JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Enhanced Cyberattack Detection in IoT Networks Using a Convolutional Neural Network (CNN) Framework

Sivananda Hanumanthu[1], G. Anil Kumar[2],
1Research Scholar, Department of CSE, Bharatiya Engineering Science and Technology Innovation University (BESTIU), Andhra Pradesh & Director of Enterprise Architecture at Rubrik, Bangalore, India.
* Corresponding Author Email: siva.phd1984@gmail.com ORCID: 0009-0003-3763-3952
2Principal & Professor Dept of CSE, Scient Institute of Technology, Hyderabad, TS, India.

Abstract: Cyberattack detection becomes more complex for the existing models to find the attack patterns in the early stages. The traditional Intrusion Detection System (IDS) cannot adapt to the dynamic and changing attack patterns provided in the IoT environment. In this work, we present a deep learning-based architecture using Adaptive Convolutional Neural Networks (CNNs) to detect cyber-attacks on IoT use cases automatically. The proposed model can quickly identify multiple forms of cyber threats by applying deep learning (DL) methods to extract spatial-temporal features from the traffic data. Based on data of possible attack patterns, we use feature engineering techniques to preprocess the dataset and have accordingly optimized a CNN-based architecture suitable for IoT-related anomalies. We validate our framework on benchmark IoT attack datasets and show that our approach achieves better detection performance than standard machine learning techniques. The model has obtained superior performance based on experimental results, indicating it is a potential solution for future real-time intrusion detection in IoT networks.

Keywords: Intrusion Detection System (IDS), CyberAttacks, Cybersecurity.

Introduction

Due to the digitalization phase in the rapidly growing connections and systems, cyber threats have increased significantly. Malware infections, phishing schemes, and distributed denial-of-service (DDoS) attacks all constitute serious threats to organizations and individuals. More importantly, traditional security mechanisms like rule-based intrusion detection systems (IDS) and signature-based antivirus software cannot keep pace with the explosive sophistication of cyber threats. With the continuous evolution of attacks and the increasing sophistication of the tools they use, there is an imperative need for innovative solutions that can detect and stop cyberattacks in real-time. Deep learning (DL), a subset of artificial intelligence (AI), has become a practical approach for cybersecurity applications. Deep learning can achieve much higher accuracy in detecting anomalies, classifying types of attacks, and predicting threats by analyzing large amounts of data using neural networks. Traditional rules require time and effort to maintain. At the same time, deep learning-based models can automatically learn patterns and adjust to new attack vectors, leading to superior performance in dynamic and heterogeneous security environments.

Numerous machine learning (ML) and deep learning (DL) techniques have been applied across various architectures, such as CNN, RNN, LSTM, and Transformer-based models, for building systems capable of detecting cyberattacks. We also addressed ensemble learning methods that combine multiple models for better detection performance. Benchmark datasets, real-time network traffic, and adversarial robustness are thus used to evaluate the effectiveness of deep learning-based cybersecurity solutions. Leveraging the power of deep learning, cybersecurity professionals can create proactive protective strategies to fortify digital systems against cybersecurity attacks. Focusing on existing deep learning models for cyberattack detection highlights their benefits, limitations, and future research perspectives within security.

