International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *30 May 2023* ***Revised:*** *25 July 2023* ***Accepted:*** *18 August 2023*

Applications of Deep Learning Approaches to Detect Advanced Cyber Attacks

Dr. Srinivas A Vaddadi,

PhD Research Graduate, Department of Information Technology, University of the Cumberlands , USA. Vsad93@gmail.com

Dr. Rohith Vallabhaneni,

PhD Research Graduate, Department of Information Technology, University of the Cumberlands , USA. rohit.vallabhaneni.2222@gmail.com

Dr. Abhilash Maroju,

Ph.D. Research Graduate, Department of Information Technology, University of the Cumberlands , USA. doctorabhilashmaroju@gmail.com

Sravanthi Dontu,

PhD Research Student, Department of Information Technology, University of the Cumberlands, USA. sravanthi.dontu13@gmail.com

ABSTRACT

The number and sophistication of cyber attacks have grown, making it tougher to detect and prevent them using traditional security technologies. Improving cyber threat identification and response has been greatly enhanced by deep learning, a subset of machine learning. Learn how to spot advanced cyberattacks with the help of Deep Learning algorithms in this article. The proposed approach collects, categorises, and arranges network traffic data using convolutional neural networks (CNNs) and intermittent neural networks (RNNs). Combining the RNN with the CNN allows us to capture temporal dependencies and derive spatial properties from the network data. In order to find the most important qualities for classification, the proposed method also incorporates a feature selection stage. To demonstrate that the proposed system outperforms signature-based and example AI systems in terms of exactness, accuracy, review, and F1-score, we conduct an exhibition survey using various datasets. An effective tool for improving cyber defences, the proposed method can detect zero-day and previously unknown attacks.

1. INTRODUCTION

An intelligent, adaptable, and networked production environment is the focus of the most recent industrial revolution, Industry 5.0, which aims to integrate cyber-physical systems, AI, and the IoT [1]. Efficiency, productivity, and personalisation have all been greatly enhanced as a result of this paradigm change in production. Additionally, it helps with resource optimisation, which means less waste and more energy efficiency. Consequently, several industries are being impacted by Industry 5.0, such as logistics, healthcare, agriculture, and the automobile industry [2].

The growing complexity and interconnectedness of Industry 5.0 systems has introduced new cybersecurity threats, making these systems more susceptible to web-based attacks. Industry 5.0's incorporation of internet of things (IoT) devices, big data, and cloud computing increases the attack surface, which in turn exposes weaknesses that cybercriminals could exploit. When it comes to matters of trust, security, and safety, cyber-physical accidents are on the rise as a result of the convergence of OT and IT [3].

Industry 5.0 infrastructure is vulnerable to a wide variety of web-based threats, including distributed denial of service (DDoS) attacks, SQL injection, and cross-site scripting. These threats can compromise sensitive information, halt operations, and even cause financial losses. The public's faith in new technology can be eroded by these kinds of assaults, which in

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
***Article Received:** 30 May 2023 **Revised:** 25 July 2023 **Accepted:** 18 August 2023*

turn can limit innovation and prevent their broad adoption [4]. Developing reliable and effective threat detection technologies is critical for protecting assets and ensuring the resilience of Industry 5.0 systems.

Using traditional machine learning methods, the issue of web-based attack detection has been addressed [5]. Clustering algorithms, decision trees, and support vector machines are some of the technologies that have shown promise in detecting typical attack patterns. But the intricacy and complexity of cyber threats are always increasing, and conventional methods often fail to keep up. Additionally, they struggle with skewed, large-scale datasets that are typical in cybersecurity applications.

Industry 5.0 cybersecurity could benefit from deep learning techniques, which have been extremely successful in several fields like image recognition, NLP, and speech recognition. Some methods may automatically learn complicated representations and patterns from simple input; these include RNNs, transformer models, and convolutional neural networks (CNNs). Because of this feature, deep-learning models can identify complex attacks that could otherwise go undetected by more conventional machine-learning techniques [6].

Additionally, cybersecurity datasets can be trained to overcome issues like non-stationarity, imbalance, and noise using deep learning approaches. To make attack detection systems that are more resilient and adaptive, you can integrate them with other AI approaches like adversarial learning and reinforcement learning. Deep learning approaches could significantly improve the detection and prevention of web-based risks in Industry 5.0 by exploiting these expanded capabilities. Because of this, the ever-evolving digital world may become more secure, safe, and long-lasting [7].

