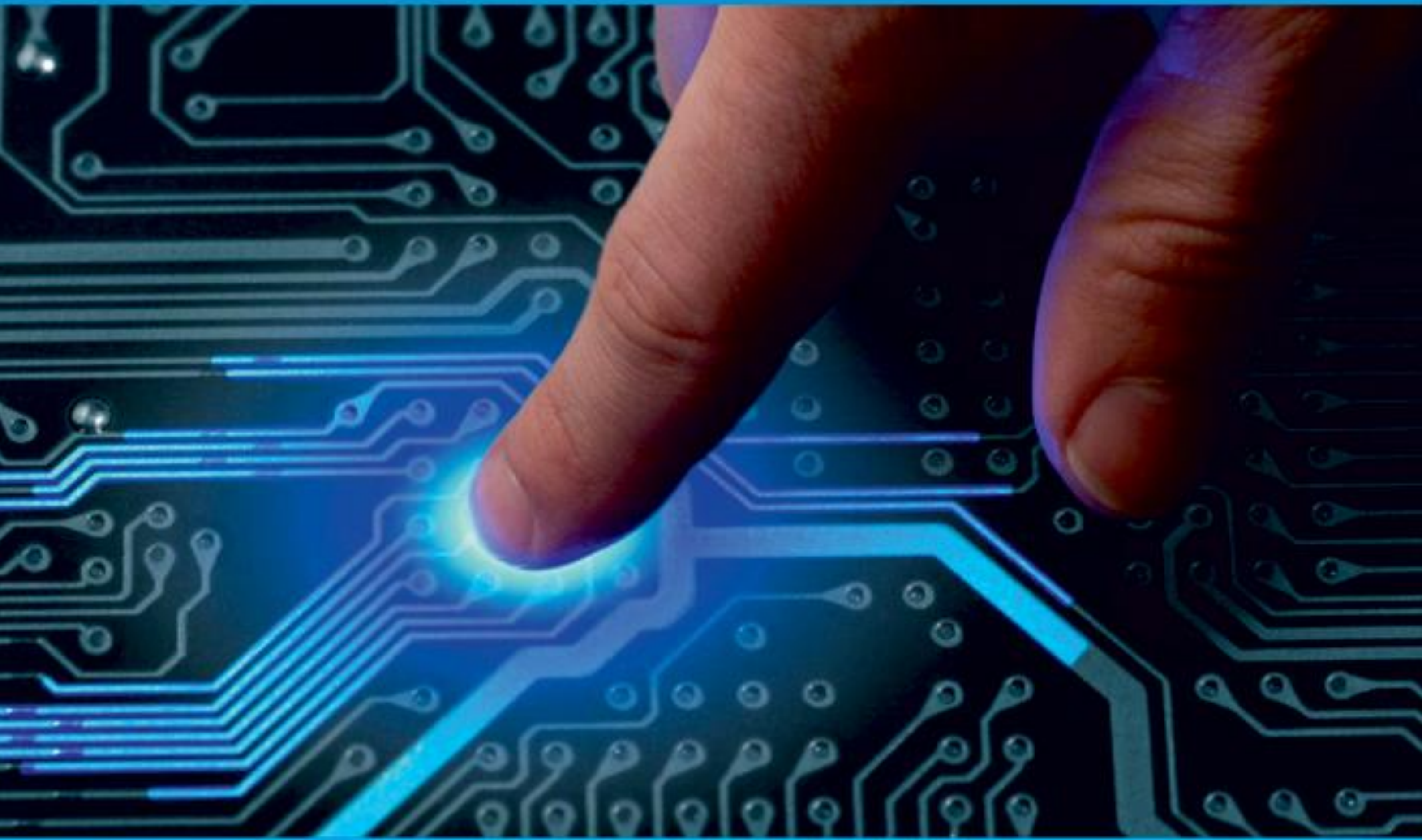
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 8, August 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.625

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Advanced Intrusion Detection System for D2D Communications Networks Using Machine Learning

VM Saravana Perumal, Jeevan M, Harsha Mallesh, Goutham P

Assistant Professor, Department of Computer Science Engineering, Rajarajeswari College of Engineering, Bangalore, Karnataka, India

