As per UGC guidelines *an electronic bar code is provided to seure your paper*

International Journal for Modern Trends in Science and Technology
Volume 10, Issue 04, pages 338-342.
ISSN: 2455-3778 online
Available online at: http://www.ijmtst.com/vol10issue04.html
DOI: https://doi.org/10.46501/IJMTST1004051

Enhancing Cybersecurity: A Model for Threat Detection Utilizing Artificial Intelligence Technology

K.Sham Sri[1] , Sri Harsutan Gollapalli[2], Lakkavarapu Hemanth[2], Jyothula Ramya[2], Pulugu Vandana[2], Balusu Vamsi Krishna[2]

[1]Assistant Professor, Department of Computer Science Engineering, Pragati Engineering College, Surampalem , Andhra Pradesh, India.
[2]Department of Computer Science Engineering, Pragati Engineering College, Surampalem , Andhra Pradesh, India.

To Cite this Article
K.Sham Sri , Sri Harsutan Gollapalli, Lakkavarapu Hemanth, Jyothula Ramya, Pulugu Vandana, Balusu Vamsi Krishna, Enhancing Cybersecurity: A Model for Threat Detection Utilizing Artificial Intelligence Technology, International Journal for Modern Trends in Science and Technology, 2024, 10(04), pages. 338-342. https://doi.org/10.46501/IJMTST1004051

Article Info
Received: 06 April 2024; Accepted: 18 April 2024; Published: 26 April 2024.

ABSTRACT

The proliferation of computer-related applications, as well as the alarming increase in computer connections in recent years, have made cyber-security increasingly difficult to manage. Strong definitions are also required for the system to withstand the growing amount of cyberattacks. As a result, the creation of intrusion detection systems (IDS) to detect threats and anomalies in computer networks might be a possible application for cyber security. AI, particularly Machine Learning methods, were employed to build a successful data-driven intrusion detection system. This work proposes a novel security model cantered on the Binary a grasshopper Optimal Twin Support Vector Model (BGOTSVM), which rates security aspects according to relevance before developing an IDS modelling based on the relevant characteristics that have been picked. By reducing feature size, this technique increases prediction accuracy for unrecognized tests while lowering the model's computing cost. To compare the results with existing methodologies, four popular predictive modelling approaches—Decision Tree, Random Decision Forest, Random Tree, and Artificial Neural Network—are used. The study's experimental results show that the proposed methodologies might be used as learning-based models to outperform existing machine learning methodologies for network breaches detection.

Keywords: Cyber security, cyber security threats, intrusion detection, Binary Grasshopper Optimized Twin SVM (BGOTSVM).

1. INTRODUCTION

Several new uses for computer and network technology have emerged in recent years, such as utilizing private data, public data, or commercial data. To stop system infiltration, cyber security has grown increasingly crucial. In the past, configuring a security policy on a firewall may not have provided adequate defence against such incursions due to the development of new types of invasions that make advantage of operating system flaws and message passing parameters, among other things. But, by employing the Intrusion Detection System (IDS), it can both identify the issue and stop the incursion [1]. Cyber security has substantially improved in answer to the expanding range of cyber threats to prevent cybercrime and it’s the term for a group of technologies, technical professionals, and procedures used to create security safeguards that keep cyberspace secure from cybercriminals.

There are two primary methods of cyber security: automated cyber security and conventional cyber security. Many drawbacks of traditional cyber security, such as untrained individuals, inadequate system resource design, and restricted access to clean data, exacerbate cybercrimes [2]. The development of AI techniques has led to improvements in learning-based methods for spotting cyberattacks, and several studies have shown that they provide meaningful outcomes. To safeguard IT systems against threats and suspicious network activity, however, is still very difficult due to cyberattacks' continual evolution. Effective defences and security concerns were given significant emphasis for creating trustworthy alternatives because of numerous network invasions and serious harm [3]. Along with this expansion, cyber criminals persisted in and broadened their fraudulent transactions, taking advantage of fresh security flaws and evading security measures to gain entry (hacking) to secret communication networks and inflict harm ranging from service interruption to the electronic theft of confidential or sensitive data or financial assets. The exponentially growing rate noted in the web ecosystem is mirrored by the growth rate of cyber-attacks, particularly those classified as AI assisted hacking, and has only recently begun to present a new challenge to the overburdened online security procedures, including many that require costly human analysis [4]. The study is organized such that section II offers

relevant work, section III describes the suggested strategy, section IV shows the results and discussion, and section V

concludes with recommendations for future research.

