنان کمترین مقادیر را دارد.

LSTM: مدل شبکه حافظه کوتاه‌مدت بلند (LSTM) سطح دقت ٪۹۱.۵۰، دقت مثبت ٪۸۷.۵۰، بازیابی ٪۸۹.۰۰ و نمره F1 برابر با ٪۸۸.۲۵ را به دست آورده است. این مدل عملکرد نسبتاً خوبی داشته اما همچنان کمتر از مدل پیشنهادی می‌باشد.

بحث و نتیجه‌گیری

هدف این پژوهش طراحی و پیاده‌سازی یک الگوریتم یادگیری عمیق ترکیبی در جهت تشخیص حملات در شبکه‌های اینترنت اشیا (IoT) با استفاده از جستجوی هارمونی برای بهینه‌سازی هایپرپارامترها و انتخاب ویژگی‌ها بود. این تحقیق با هدف بهبود دقت و کارایی مدل‌های تشخیص حملات و بررسی اثربخشی ترکیب مدل‌های CNN، GRU و LSTM در این حوزه انجام شد.

نتایج به‌دست‌آمده نشان داد که مدل ترکیبی پیشنهادی CNN-GRU-LSTM با استفاده از الگوریتم جستجوی هارمونی توانست در تمامی معیارهای ارزیابی عملکرد شامل دقت (Accuracy)، دقت مثبت (Precision)، بازیابی (Recall) و نمره F1 (F1 Score) بهبود

قابل توجهی نسبت به مدل‌های مانند CNN، CNN-LSTM، GRU و LSTM داشته باشد. به‌طور خاص، مدل پیشنهادی با میزان دقت ۹۳.۲۴٪، دقت مثبت ۸۹.۰۰٪، بازیابی ۹۱.۰۰٪ و نمره F1 برابر با ۹۰.۰۰٪ بهترین عملکرد را در شناسایی حملات در شبکه‌های اینترنت اشیا از خود نشان داد.

یافته‌های این تحقیق بیانگر سطح اهمیت به کارگیری مدل‌های ترکیبی و بهینه‌سازی هایپرپارامترها در بهبود دقت و ارتقای کارایی مدل‌های تشخیص حملات در شبکه‌های اینترنت اشیا می‌باشد. این نتایج می‌توانند در مسیر گسترش راهکارهای امنیتی پیشرفته‌تر در محیط‌های IoT مفید فایده بوده و مساعدت‌های شایانی ارائه نمایند. همچنین قادر خواهند بود میزان قابل ملاحظه‌ای از بهبود امنیت و کاهش تهدیدات را در این شبکه‌ها به همراه آورند. از دید نظری، این پژوهش به افزایش دانش در زمینه استفاده از شبکه‌های عصبی ترکیبی و الگوریتم‌های بهینه‌سازی در مسائل امنیتی IoT کمک می‌کند.

پژوهش حاضر نشان داد که استفاده از مدل‌های ترکیبی و الگوریتم‌های بهینه‌سازی می‌تواند بهبود قابل توجهی در تشخیص حملات داشته باشد، ولیکن همچنان سوالات و چالش‌هایی در این حوزه باقی‌مانده است. یکی از این سوالات، بررسی عملکرد مدل‌ها در شرایط مختلف و با داده‌های متنوع‌تر است. همچنین، نیاز به بررسی تاثیر پارامترهای مختلف بر عملکرد مدل و تعیین بهترین تنظیمات برای هر پارامتر احساس می‌شود.

تحقیقات آینده می‌توانند به تحلیل دقیق‌تر تاثیر داده‌های متنوع‌تر و حجیم‌تر بر عملکرد مدل‌ها بپردازند. همچنین، بهره‌گیری از تکنیک‌های بهینه‌سازی جدیدتر و مقایسه آن‌ها با جستجوی هارمونی می‌تواند مسیر جدیدی برای تحقیقات باشد. پیشنهاد می‌شود که تحقیقات آتی به بررسی استفاده از ترکیب مدل‌های دیگر و ارزیابی عملکرد آن‌ها در تشخیص حملات در شبکه‌های IoT بپردازند. همچنین، بهینه‌سازی زمان آموزش مدل‌ها و کاهش پیچیدگی محاسباتی نیز می‌تواند از جمله موضوعات مفید برای تحقیقات بیشتر باشد.

نتایج این پژوهش قادر خواهند بود به توسعه سیستم‌های تشخیص حملات پیشرفته‌تر در محیط‌های IoT کمک نمایند. این سیستم‌ها می‌توانند در صنعت، تکنولوژی‌های هوشمند، سیاست‌های امنیتی و سایر حوزه‌های مرتبط به کار گرفته شوند. در همین راستا افزایش سطح دقت و ارتقای کارایی مدل‌های تشخیص حملات به کاهش خطرات امنیتی و افزایش اعتماد به سیستم‌های IoT منجر می‌گردد. پژوهش‌های آتی می‌توانند با تمرکز روی پیاده‌سازی عملی این مدل‌ها و ارزیابی عملکرد آن‌ها در شرایط واقعی، تاثیر بیشتری بر توسعه فناوری‌های امنیتی داشته باشند.

