WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

An Analysis Cyber Threat Detection Using Machine Learning

Jogula Sharat Kumar

B. Tech Student, Department of IT, GMR Institute of Technology, Rajam-532127, Andhra Pradesh, India
Email: 21341A1253@gmrit.edu.in

ABSTRACT

A cyber threat denotes a possible occurrence or instance involving the unauthorized entry, harm, disturbance, of data using computer systems and networks, often carried out with malicious intent. Cyber threats pose numerous drawbacks and negative consequences for individuals, organizations, and society as a whole. Mitigating cyber threats on online platforms requires a comprehensive approach that combines technology, processes, and user education where as to provide a strong authentication system, regular software updates, phishing prevention, data encryption, and various types of security assessments. But still there is a chance for getting various challenges due to lack of intellectual knowledge at our user side. So, we need to provide an intellectual and statistical mechanism such as Machine Learning (ML) and Deep Learning (DL) models for identifying cyber threats effectively. In this work I am going to analyse various algorithms like support vector machine (SVM), K-Nearest neighbour (KNN), Decision Tree (DT) algorithms, along with various neural network concepts. After analysing we need to declare which algorithm/model is working effectively for identifying cyber threat detection this analysis is mainly helpful for getting knowledge in terms of various parameters like accuracy in identification of attack, how much efficiency in detection of unauthorized activity and so on.

Keywords: *Machine Learning (ML) and Deep Learning (DL), Cyber threat, Security*

INTRODUCTION

In our increasingly digital world, cyber threats pose a persistent and evolving danger. These threats range from unauthorized data access to deliberate disruption of computer systems and networks, often driven by malicious intent. Their consequences ripple across individuals, organizations, and society at large. To effectively combat these threats on online platforms, a holistic strategy is essential, encompassing advanced technology, robust processes, and user education. This includes measures like strong authentication, software updates, phishing prevention, data encryption, and security assessments. However, the dynamic nature of cyber threats and potential user unawareness present ongoing challenges. This research delves into the vital role of Machine Learning (ML) and Deep Learning (DL) models, evaluating algorithms such as SVM, KNN, and DT, and cutting-edge neural networks. The aim is to identify the most effective approach for cyber threat detection, considering parameters like accuracy and efficiency. This analysis contributes to a deeper understanding of cyber threat detection in the digital age.

RESEARCH APPROACH

The paper presents techniques based on machine learning for analyzing cybersecurity threats in cloud environments, specifically in the fields of telecommunications and IoT the proposed techniques include Support Vector Machines, Neural networks, and Deep Neural Networks, which are combined for analyzing monitoring data.

The paper also proposes an approach for combining classifier results based on performance weights the achieved results of the proposed approach are comparable to existing algorithms and suitable for enterprise-grade security applications.

The paper mentions the use of Deep Neural networks for analyzing cybersecurity threats in cloud applications, with 4 neural classifiers for network traffic, spam comments, spam email, and imagesthe achieved accuracy for the individual components is comparable to contemporary works.

The authors aim to build a comprehensive framework for cybersecurity threat detection in the cloud in the future the paper also mentions the use of a CNN trained in the Weka tool for content analysis in terms of spam detection, achieving an accuracy of about 70% in two classes.

METHODOLOGY:

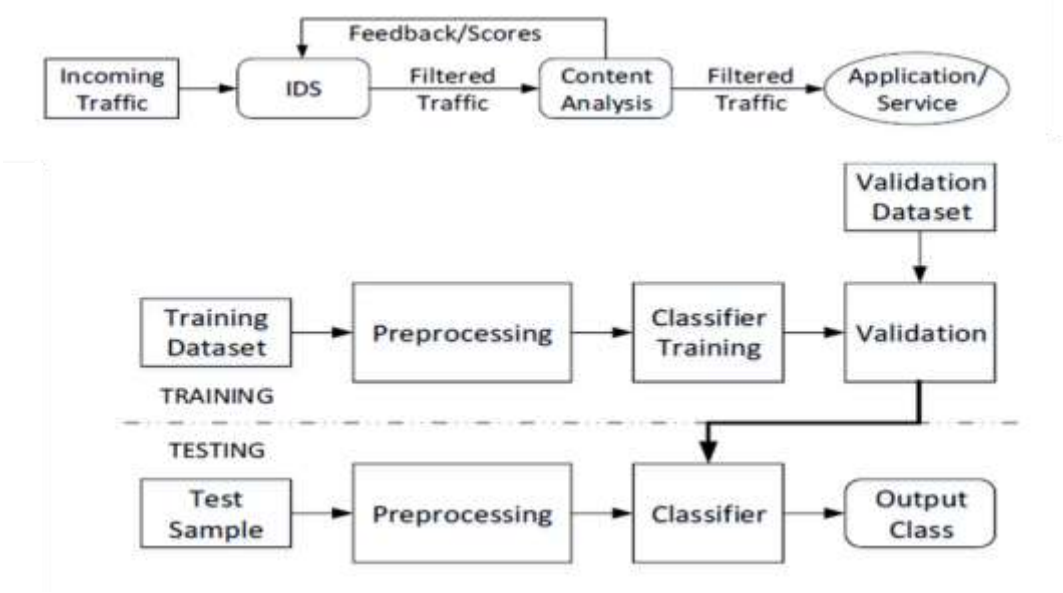

Figure 1 : Block diagram threat detection

- Figure The incoming traffic is analyzed in an IDS (intrusion detection system) and threats are blocked based on rules, anomaly detection and correlation analysis
- The IDS filtered traffic is then subjected to content analysis where the traffic is decoded in a proxy server and the incoming text, video and images are analyzed with deep neural network classifiers

Training dataset: A training dataset is a subset of data used to train machine learning models. It consists of input-output pairs, where the model learns patterns and relationships between inputs and corresponding outputs.

Preprocessing: Preprocessing is the preliminary step in data analysis or machine learning, involving the transformation and cleaning of raw data The goal is to enhance data quality, making it suitable for analysis and improving the performance of machine learning models.

Classifier training: Classifier training involves feeding a machine learning algorithm with labeled data to learn patterns and relationships. The algorithm adjusts its parameters through iterative optimization, aiming to accurately classify new, unseen data. This process requires a training dataset, a suitable algorithm, and evaluation to ensure the classifier's effectiveness

Validation of dataset : Data validation involves inspecting and cleaning a dataset to ensure accuracy, reliability, and suitability for analysis. This process includes checking for missing values, outliers, and inconsistencies. Techniques such as imputation, normalization, and cross-validation may be employed.

Classifier: A classifier is a machine learning algorithm trained on labeled data to categorize or predict new, unseen instances into predefined classes or categories. It learns patterns and relationships in the training data to make accurate predictions, making it a fundamental tool in tasks like image recognition, spam filtering, and sentiment analysis

RESULTS

Test/Analysis	**Accuracy (%)**
Suricata IDS Ruleset Testing	85%
Neural Classifier (Weka) - Inputs: 115, Hidden Layers: 4 - Output Neurons: 11 - Dataset: [23] (10 types, 249 attrs)	83%
Content Analysis - Spam Detection (CNN) - Model Trained in Weka - Dataset: [32]	70%
Image Classification - Based on Human Emotion Analysis - 5 Classes	73%

CONCLUSION

This paper introduces a clever method using advanced computer systems called Deep Neural Networks to tackle cybersecurity threats in cloud applications. Our system involves four specialized detectors for different tasks: one for monitoring network traffic, another for identifying spam comments, a third for flagging potentially harmful emails, and a fourth for scanning images for hidden dangers. The outcomes we achieved are on par with other modern methods, showing that our system is just as accurate. Looking ahead, our future plan is to expand our efforts by creating a complete system that can handle all sorts of cybersecurity threats in the cloud. Our aim is to make the online world safer for everyone by building a comprehensive framework for detecting and preventing threats.

References

[1] "Sokolov, S. A., Iliev, T. B., & Stoyanov, I. S. (2019, May). Analysis of cybersecurity threats in cloud applications using deep learning techniques. In *2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (pp. 441-446). IEEE.