2. LITERATURE REVIEW

Cyberattack detection has been the subject of a great number of written material. Both GentleBoost and Bagged tree outperformed other measures linked to trees in terms of accuracy and ROC values while testing ensemble machine learning techniques on imbalanced datasets. By comparing the KDD-99 and NSL-KDD datasets, Ibrahimi et al. [8] show that PCA accurately distinguishes between malicious cyberattacks and normal internet queries.

Results from the experiments also revealed an issue with LDA, namely that it performs poorly when it comes to computing the covariance matrix. To prevent Denial of Service assaults, a crucial issue for communication networks, the Ozc¸elik's employ cumulative sum entropy detection. There was little evidence of false positives and excellent detection accuracy in the results. The findings are also better when contrasted with other detection methods that rely on the entropy obtained from packet header information. Support Vector Machine (SVM) is a Machine Learning (ML) approach that Ghanem employed in [9] to enhance the effectiveness of intrusion detection systems while decreasing the number of false positives.

New detection algorithms that could categorise both frequent and uncommon forms of attacks were generated using an innovative methodology in [10]. While the DFEL technique achieves better results than competing ML methods on the simpler KDD-99 and NSLKDD datasets, it has room to grow on the more complex UNSW-NB15 dataset that represents contemporary internet traffic.

Recent years have seen tremendous growth in the capabilities of deep learning, which can process both textual and visual data with remarkable speed and accuracy. To identify intrusions, the authors of [11] used a deep learning binomial classifier after applying the Gedeon approach to choose the top fifteen percent of features.

In order to create several training subsets, Wang Gang [12] used the fuzzy clustering method. Consequently, several classic ML methods, such decision trees and Naive Bayes, may not be the best choice when training multiple neural networks on separate training subsets.

In order to differentiate between DoS and non-DoS data, a Feed-forward Neural Network was constructed using unsupervised Correlation-based Feature Selection (CFS) in [13]. The results of these studies demonstrated effective intrusion detection. On the other hand, the correlation between training duration and performance was under-discussed. Traditional machine learning algorithms may take advantage of huge data with the help of DFEL, which also drastically reduces detection time. Additionally, DFEL determines the magnitude of the encoding latent variables by algorithm 1, which minimises the data dimension.

More complex and abstract features based on less abstract concepts make up the higher-level features. They stand in for the characteristics at the base of the learning hierarchy. Given this, a supervised predictor would benefit from the complex and high-level representations [14]. The DFEL method was developed based on existing research in visual classification [15-16-17] and word embedding text analysis, as well as several preceding investigations.

3. METHODOLOGY

This section delves into the approach that was employed to create and assess intrusion detection deep learning models. Various deep learning models (including CNNs, RNNs, and transformer models) are covered, along with dataset preparation and description, feature selection, and feature

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *30 May 2023* ***Revised:*** *25 July 2023* ***Accepted:*** *18 August 2023*

extraction. Furthermore, it specifies the evaluation criteria used to determine the models' effectiveness. The proposed method is illustrated at a high level in Figure 1.