U.G. Student, Department of Computer Science Engineering, Rajarajeswari College of Engineering, Bangalore, Karnataka, India

U.G. Student, Department of Computer Science Engineering, Rajarajeswari College of Engineering, Bangalore, Karnataka, India

U.G. Student, Department of Computer Science Engineering, Rajarajeswari College of Engineering, Bangalore, Karnataka, India

ABSTRACT: The abstract introduces a Deep Hierarchical Machine Learning (DHML) approach tailored for identifying security attacks in Device-to-Device (D2D) communication networks. While D2D technology enhances efficiency and flexibility in contemporary communication systems, its decentralized nature poses new security challenges. Conventional security measures struggle to detect emerging threats and novel attack patterns effectively. Our proposed DHML framework addresses this challenge by utilizing depth learning techniques to automatically learn hierarchical representations of network traffic patterns. This enables the identification of known hazards and identification of anomalies indicative of previously unseen threats. The hierarchical architecture of our model facilitates the combination of diverse data sources and the extraction of multi- level features, thereby enhancing the robustness of the detection system. Through immense experimentation on real-world D2D communication datasets, we de3monstrate the effectiveness of our approach, achieving superior performance in terms of accuracy compared to existing methods.

KEYWORDS: Text detection, Inpainting, Morphological operations, Connected component labelling.

I. INTRODUCTION

The introduction lays the groundwork by showcasing the significance of a new Deep Hierarchical Machine Learning (DHML) approach designed for identifying various security attacks within D2D communications networks. Our framework utilizing the features of deep learning to autonomously acquire hierarchical representations of network traffic patterns. This allows the system to detect both known attacks and anomalies indicative of previously unencountered threats.

The hierarchical structure of our model facilitates the integration of diverse data sources, enabling the extraction of multi-level features. This enhances the system's ability to withstand evasion techniques and learn the evolving landscape of threats. Through extensive experimentation on real-world D2D communication datasets, our aim is to showcase the scalability of our approach compared to present methods.

This paper showcases the design and implementation of our DHML framework, alongside a thorough evaluation of its performance in identifying known and unknown security attacks. Our discovery shows that our approach surpasses traditional methods in the form of accuracy, scalability, and resilience to adversarial manipulation.

II. FUNDAMENTAL DETAILS

A. Hierarchical Structure

The Deep Hierarchical Machine Learning Model (DHMLM) is built on a hierarchical architecture comprising multiple levels of Deep Neural Networks (DNNs). This hierarchical design provides the decomposition of complex security issues into smaller, interconnected problems, enabling themodel to effectively capture intricate patterns and data relationships. At each level of the hierarchy, specific aspects of data are learned, leading to a more nuanced understanding of network's security landscape. This hierarchical approach enhances the model's interpretability, scalability, and adaptability, making it well- suited for detecting a vast range of security threats in Device-to-Device (D2D) communication networks.

B. Unknown Attack Identification

A key feature of the DHMLM is its ability to detect unknown or Zero-day attacks, which are previously unseen security threats. By leveraging the hierarchical structure and advanced machine learning algorithms, the model can generalize patterns from known attacks to detect and classify novel threats effectively. This capability is essential for enhancing the network's resilience against emerging security risks and ensuring robust intrusion detection in dynamic environments.

C. Reduced Training Time

The DHMLM offers a significant advantage in training efficiency by employing one or two relatively shallow DNNs within the hierarchical framework. This design optimization results in reduced training time compared to traditional deep learning models, enabling quicker model deployment and real-time threat detection. The modular nature of model allows for parallel training of different levels in the hierarchy, leading to faster convergence and improved overall performance.

D. Enhanced Detection Accuracy:

Through the usage of hierarchical patterns of data and integration of diverse machine learning algorithms, the DHMLM achieves superior detection accuracy for many security threats, including Distributed Denial of Service (DDoS) attacks, SQL injection, and Man-in-the- Middle (MITM) attacks. The hierarchical architecture enables model to capture relationships and dependencies within the data, resulting in more precise and reliable detection of known and unknown security threats. This enhanced accuracy is required for effectively reducing risks and safeguarding D2D communication networks against malicious activities.