2. LITERATURE SURVEY

The study [5-6] discussed current Deep Learning (DL) techniques, conventional Machine Learning (ML) techniques, and ongoing research on using AI to prevent cybercrime. Lastly, evaluate the counterattacks that AI itself could face, identify the relevant defensive tactics, and study their characteristics. Unlike the natural intelligence that humans possess or the sort of intelligence that can be created in machines that operate and act like people, AI is the form of intellect that robots can display [7]. AI, also known as ML, is essentially the term used when a computer acts like a person while doing tasks like problem-solving or.

learning. The article [8] presented the AI methods may be used to cybersecurity and highlight a few of the intelligent based strategies that are currently in use. In addition, the shortcomings of AI-based cybersecurity techniques were emphasised and potential future research options were provided. A system that detects intrusions using data may be constructed using AI, especially ML methods. The article [9] discussed the security approach that uses an intrusion

detection tree and ML. Based on the fundamental characteristics that have been selected after ranking the security features in order of importance, this model provides a tree-based generic intrusion detection model. The research [10] suggested a new hybrid ML-based cyber network security framework for multiple cyber intrusion detection. Moreover, the correlation-based feature selection is utilised to exclude the irrelevant features, and the weight factor of adaptive boosting, which is used to combine several classifiers, is highlighted. The research [11] conducted a literature review on the use of AI in network situation awareness, monitoring of harmful behaviour, and detection of aberrant traffic. A hypothetical human-in-the-loop intelligence cyber security model is offered according to the findings, which also identify a number of limits and concerns. Also, these data sets underwent limit standardization, and classification was carried out using the traditional ML techniques of support vector machines, KNearest Neighbour, and decision trees [12]. The study [13] proposed AI methods may be used to cybersecurity and highlight a few of the intelligent-based strategies that are currently in use.

3. SYSTEM ANALYSIS

A. EXISTING SYSTEM

The existing system for your project, "Cyber Security Threat Detection Model using Artificial Intelligence Technology," leverages Machine Learning techniques, particularly the Binary Grasshopper Optimized Twin Support Vector Machine (BGOTSVM) model. This system is designed to address the escalating challenge of cybersecurity by detecting inconsistencies and threats within computer networks. It begins with the collection and preprocessing of network data, followed by feature ranking to prioritize relevant security features. The IDS model is then developed based on the selected significant features, reducing feature dimensions and computational costs. Comparative experiments are conducted against traditional Machine Learning approaches like Decision Tree, Random Decision Forest, Random Tree, and Artificial Neural Network. The system's experimental results demonstrate its superiority in network intrusion detection and its potential for real-world cybersecurity applications.

DISADVANTAGES OF THE EXISTING SYSTEM

Limited Scalability: The system may face challenges in scaling to handle large and complex network environments, making it less suitable for organizations with extensive and diverse network infrastructures.

Dependency on Feature Selection: The effectiveness of the system relies heavily on the initial feature selection process, which may not always guarantee optimal feature relevance, leading to potential false positives or negatives.

Lack of Real-Time Detection: Real-time detection is essential for promptly responding to cyber threats, and the existing system's ability to provide real-time monitoring and immediate alerts may be limited.

> Interpretability: Complex Machine Learning models like BGOTSVM can be difficult to interpret, which may hinder the system's transparency and the ability to explain its decisions to cybersecurity professionals.

Continuous Adaptation: The cybersecurity landscape is dynamic, with evolving threats. The existing system may not have built-in mechanisms for continuous adaptation and updating of threat detection algorithms, potentially leaving it vulnerable to emerging threats.

B. PROPOSED SYSTEM

The proposed system for the project, "Cyber Security Threat Detection Model using Artificial Intelligence Technology," aims to address the limitations of the existing system. It seeks to enhance scalability by incorporating distributed computing and cloud-based solutions, making it suitable for large and complex network environments. The proposed system will focus on automating the feature selection process using advanced feature engineering techniques, reducing the reliance on manual feature selection. It will also implement real-time detection capabilities for immediate threat response. To improve interpretability, the system will incorporate explainable AI techniques, making its decisions more understandable for cybersecurity professionals. Additionally, the proposed system will emphasize adaptability and continuous learning, integrating threat intelligence feeds and ensuring timely updates to stay ahead of evolving cyber threats.

ADVANTAGES OF THE PROPOSED SYSTEM

Enhanced Scalability: The system can efficiently scale to handle large and complex network environments, making it suitable for organizations with extensive and diverse network infrastructures.

Automated Feature Selection: By automating the feature selection process, the system reduces the risk of human error and ensures that the most relevant security features are consistently chosen.

Real-Time Detection: The system provides real-time monitoring and immediate threat detection, enabling organizations to respond swiftly to cyber threats, minimizing potential damage.

Improved Interpretability: Incorporating explainable AI techniques enhances the transparency of the system, making it easier for cybersecurity professionals to understand and trust its decisions.