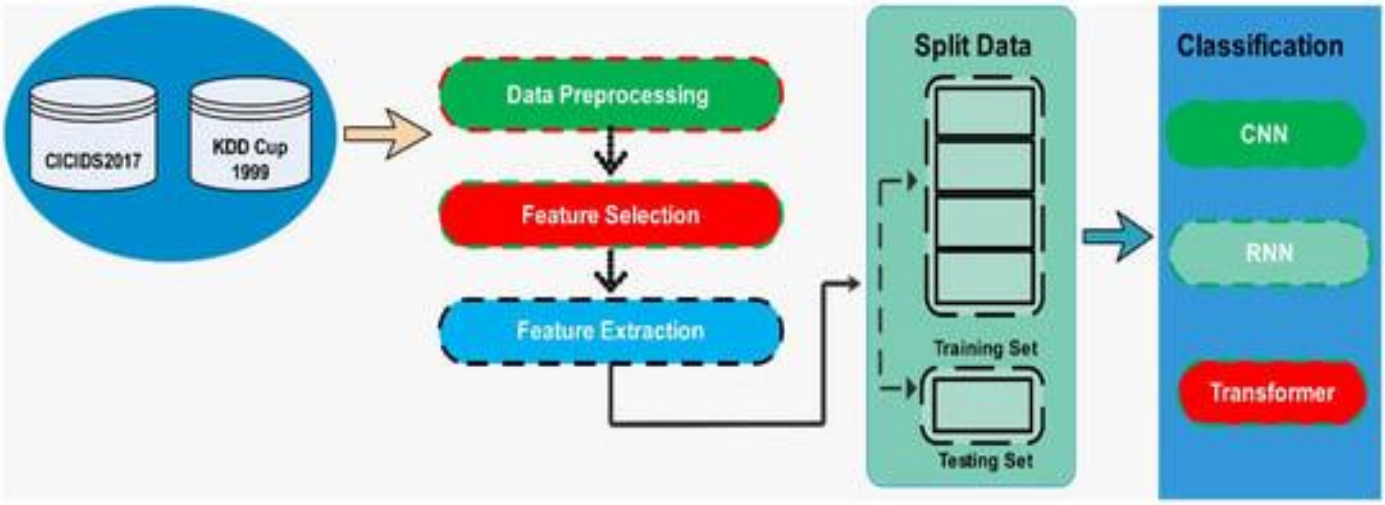

Figure 1. Proposed deep learning methodology for web-based Cyber attack detection.

3.1. Datasets and Pre-Processing

The dataset used in this study is a combination of two older datasets, the KDD Cup 1999 dataset and the more recent CICIDS2017 dataset. Database injection, distributed denial of service, and cross-site scripting are only a few examples of the many web-based assaults collected in these datasets. These datasets were created by recording TCP/IP traffic in a regulated network setting that was used to mimic different types of attacks. One can find a detailed summary in Table 1.

Table 1. Description of datasets.

Dataset	No. of Instances	Attack Types
KDD Cup 1999	5 million	DoS, R2L, U2R, probe
CICIDS2017	2.8 million	Brute force, web attack, infiltration, botnet, DDoS

Approximately 5 million connection records make up the KDD Cup 1999 dataset. We classify each connection as either "normal" or "attack" based on 41 characteristics. The four primary categories of attacks are denial of service (DoS), remote to local (R2L), user to root (U2R), and probing.

When it comes to researching and evaluating intrusion detection systems (IDS), the CICIDS2017 dataset is a go-to resource. Roughly 2.8 million cases with 79 features apiece make it up. The dataset does include human components in several ways, including the fact that real-world network traffic represents users' actual behaviour and activities, even if the primary focus is on system events and network traffic. When thinking about the human aspect in attack scenarios, it's important to diversify the motives and techniques of the attackers. Researchers can study and simula'e the human behaviour components of cyber-attacks with the use of the CICIDS2017 data, which includes source and destination IP addresses, ports, and protocol types. In addition, the methods used to exploit vulnerabilities and trick users can be better understood by analysing attack payloads. By looking at how it affects people's systems and data, this part adds to the human factor consideration.

It was necessary 'o clean the data by deleting duplicate entries and dealing with missing values before pre-processing could begin. To further decrease the possibility of bias towards characteristics with high magnitude, it was normalised to make sure all features are on the same scale. The min-max scaling method, which reduces the feature range to the interval [0, 1], was used to normalise the data.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
Article Received: *30 May 2023* ***Revised:*** *25 July 2023* ***Accepted:*** *18 August 2023*