[2] Bécue, A., Praça, I., & Gama, J. (2021). Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. *Artificial Intelligence*

[3] Ahsan, M., Nygard, K. E., Gomes, R., Chowdhury, M. M., Rifat, N., & Connolly, J. F. (2022). Cybersecurity threats and their mitigation approaches using Machine Learning—A Review. *Journal of Cybersecurity and Privacy*, *2*(3), 527-555.

[4] Farooq, H. M., & Otaibi, N. M. (2018, March). Optimal machine learning algorithms for cyber threat detection. In *2018 UKSim-AMSS 20th International Conference on Computer Modelling and Simulation (UKSim)* (pp. 32-37). IEEE.

[5] Al-Taleb, N., & Saqib, N. A. (2022). Towards a hybrid machine learning model for intelligent cyber threat identification in smart city environments. *Applied Sciences*, *12*(4), 1863.

[6] Shaukat, K., Luo, S., Chen, S., & Liu, D. (2020, October). Cyber threat detection using machine learning techniques: A performance evaluation perspective. In 2020 international conference on cyber warfare and security (ICCWS) (pp. 1-6). IEEE.

[7] Lee, J., Kim, J., Kim, I., & Han, K. (2019). Cyber threat detection based on artificial neural networks using event profiles. Ieee Access, 7, 165607-165626..

[8] Zhang, J., Pan, L., Han, Q. L., Chen, C., Wen, S., & Xiang, Y. (2021). Deep learning based attack detection for cyber-physical system cybersecurity: A survey. IEEE/CAA Journal of Automatica Sinica, 9(3), 377-391.

[9] Kumar, S., Singh, B. P., & Kumar, V. (2021, December). A Semantic Machine Learning Algorithm for Cyber Threat Detection and Monitoring Security. In 2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N) (pp. 1963-1967). IEEE.

[10] Buczak, A. L., & Guven, E. (2015). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications surveys & tutorials, 18(2), 1153-176.

[11] Sentuna, A., Alsadoon, A., Prasad, P. W. C., Saadeh, M., & Alsadoon, O. H. (2021). A novel Enhanced Naïve Bayes Posterior Probability (ENBPP) using machine learning: Cyber threat analysis. Neural Processing Letters, 53, 177-209.

[12] Sarker, I. H. (2021). CyberLearning: Effectiveness analysis of machine learning security modeling to detect cyber-anomalies and multi-attacks. Internet of Things, 14, 100393.

[13] Nassar, A., & Kamal, M. (2021). Machine Learning and Big Data Analytics for Cybersecurity Threat Detection: A Holistic Review of Techniques and Case Studies. Journal of Artificial Intelligence and Machine Learning in Management, 5(1), 51-63.

[14] Bouchama, F., & Kamal, M. (2021). Enhancing Cyber Threat Detection through Machine Learning-Based Behavioral Modeling of Network Traffic Patterns. International Journal of Business Intelligence and Big Data Analytics, 4(9), 1-9.

[15] Akhtar, M. S., & Feng, T. (2022). Malware Analysis and Detection Using Machine Learning Algorithms. Symmetry, 14(11), 2304.

[16] K. Mohammed, A. H., Jebamikyous, H., Nawara, D., & Kashef, R. (2021, April). Iot cyber-attack detection: A comparative analysis. In International Conference on Data Science, E-learning and Information Systems 2021 (pp. 117-123).

[17] Rupa, C., Srivastava, G., Bhattacharya, S., Reddy, P., & Gadekallu, T. R. (2021, August). A machine learning driven threat intelligence system for malicious URL detection. In Proceedings of the 16th International Conference on Availability, Reliability and Security (pp. 1-7).

[18] Strecker, S., Van Haaften, W., & Dave, R. (2021). An analysis of IoT cyber security driven by machine learning. In Proceedings of International Conference on Communication and Computational Technologies: ICCCT 2021 (pp. 725-753). Springer Singapore.

[19] Ahsan, M., Nygard, K. E., Gomes, R., Chowdhury, M. M., Rifat, N., & Connolly, J. F. (2022). Cybersecurity threats and their mitigation approaches using Machine Learning—A Review. Journal of Cybersecurity and Privacy, 2(3), 527-555..

[20] Rachmawati, A. (2022). Analysis of Machine Learning Systems for Cyber Physical Systems. International Transactions on Education Technology, 1(1), 1-9.