Feature Engineering
Constitutes a vital component of data preprocessing within machine learning, focusing on selecting, transforming, and crafting pertinent features from raw data to bolster model performance. In the realm of Intrusion Detection Systems (IDS) for threat detection, feature engineering assumes paramount importance, facilitating the extraction of meaningful insights from acoustic signals to enable precise threat identification.

The aim8 of feature engineering techniques is to accentuate crucial aspects of the DHML model that are most informative for predicting both known and unknown threats. This process may encompass extracting statistical attributes like mean, variance, and spectral properties from the acoustic signals, alongside devising domain-specific features.

Central to optimizing machine learning model performance is the pivotal role of feature engineering, which elevates the quality and relevance of input features. Through meticulous selection, transformation, and extraction of features rooted in domain expertise and data characteristics, feature engineering empowers models to adeptly capture underlying patterns and relationships. This, in turn, fosters heightened accuracy in predictions and enhances decision-making capabilities.

A. Data consistency

Data Validation Techniques: This process entails confirming the accuracy and completeness of collected data through checks for errors, inconsistencies, missing values, and outliers. Utilizing methods like cross- validation, outlier detection, and error checking ensures the reliability of data utilized for stress detection.
Quality Control Measures: Establishing rules for collection of data, storage, and processing is essential for maintaining consistency and reliability. Periodic audits and checks are performed to monitor data quality, promptly addressing any issues to uphold data integrity throughout the analysis process.

B. Existing System

The existing system in the factor of a D2D communications network comprises legacy infrastructure with technological limitations, data silos, security vulnerabilities, and scalability challenges. The system may be characterized by outdated software, fragmented data storage, potential security risks, and constraints in adapting to evolving business necessity and technological advancements. Integration complexities and inefficiencies in data management and security protocols further contribute to the system's limitations, hindering optimal performance, innovation, and responsiveness to changing requirements. Addressing these shortcomings through modernization, enhanced security measures, data integration strategies, and scalability enhancements is required to enhance the system's efficiency, resilience, and alignment with current industry standards and best practices.

C. Proposed System

Current DDoS defensive methods have struggled to effectively detect and react to attacks, often resulting in high false alarm rates and the necessity in real-time transmission of all packets simultaneously.

The detection system employs a two-step process to extract numerical or categorical information (features) from observed traffic: packet grouping and statistics computation. Packet grouping involves aggregating packets generated between the same pairs of applications by monitoring origin, destination, and protocol fields.

The obtained feature values are normal in nature and used as a training set, representing the regularity of network traffic changes. Despite similarities with conventional network data, the collected data still exhibit some differences due to the abrupt and volatile nature of network traffic.

During training, the objective is to reduce the cost function by iteratively updating all weights and biases within the model, also known as trainable or learnable parameters. Cost function calculates the error or loss in between the model's prediction and the ground truth of the input. Optimizing this cost function reduces prediction error.

In each training iteration, input data is fed forward through the network, the error is calculated, and then back-propagated through the network. This process continues until intersection, where further updates no longer reduce the error or the training process reaches the maximum number of epochs set.

III. CONCLUSION

The research introduced a novel Deep Hierarchical Machine Learning Model (DHMLM) tailored for detecting both known and unknown security threats in Device-to-Device (D2D) communication networks. Through its hierarchical architecture, the DHMLM displayed superior performance compared to existing methods, effectively identifying various types of attacks with high accuracy. These findings underscore the importance of robust and real-time Intrusion Detection Systems (IDS) powered by Artificial Intelligence/Machine Learning (AI/ML) techniques in safeguarding D2D networks.

In conclusion, the DHMLM emerges as a promising solution for bolstering the security of D2D communication networks. Leveraging its hierarchical design, the model exhibited reduced training times, the ability to detect multiple attack types, including Zero-Day attacks, and a simplified model structure with impressive overall accuracy. The

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

study's contributions include introducing the DHMLM for attack detection in D2D networks, developing a hierarchical IDS for enhanced performance, and creating a unique dataset comprising common attacks for training and evaluation purposes.