Continuous Adaptation: The system's focus on adaptability and continuous learning ensures it remains up to date with evolving cyber threats, offering robust protection against emerging security challenges.

4. SYSTEM DESIGN

SYSTEM ARCHITECTURE

Below diagram depicts the whole system architecture.

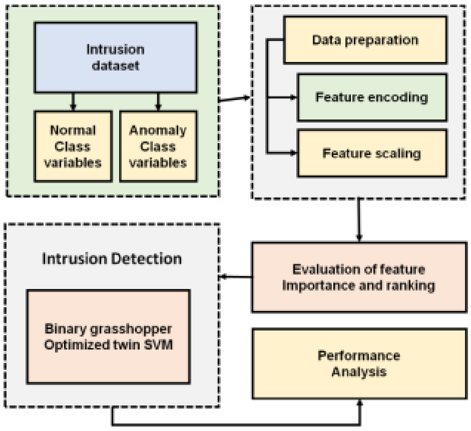


Fig 1. Methodology followed for proposed model

5. SYSTEM IMPLEMENTATION MODULES

The modules for the "Cyber Security Threat Detection Model using Artificial Intelligence Technology" project can be outlined as follows:

1. **Data Collection and Preprocessing**:
   - Collect and preprocess network data, logs, and activity parameters for analysis, ensuring data quality and consistency.
2. **Feature Engineering and Selection**:
   - Implement advanced feature engineering techniques to extract relevant security features and automate feature selection processes to prioritize critical attributes.
3. **Model Development**:
   - Develop the core Intrusion Detection System (IDS) using the Binary Grasshopper Optimized Twin Support Vector Machine (BGOTSVM) model, optimizing the chosen algorithm for enhanced accuracy.
4. **Real-Time Monitoring and Alerting**:
   - Integrate real-time monitoring capabilities to continuously analyze network data and trigger immediate alerts upon detecting suspicious or malicious activities.
5. **Explainability and Adaptation**:
   - Incorporate explainable AI techniques for improved model interpretability and implement mechanisms for continuous adaptation, integrating threat intelligence feeds and timely updates to stay current with evolving cyber threats.

6. RESULTS AND DISCUSSION

The efficacy of ML classification methods for detecting attacks is shown in the section. In this IDS model, a number of well-known classification methods, such as the tree-based model, and artificial neural networks are investigated. Particularly, in order to assess the intrusion detection model, the efficacy of a number of widely used classification algorithms, including Decision Tree (DT), Random Forest (RF), Random Tree (RT), and Artificial Neural Network (ANN) are examined. Calculations of precision, recall, fscore, and accuracy are used to assess the potential of different models. By performing tests on cyber security datasets with various types of assaults, the performance metrics for intrusion detection are discussed.

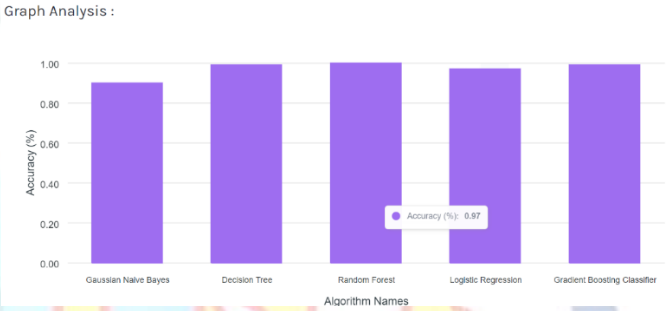


Fig 2. Algorithms Accuracy Comparison

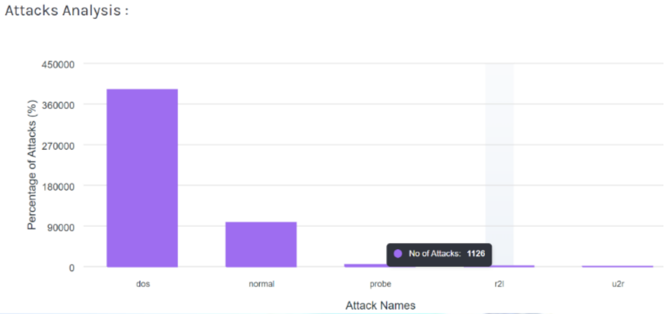
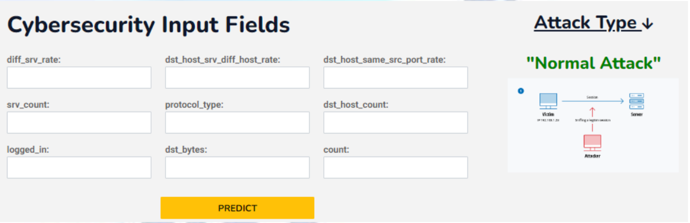