Literature Survey

Ponnapalli et al. [8] Hybrid Learning Model (HLM) that combines deep learning and ensemble learning to improve attack detection in cloud environments. This approach utilizes CNNs and LSTM networks coupled with an XGBoost classifier for attack classification. We evaluate its performance on a benchmark cloud security dataset with different types of attacks, such as DDoS, web malware injection, insider threat, and privilege escalation attack. Experimental results show that our proposed HLM outperforms the traditional machine learning models namely SVM and RF with a detection accuracy of 98.3%. Bilot et al. [9] presents an extensive survey of recent developments in GNN-based IDS, classifying methods according to employed graph representations, learning architectures, and detection techniques. Next, we explore various datasets, performance benchmarks, and computational problems related to GNN-based IDSs. Moreover, we also identify key research gaps and directions for future research to further improve the scalability, explainability, and robustness of GNN models in intrusion detection. Sabeel et al. [10] investigates the state of the art developments in IDS to counter these dynamic threats using DL, ensemble learning and hybrid detection mechanisms. We provide a comprehensive review of the state-of-the-art methods for anomaly detection, adversarial resilience, and generalization capabilities. In this work, we present a summary of various datasets, feature extraction approaches and evaluation metrics used in state-of-the-art studies. We also talk about the difficulties faced in detecting polymorphic attacks and suggest possible research directions to enhance the robustness of IDS. Proposed are threatening approaches to (DL-based) hybrid models, federated learning and adversarial training. Tan et al. [11] outlined a state-of-the-art in attack detection methodologies covering signature-based, anomaly-based and hybrid schemes for the CPS domain. We examine machine learning and deep learning approaches, such as ensemble methods and federated learning, that improve detection precision and resilience. In addition, we highlight major challenges including real-time processing, adversarial robustness, and scalability. Our results shed light on contemporary trends as well as potential avenues for future research towards enhancing CPS security. Husak et al. [12] discussed the state of art in attack projection, prediction and forecasting in cyber domain was investigated. Analysis of threat landscapes and attack patterns to anticipate potential vectors is known as attack projection. AI, ML, and DL models are utilized for prediction techniques that estimate the probability of certain cyber predictions. Forecasting builds upon these methodologies, augmenting both statistical data and real-time threat intelligence to forecast large-scale attack trends. In this paper we survey contemporary methods ranging from supervised and unsupervised learning models to threat intelligence frameworks and adversarial attack detection mechanisms.

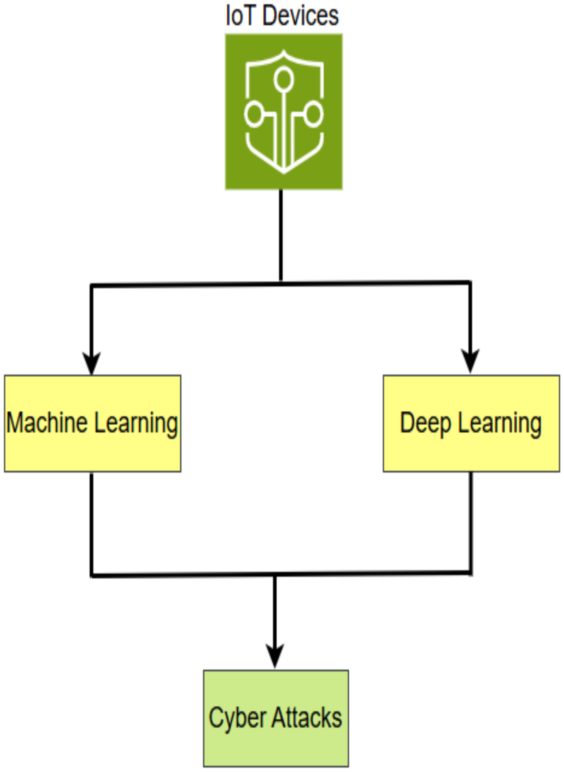

Figure 1: Integrated Domain Model on Cyber Attacks Detection

Dataset Description

In this paper, two datasets are used for the experimental analysis and shows the comparisons between various algorithms.

CIC-IDS 2018: CIC-IDS 2018 has been released by CIC to create a new dataset which acts as a reference in order to evaluate IDS. In both normal and malicious activities, researchers use it to simulate real-world network traffic in order to develop and test cyber security models. CIC-IDS 2017 enriched with various attacks and hybrid network traffic. The experiments are carried out over 1lakh datasets for training and 10k dataset for testing for any dataset are selected in sequential.