4. RESULTS AND STUDY

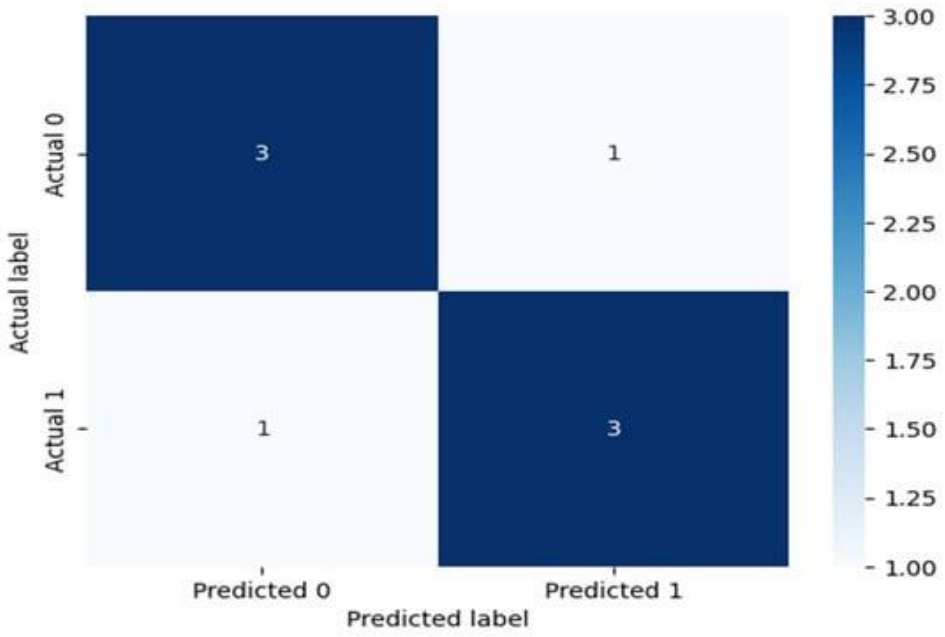

Figure 2. Confusion matrix of predicted data.

The three models all performed admirably, with F1 scores over 0.92 and accuracy levels over 0.94. This provides more evidence that deep learning methods have great promise for detecting web-based attacks in Industry 5.0. In Figure 2, we can observe the expected data confusion matrix.

Table 2. Performance of deep learning models.

Model	Accuracy	Precision	Recall	F1 Score
CNNs	0.94	0.92	0.91	0.92
RNNs	0.95	0.93	0.92	0.93
Transformer model	0.96	0.94	0.94	0.94

Table 2 displays the model performance according to the four metrics. The values represent the means of many experimental runs with various model initializations.

Table 3. F1 scores for different types of attacks.

Model	DDoS	SQL Injection	Cross-Site Scripting
CNNs	0.91	0.90	0.92
RNNs	0.92	0.91	0.93
Transformer Models	0.94	0.94	0.95

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
***Article Received:** 30 May 2023 **Revised:** 25 July 2023 **Accepted:** 18 August 2023*

We measured not only the overall performance but also the models' attack detection capabilities. Distributed denial of service (DDoS), SQL injection, and cross-site scripting are three prevalent forms of web-based attacks. Table 3 displays the F1 scores of each model for these threats.

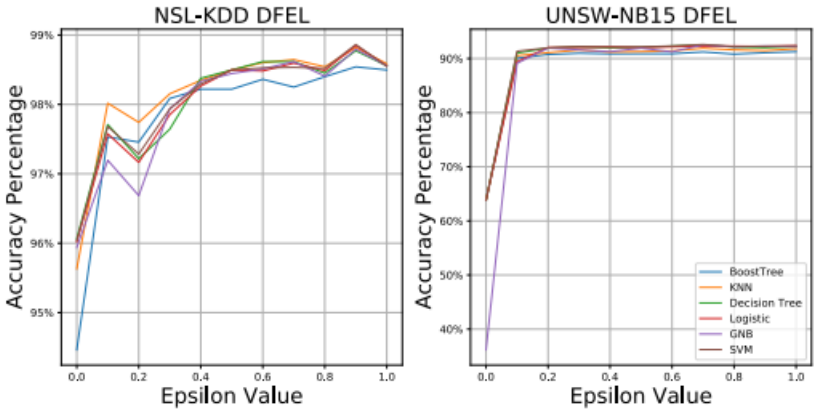

Fig. 4. ϵ effects on accuracy

Figure 4 displays the impact on classifier accuracy. The model's performance and the time it takes to identify cyberattacks can be balanced effectively by the ϵ.

CONCLUSIONS AND FUTURE WORK

The purpose of this work was to present DFEL, a novel deep learning method for detecting cyberattacks in the IoT environment in real-time. A high-level feature r (r < d) is mapped from the original low-level feature d, which is the fundamental concept of this method. The results show that our method is quite accurate and saves a lot of time in our experiment. When configured correctly, the IDS may balance detection speed with efficiency. This method could potentially be used in another setting that requires real-time prediction and has a lot of data. While our work does make a few important contributions, it does have several limitations that should be considered when planning future studies. First, we focused our research on three different types of deep learning models and three different types of attacks. Future research should examine several models and attacks to better understand the potential of deep learning for web-based threat detection. Secondly, we did not investigate the possibility of hybrid methods that integrate various approaches, even if our data show that our suggested models beat conventional methods. Such hybrid approaches could be the subject of future study; they have the ability to combine the best features of classical and deep learning approaches.