Fig 3. **Cyber Attacks Analysis**



Cybersecurity Input Fields

diff_srv_rate:

dst_host_srv_diff_host_rate:

dst_host_same_src_port_rate:

srv_count:

protocol_type:

dst_host_count:

logged_in:

dst_bytes:

count:

Attack Type ↓

"Normal Attack"

Fig 4. **Cyber Attacks Detection**

7. CONCLUSION

Security issues have caused application developers, e-commerce specialists, and IT professionals to be increasingly concerned about the practicality and potential of machine learning-based intrusion detection models. A cyber-security data collection frequently includes many types of cyberattacks with important features. As a result, certain classifiers with several attack kinds and parameters may not reach ideal accuracy and true prediction rate. The performance of the BGOTSVM model was discussed in this paper. The performance metrics recall, f1-score, and total accuracy were also examined. The goal is to develop a data-driven intrusion detection system and expand cyber-security datasets so that automated security services may be provided to the cyber-security community in the future.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] P. Sornsuwit,and S. Jaiyen, “A new hybrid machine learning for cybersecurity threat detection based on adaptive boosting,”Applied Artificial Intelligence, 33(5), pp.462-482, 2019.

[2] K.Shaukat, S. Luo, S.Chen, and D. Liu, “Cyber threat detection using machine learning techniques: A performance evaluation perspective,”inIEEE international conference on cyber warfare and security. IEEE, October2020,pp. 1-6.

[3] Q.H. Vu, D.Ruta, and L.Cen, “Gradient boosting decision trees for cyber security threats detection based on network events logs,” in 2019IEEE International Conference on Big Data (Big Data). IEEE, December2019, pp. 5921-5928.

[4] J. Lee, J. Kim, I.Kim, and K. Han,“Cyber threat detection based on artificial neural networks using event profiles,”IEEE Access, vol. 7, pp.165607-165626, 2019.

[5] J.H. Li, “Cyber security meets artificial intelligence: a survey;” Frontiers of Information Technology & Electronic Engineering, vol. 19,no.12, pp.1462-1474, 2018.

[6] N.Rawindaran, A.Jayal, E.Prakash, and C.Hewage, “Cost benefits of using machine learning features in NIDS for cyber security in UK small medium enterprises (SME),” Future Internet, vol. 13, no. 8, p.186, 2021.

[7] R.Prasad, V.Rohokale, R.Prasad, and V.Rohokale, “Artificial intelligence and machine learning in cyber security,” Cyber security: the lifeline of information and communication technology, pp.231-247, 2020.

[8] T.C.Truong, I.Zelinka, J.Plucar,M.Čandík, and V.Šulc,“Artificial intelligence and cybersecurity: Past, presence, and future,” In Artificial intelligence and evolutionary computations in engineering systems, pp. 351-363, Springer Singapore, 2020.

[9] I.H.Sarker, Y.B.Abushark, F.Alsolami, and A.I. Khan,“Intrudtree: a machine learning based cyber security intrusion detection model,” Symmetry, vol. 12, no. 5, p.754, 2020.

[10] Diro, and N.Chilamkurti, “Distributed attack detection scheme using deep learning approach for Internet of Things,” Future Generation Computer Systems, vol. 82, pp.761-768, 2018.

[11] Z.Zhang, H.Ning, F.Shi, F.Farha, Y.Xu, F.Zhang, and K.K.R. Choo,“Artificial intelligence in cyber security: research advances, challenges, and opportunities,” Artificial Intelligence Review, pp.1-25, 2022.

[12] I.F.Kilincer, F.Ertam, and A.Sengur, “Machine learning methods for cyber security intrusion detection: Datasets and comparative study,” Computer Networks, vol. 188, p.107840, 2021.

[13] Ramkumar, M. S., Emayavaramban, G., Amudha, A., Nagaveni, P., Divyapriya, S., & SivaramKrishnan, M. (2021, October). A Hybrid AI Based and IoT Model Generation of Nonconventional Resource of Energy. In 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC) (pp. 1-6). IEEE.

[14] Network Intrusion Detection. Available online: https://www.kaggle.com/ (accessed on 12 March 2020).

[15] H. Alqahtani, I.H. Sarker, A. Kalim, S.M. Minhaz Hossain, S. Ikhlaq, and S. Hossain, 2020. “Cyber intrusion detection using machine learning classification techniques”, In Computing Science, Communication and Security: First International Conference, COMS2 2020, Gujarat, India, March 26–27, 2020, Revised Selected Papers 1 (pp. 121-131). Springer Singapore.

[16] Kumar, A. Senthil, and EaswaranIyer. "An industrial iot in engineering and manufacturing industries—benefits and challenges." International journal of mechanical and production engineering research and dvelopment (IJMPERD) 9.2 (2019): 151-160