Firstly, exploring how Neural Networks can autonomously restructure to accurately identify Zero-Day attacks could enhance the model's adaptability to evolving threats. Additionally, delving into the significant correlation between certain attack patterns, such as NetBIOS and Port map attacks, may offer insights into improving the model's accuracy in classifying complex attack scenarios.

Moreover, broadening the implementation of IDS beyond D2D environments to encompass edge IoT networks could expand the applicability of the DHMLM in securing diverse network architectures. By expanding the dataset to encompass a wider array of attack variations, the model's sensitivity to evolving threat landscapes can be heightened, ensuring robust defense against sophisticated cyber threats.

Furthermore, future research may entail deploying identification models in Snort IDS and IPS systems to validate their efficacy in thwarting renowned attacks targetingD2D and IoT communication networks. By combining the DHMLM with established security tools like Sn2ort, the study aims to demonstrate the practical feasibility real-world network defence scenarios.

In summary, the study's conclusion submerges the significance of the DHMLM in fortifying D2D network security and outlines a scheme for further research attempts aimed at advancing the model's capabilities, addressing intricate attack scenarios, and validating its effectiveness in practical security implementations.

REFERENCES

[1] M. Bertalmio, G. Sapiro, V. Caselles, and C. Ballester, “Image inpainting”, in Proc. SIGGRAPH, pp. 417–424, 2000.
[2] A. Criminisi, P. Perez, and K. Toyama, “Region filling and object removal by exemplar-based image inpainting.”, IEEE Transactions on Image Processing, vol. 13, no.9, pp. 1200–1212, 2004.
[3] Marcelo Bertalmio, Luminita Vese, Guillermo Sapiro, Stanley Osher, “Simultaneous Structure and Texture Image Inpainting”, IEEE Transactions On Image Processing, vol. 12, No. 8, 2003.
[4] Yassin M. Y. Hasan and Lina J. Karam, “Morphological Text Extraction from Images”, IEEE Transactions On Image Processing, vol. 9, No. 11, 2000
[5] Eftychios A. Pnevmatikakis, Petros Maragos “An Inpainting System For Automatic Image Structure-Texture Restoration With Text Removal”, IEEE trans. 978-1-4244-1764, 2008
[6] S.Bhuvaneswari, T.S.Subashini, “Automatic Detection and Inpainting of Text Images”, International Journal of Computer Applications (0975 – 8887) Volume 61– No.7, 2013
[7] Aria Pezeshk and Richard L. Tutwiler, “Automatic Feature Extraction and Text Recognition from Scanned Topographic Maps”, IEEE Transactions on geosciences and remote sensing, VOL. 49, NO. 12, 2011
[8] Xiaoqing Liu and Jagath Samarabandu, “Multiscale Edge-Based Text Extraction From Complex Images”, IEEE Trans., 1424403677, 2006
[9] Nobuo Ezaki, Marius Bulacu Lambert , Schomaker , “Text Detection from Natural Scene Images: Towards a System for Visually Impaired Persons” , Proc. of 17th Int. Conf. on Pattern Recognition (ICPR), IEEE Computer Society, pp. 683-686, vol. II, 2004
[10] Mr. Rajesh H. Davda1, Mr. Noor Mohammed, “ Text Detection, Removal and Region Filling Using Image Inpainting”, International Journal of Futuristic Science Engineering and Technology, vol. 1 Issue 2, ISSN 2320 – 4486, 2013
[11] Uday Modha, Preeti Dave, “ Image Inpainting-Automatic Detection and Removal of Text From Images”, International Journal of Engineering Research and Applications (IJERA), ISSN: 2248-9622 Vol. 2, Issue 2, 2012
[12] Muthukumar S, Dr.Krishnan .N, Pasupathi.P, Deepa. S, “Analysis of Image Inpainting Techniques with Exemplar, Poisson, Successive Elimination and 8 Pixel Neighborhood Methods”, International Journal of Computer Applications (0975 – 8887), Volume 9, No.11, 2010

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

📱 9940 572 462 ☎ 6381 907 438 ✉ ijircce@gmail.com

www.ijircce.com

Scan to save the contact details