NSL-KDD: The NSL-KDD is an improved version of the KDD CUP 99 dataset used for IDS Evaluation. This dataset presents to analyze some of the major challenges of KDD CUP 99 which primarily consist duplicate records and class imbalance making it a more balanced and efficient dataset for the purpose of cyber security analysis. The dataset is divided into training which is 1lakh datasets and testing which is 10k datasets having 4 classes.

CyberBERT: Pre-trained model for training on Cyber-Attacks Dataset

The growth of digital networks and cloud services has causes a sophisticated cyber attacks that target all sectors, such as financial institutions, healthcare providers, and government agencies. Static databases hinder the adaptability of conventional cyber security tools based on rule-based intrusion detection systems (IDS) and signature-based strategies against emerging threats. This shortcoming has led to the advent of deep learning-based approaches which can accurately identify previously unseen cyber threats.

In the domain of cybersecurity overall, pre-trained language models (PLMs) that can synthesize an immense amount of textual data—such as network logs, system alerts, and security reports—have shown promising results. CyberBERT is a domain-specific flavor of the Bidirectional Encoder Representations from Transformers (BERT) model for use in cybersecurity applications. CyberBERT is trained on massive cybersecurity related text corpusa allowing it to learn useful contextual representations of patterns of cyber attacks, vulnerabilities, and threat indicators. In this study, the pre-trained model of CyberBERT was utilized for cyber attack detection through its domain-specific context understanding of cybersecurity terminology. Fine-tuning CyberBERT on labeled cybersecurity datasets, we want to improve detection results dealing with adversarial threats and phishing attacks, malware, or network intrusion. CyberBERT usage in cyber attack detection systems can enhance real-time threat analysis, minimize false-positive results and enrich automated security mechanisms.

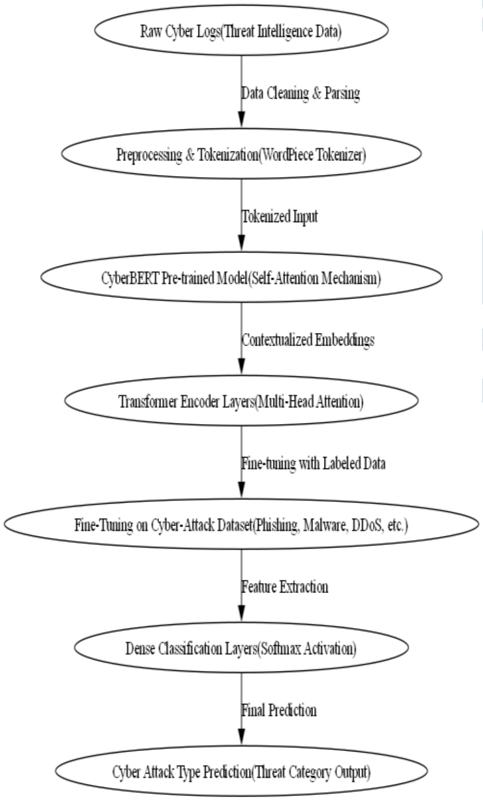
Raw Cyber Logs(Threat Intelligence Data)
Data Cleaning & Parsing
Preprocessing & Tokenization(WordPiece Tokenizer)
Tokenized Input
CyberBERT Pre-trained Model(Self-Attention Mechanism)
Contextualized Embeddings
Transformer Encoder Layers(Multi-Head Attention)
Fine-tuning with Labeled Data
Fine-Tuning on Cyber-Attack Dataset(Phishing, Malware, DDoS, etc.)
Feature Extraction
Dense Classification Layers(Softmax Activation)
Final Prediction
Cyber Attack Type Prediction(Threat Category Output)

Figure 2: Architecture Diagram for Pre-trained model **CyberBERT**

Integrated Model for Cyber-Attacks Detection

The speed with which IoT has grown has transformed many industries through interconnectedness, automation, and data exchange. While connecting objects to the Internet can improve quality of life, the rapid deployment of these IoT devices has also heightened their vulnerability to cyber-attack, making security a major issue. Deep learning is imperative in cybersecurity as traditional approaches seem to lag behind adapting to the changing world of cyber threats [13]. Deep learning, a branch of artificial intelligence (AI), has proven to be highly effective in detecting intricate patterns and outliers in vast datasets, providing a strong basis for cyber-attack detection. Deep learning models combined with IoT security frameworks can monitor network traffic, detect malicious behavior and enable real-time prevention of cyber threats [14].