References

1. Coelho, P.; Bessa, C.; Landeck, J.; Silva, C. Industry 5.0: The Arising of a Concept. *Procedia Comput. Sci.* **2023**, *217*, 1137–1144. [**Google Scholar**] [**CrossRef**]
2. Leng, J.; Sha, W.; Wang, B.; Zheng, P.; Zhuang, C.; Liu, Q.; Wuest, T.; Mourtzis, D.; Wang, L. Industry 5.0: Prospect and retrospect. *J. Manuf. Syst.* **2022**, *65*, 279–295. [**Google Scholar**] [**CrossRef**]
3. Nahavandi, S. Industry 5.0—A human-centric solution. *Sustainability* **2019**, *11*, 4371. [**Google Scholar**] [**CrossRef**][**Green Version**]
4. Janković, A.; Adrodegari, F.; Saccani, N.; Simeunović, N. Improving service business of industrial companies through data: Conceptualization and application. *Int. J. Ind. Eng. Manag.* **2022**, *13*, 78–87. [**Google Scholar**] [**CrossRef**]
5. Raman, R.; Gupta, N.; Jeppu, Y. Framework for Formal Verification of Machine Learning Based Complex System-of-Systems. *Insight* **2023**, *26*, 91–102. [**Google Scholar**] [**CrossRef**]
6. Kolosnjaji, B.; Demontis, A.; Biggio, B.; Maiorca, D.; Giacinto, G.; Eckert, C.; Roli, F. Adversarial malware binaries: Evading deep learning for malware detection in executables. In Proceedings of the 2018 26th European Signal Processing Conference (EUSIPCO), Rome, Italy, 3–7 September 2018; pp. 533–537. [**Google Scholar**]
7. Stouffer, K.; Pease, M.; Tang, C.; Zimmerman, T.; Pillitteri, V.; Lightman, S. *Guide to Operational Technology (OT) Security*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2022. [**Google Scholar**]

8. Al-Doghman, F.; Moustafa, N.; Khalil, I.; Tari, Z.; Zomaya, A. Ai-enabled secure microservices in edge computing: Opportunities and challenges. *IEEE Trans. Serv. Comput.* **2022**, *16*, 1485–1504. [**Google Scholar**] [**CrossRef**]
9. Bertino, E.; Ghinita, G.; Kamra, A. Access control for databases: Concepts and systems. *Found. Trends® Databases* **2011**, *3*, 1–148. [**Google Scholar**]
10. Liu, Q.; Li, P.; Zhao, W.; Cai, W.; Yu, S.; Leung, V.C. A survey on security threats and defensive techniques of machine learning: A data driven view. *IEEE Access* **2018**, *6*, 12103–12117. [**Google Scholar**] [**CrossRef**]
11. Ullah, F.; Javaid, Q.; Salam, A.; Ahmad, M.; Sarwar, N.; Shah, D.; Abrar, M. Modified decision tree technique for ransomware detection at runtime through API Calls. *Sci. Program.* **2020**, *2020*, 8845833. [**Google Scholar**] [**CrossRef**]
12. Noor, U.; Anwar, Z.; Altmann, J.; Rashid, Z. Customer-oriented ranking of cyber threat intelligence service providers. *Electron. Commer. Res. Appl.* **2020**, *41*, 100976. [**Google Scholar**] [**CrossRef**]
13. Li, Z.; Zou, D.; Xu, S.; Jin, H.; Zhu, Y.; Chen, Z. Sysevr: A framework for using deep learning to detect software vulnerabilities. *IEEE Trans. Dependable Secur. Comput.* **2021**, *19*, 2244–2258. [**Google Scholar**] [**CrossRef**]
14. Yin, X.; Zhu, Y.; Hu, J. A comprehensive survey of privacy-preserving federated learning: A taxonomy, review, and future directions. *ACM Comput. Surv. (CSUR)* **2021**, *54*, 1–36. [**Google Scholar**] [**CrossRef**]
15. Ullah, F.; Salam, A.; Abrar, M.; Ahmad, M.; Ullah, F.; Khan, A.; Alharbi, A.; Alosaimi, W. Machine health surveillance system by using deep learning sparse autoencoder. *Soft Comput.* **2022**, *26*, 7737–7750. [**Google Scholar**] [**CrossRef**]
16. Ramya Manikyam, J. Todd McDonald, William R. Mahoney, Todd R. Andel, and Samuel H. Russ. 2016.Comparing the effectiveness of commercial obfuscators against MATE attacks. In Proceedings of the 6th Workshop on Software Security, Protection, and Reverse Engineering (SSPREW'16)
17. R. Manikyam. 2019.Program protection using software based hardware abstraction.Ph.D.Dissertation.University of South Alabama