تعارض منافع

در انجام مطالعه حاضر، هیچ‌گونه تضاد منافعی وجود ندارد.

مشارکت نویسندگان

در نگارش این مقاله تمامی نویسندگان نقش یکسانی ایفا کردند.

موازین اخلاقی

در انجام این پژوهش تمامی موازین و اصول اخلاقی رعایت گردیده است.

E-ISSN: 3041-8933

شفافیت داده‌ها

داده‌ها و مآخذ پژوهش حاضر در صورت درخواست از نویسنده مسئول و ضمن رعایت اصول کپی رایت ارسال خواهد شد.

حامی مالی

این پژوهش حامی مالی نداشته است.

References

Aldallal, A. (2022). Toward Efficient Intrusion Detection System Using Hybrid Deep Learning Approach. *Symmetry*, *14*(9). https://doi.org/10.3390/sym14091916

Aribisala, A., Khan, M. S., & Husari, G. (2022). Feed-Forward Intrusion Detection and Classification on a Smart Grid Network. 2022 IEEE 12th Annual Computing and Communication Workshop and Conference, CCWC 2022,

Chataut, R., Phoummalayvane, A., & Akl, R. (2023). Unleashing the Power of IoT: A Comprehensive Review of IoT Applications and Future Prospects in Healthcare, Agriculture, Smart Homes, Smart Cities, and Industry 4.0. *Sensors*, *23*(16). https://doi.org/10.3390/s23167194

Chattopadhyay, M. (2015). Modelling of intrusion detection system using artificial intelligence-evaluation of performance measures. In *Studies in Fuzziness and Soft Computing* (Vol. 319). https://doi.org/10.1007/978-3-319-12883-2_11

Emeç, M., & Özcanhan, M. H. (2022). A Hybrid Deep Learning Approach for Intrusion Detection in IoT Networks. *Advances in Electrical and Computer Engineering*, *22*(1). https://doi.org/10.4316/AECE.2022.01001

Gautam, S., Henry, A., Zuhair, M., Rashid, M., Javed, A. R., & Maddikunta, P. K. R. (2022). A Composite Approach of Intrusion Detection Systems: Hybrid RNN and Correlation-Based Feature Optimization. *Electronics (Switzerland)*, *11*(21). https://doi.org/10.3390/electronics11213529

Khan, M. A. (2021). HCRNNIDS: Hybrid convolutional recurrent neural network-based network intrusion detection system. *Processes*, *9*(5). https://doi.org/10.3390/pr9050834

Khan, M. A., Karim, M. R., & Kim, Y. (2019). A scalable and hybrid intrusion detection system based on the convolutional-LSTM network. *Symmetry*, *11*(4). https://doi.org/10.3390/sym11040583

Lin, W. H., Wang, P., Wu, B. H., Jhou, M. S., Chao, K. M., & Lo, C. C. (2020). Behaviorial-Based Network Flow Analyses for Anomaly Detection in Sequential Data Using Temporal Convolutional Networks. In *Lecture Notes on Data Engineering and Communications Technologies* (Vol. 41). https://doi.org/10.1007/978-3-030-34986-8_12

Nazir, A., He, J., Zhu, N., Wajahat, A., Ma, X., Ullah, F., Qureshi, S., & Pathan, M. S. (2023). Advancing IoT security: A systematic review of machine learning approaches for the detection of IoT botnets. *Journal of King Saud University - Computer and Information Sciences*, *35*(10). https://doi.org/10.1016/j.jksuci.2023.101820

Raeisi, N., Jafarinea, S., & Zare, H. (2024). Testing the Model for Enhancing Administrative Transparency in Interaction with E-Government Development Programs in the Social Security Organization. *Dynamic Management and Business Analysis*, *3*(1), 320-334. https://doi.org/10.61838/dmbaj.3.1.18

Sun, P., Liu, P., Li, Q., Liu, C., Lu, X., Hao, R., & Chen, J. (2020). DL-IDS: Extracting features using CNN-LSTM hybrid network for intrusion detection system. *Security and Communication Networks*. https://doi.org/10.1155/2020/8890306

Yousefnezhad, N., Malhi, A., & Främling, K. (2020). Security in product lifecycle of IoT devices: A survey. *Journal of Network and Computer Applications*, *171*. https://doi.org/10.1016/j.jnca.2020.102779