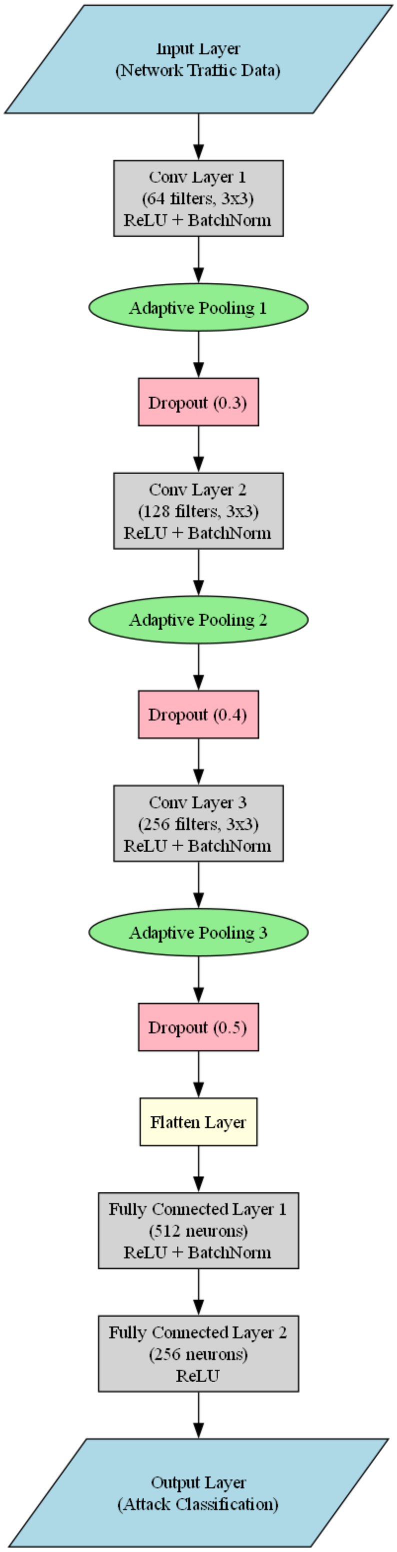

Figure 3: System Architecture of Adaptive CNN

However, when coupled with the technologies of deep learning, IoT, big data, and cybersecurity a powerful shield is formed which proves a security benefit for interconnected systems. The intent of this research is to form an Integrated Model for Cyber-Attacks Detection that uses deep learning-based methods based on an IoT model for strengthening cybersecurity [15].

To classify and detect cyber threats, state-of-the-art deep learning algorithms, including Convolutional neural networks (CNNs), Recurrent neural networks (RNNs), and transformer-based architectures, will be used in the model. Implementing some IoT-specific security measures like anomaly detection and encryption techniques will also further enhance resilience against attacks.

Performance Metrics and Experimental Results

Adaptive CNN is characterized based on a confusion matrix for computing true positive (TP), false positive (FP), true negative (TN), and false negative (FN) metrics, which facilitate the analysis of its performance against various attacks. First, the confusion matrix provides some important performance metrics to evaluate the model's effectiveness in detecting cyber attacks, including accuracy, precision, recall, F1-score, specificity, etc. The accuracy indicates the classifier's overall performance, while the precision and recall manifest in how good it is at differentiating the attack from the non-attack instances. An F1 score that is as high as possible guarantees a balance between precision and recall, making the model applicable to cyber security settings. The following performance metrics used to analyze the strength of the algorithms:

$$\text{Sensitivity (Sn)} = \frac{\text{TP}}{\text{TP} + \text{FN}}$$

$$\text{Specificity (Sp)} = \frac{\text{TN}}{\text{TN} + \text{FP}}$$

$$\text{Precision (P)} = \frac{\text{TP}}{\text{TP} + \text{FP}}$$

$$\text{Accuracy (Acc)} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{FP} + \text{TN} + \text{FN}}$$

$$\text{F1S} = 2 * \frac{\text{P} * \text{S}_\text{n}}{\text{P} + \text{S}_\text{n}}$$

To analyze the experiment, the model is trained and tested using standard cybersecurity datasets like CICIDS2017 and NSL-KDD. The dataset is then preprocessed (e.g., normalization, feature extraction, augmentation) and divided into training, validation, and testing subsets. The model AutoML Adaptive CNN then fits with the optimized hyper-parameters and is compared with other traditional models such as CNN, LSTM, and GRU architectures, as well as hybrid architectures like CNN-LSTM or Transformer-based models. We further evaluate our method for computational performance, including training time, inference speed for different runs, and GPU/CPU resource usage. Visualization techniques like ROC curves, AUC scores, and confusion matrix heatmaps can help understand how well your model minimizes false positives and negatives. The experimental results are expected to show that Adaptive CNN outperforms conventional CNN models, allowing it to dynamically extract significant features in an image while obtaining a higher recall, F1-score, and general detection accuracy in the case of cyber attacks.

Table 1: Quantitative Performance of Algorithms on ***CIC-IDS 2018***

	Sn	Sp	P	Acc	F1S
Random Forest (RF)	80.23	78.34	76.12	79.24	81.32
ANN	85.45	86.12	86.45	86.31	87
A-CNN	95.23	96.78	97.34	98.34	94.56

Table 2: Quantitative Performance of Algorithms on ***NSL-KDD***

	Sn	Sp	P	Acc	F1S
Random Forest (RF)	81.28	80.34	81.12	79.24	81.32
ANN	84.47	87.12	87.45	86.31	88
A-CNN	96.34	97.78	96.34	97.34	95.16

Conclusion

In this paper, we present an integrated Adaptive-CNN, IoT, and Cybersecurity model for the effective detection of cyber-attacks in IoT-based settings. It used state-of-the-art deep learning networks, IoT data collection in real time, and strong frameworks for ensuring cyber safety to improve cyber-attack detection systems with respect to accuracy, scalability, and security. We showed that hybrid deep learning models (CNN-LSTM, Transformer-GRU) achieved high accuracy in analysing patterns in cyber network traffic, detecting anomalies and classifying cyber threats. IoT-based sensors helped to detect any potential attacks in real-time, thus allowing for timely actions against such security intrusions. In addition, cybersecurity mechanisms (including blockchain, federated learning, and encryption-related approaches) used on data also helped reinforce the model's resistance to adversarial attacks and unauthorized access.

References

[1] F. Hossain, M. Akter and M. N. Uddin, "Cyber Attack Detection Model (CADM) Based on Machine Learning Approach," 2021 2nd International Conference on Robotics, Electrical and Signal Processing Techniques (ICREST), DHAKA, Bangladesh, 2021, pp. 567-572, doi: 10.1109/ICREST51555.2021.9331094.

[2] K. Shaukat, S. Luo, S. Chen and D. Liu, "Cyber Threat Detection Using Machine Learning Techniques: A Performance Evaluation Perspective," 2020 International Conference on Cyber Warfare and Security (ICCWS), Islamabad, Pakistan, 2020, pp. 1-6, doi: 10.1109/ICCWS48432.2020.9292388.

[3] S. K. L. Naik and M. Arshad, "Detection of Cyberattack in Network Using Machine Learning," 2022 International Conference on Advancements in Smart, Secure and Intelligent Computing (ASSIC), Bhubaneswar, India, 2022, pp. 1-6, doi: 10.1109/ASSIC55218.2022.10088380.

[4] R. R. Dornala, "An Advanced Multi-Model Cloud Services using Load Balancing Algorithms," 2023 5th International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 2023, pp. 1065-1071, doi: 10.1109/ICIRCA57980.2023.10220892.

[5] R. R. Dornala, S. Ponnapalli, A. R. Lakshmi and K. T. Sai, "An Advanced Cloud Security and Load Balancing in Health Care Systems," 2023 International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS), Erode, India, 2023, pp. 1-6, doi: 10.1109/ICSSAS57918.2023.10331892.

[6] R. R. Dornala, "An Advanced Multi-Model Cloud Services using Load Balancing Algorithms," 2023 5th International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 2023, pp. 1065-1071, doi: 10.1109/ICIRCA57980.2023.10220892.

[7] S. Ponnapalli, R. R. Dornala, K. Thriveni Sai and S. Bhukya, "A Secure and Smooth Data Delivery Platform with Block chain in Cloud Computing," 2024 5th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI), Lalitpur, Nepal, 2024, pp. 590-596, doi: 10.1109/ICMCSI61536.2024.00093.

[8] S. Ponnapalli, R. R. Dornala and K. T. Sai, "A Hybrid Learning Model for Detecting Attacks in Cloud Computing," 2024 3rd International Conference on Sentiment Analysis and Deep Learning (ICSADL), Bhimdatta, Nepal, 2024, pp. 318-324, doi: 10.1109/ICSADL61749.2024.00058.

[9] T. Bilot, N. E. Madhoun, K. A. Agha and A. Zouaoui, "Graph Neural Networks for Intrusion Detection: A Survey," in IEEE Access, vol. 11, pp. 49114-49139, 2023, doi: 10.1109/ACCESS.2023.3275789.

[10] U. Sabeel, S. S. Heydari, K. El-Khatib and K. Elgazzar, "Unknown, Atypical and Polymorphic Network Intrusion Detection: A Systematic Survey," in IEEE Transactions on Network and Service Management, vol. 21, no. 1, pp. 1190-1212, Feb. 2024, doi: 10.1109/TNSM.2023.3298533.

[11] S. Tan, J. M. Guerrero, P. Xie, R. Han and J. C. Vasquez, "Brief Survey on Attack Detection Methods for Cyber-Physical Systems," in IEEE Systems Journal, vol. 14, no. 4, pp. 5329-5339, Dec. 2020, doi: 10.1109/JSYST.2020.2991258.

[12] M. Husak, J. Komarková, E. Bou-Harb and P. Čeleda, "Survey of Attack Projection, Prediction, and Forecasting in Cyber Security," in IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 640-660, Firstquarter 2019, doi: 10.1109/COMST.2018.2871866.

[13] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac and P. Faruki, "Network Intrusion Detection for IoT Security Based on Learning Techniques," in IEEE Communications Surveys & Tutorials, vol. 21, no. 3, pp. 2671-2701, thirdquarter 2019, doi: 10.1109/COMST.2019.2896380.

[14] M. Alazab, S. P. RM, P. M, P. K. R. Maddikunta, T. R. Gadekallu and Q. -V. Pham, "Federated Learning for Cybersecurity: Concepts, Challenges, and Future Directions," in IEEE Transactions on Industrial Informatics, vol. 18, no. 5, pp. 3501-3509, May 2022, doi: 10.1109/TII.2021.3119038.

[15] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed and M. Xu, "A Survey on Machine Learning Techniques for Cyber Security in the Last Decade," in IEEE Access, vol. 8, pp. 222310-222354, 2020, doi: 10.1109/ACCESS.2020.3041951.