International Journal of

DATA SCIENCE AND IOT MANAGEMENT SYSTEM

Peer Reviewed, Referred & Indexed Journal

ISSN: 3068-272X ww.ijdim.com Original Research Paper

Cyber Security Threat Detection Framework Using Artificial Intelligence Techniques

Mr. K Subrahmanyam[1], Kokkiligadda Sai Vamsi[2], Marpu Nikith Babu[3], Palaparthi Pulla Rao[4], Gundapu Rupesh Kumar[5], Bandi Asrith Nath[6]

[1]Assistant Professor, St. Ann's College of Engineering & Technology, Chirala, Andhra Pradesh – 523157

[2-6]UG Student, St. Ann's College of Engineering & Technology, Chirala, Andhra Pradesh - 523157

ABSTRACT: The difficulty of ensuring cyber-security is steadily growing as a result of the alarming development in computer connectivity and the sizeable number of applications associated to computers in recent years. The system also requires robust defines against the growing number of cyber threats. As a result, a possible role for cyber-security might be performed by developing Intrusion Detection Systems (IDS) to detect inconsistencies and threats in computer networks. An effective data-driven intrusion detection system has been created with the use of Artificial Intelligence, particularly Machine Learning techniques. This research proposes a novel Voting Classifier based security model which first considers the security features ranking according to their relevance before developing an IDS model based on the significant features that have been selected. By lowering the feature dimensions, this approach not only improves predictive performance for unidentified tests but also lowers the model's computational expense. The machine learning techniques used to compare the results to the current approaches were Decision Tree, Random Decision Forest, Random Tree. The experimental findings of this study confirm that the suggested methods may be used as learning-based models for network intrusion detection and demonstrate that, when used in the real world, they outperform conventional machine learning techniques.

Key words: *Cyber-Security, Intrusion Detection System, Machine Learning, Voting Classifier, Feature Selection.*

1. INTRODUCTION

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X ww.ijdim.com Original Research Paper

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 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].

2. LITERATURE SURVEY

The study [5-6] discussed current Deep Learning (DL) techniques, conventional cyber threats to prevent cybercrime and it’s

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X ww.ijdim.com Original Research Paper

the term for a group of technologies, technical professionals, and procedures used to create security safeguards that keep cyberspace secure from cybercriminals. 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 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 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, K Nearest Neighbour, and decision trees .

3 SYSTEM ARCHITECTURE

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X ww.ijdim.com Original Research Paper

The system architecture illustrates an AI-powered intrusion detection system. Network data undergoes feature ranking, selection, and processing through decision trees and random forests. Significant features are passed to a machine learning IDS using Decision Tree, Random Tree, and Voting Classifier. Anomalies trigger security alerts, ensuring robust detection of cyber threats.

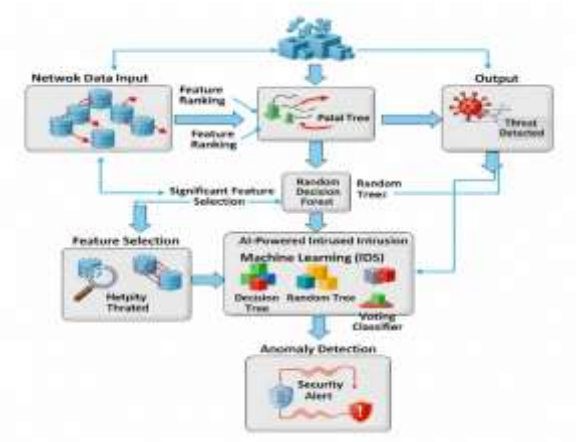


Fig1: **System Architecture**

3.1 METHODOLOGY

The proposed cyber-security threat detection framework is developed using machine learning techniques on the KDD Cup 1999 intrusion detection dataset. The methodology follows six systematic steps:

3.2 Dataset Preparation The dataset includes 41 features representing network traffic behavior. Attack labels are mapped into five categories: Normal, DoS, Probe, R2L, and U2R. Preprocessing involves encoding categorical attributes (protocol type, service, flag) into numerical values and reducing multi-class labels for generalization.

3.3 Feature Selection and Ranking Security features are ranked according to relevance. Irrelevant or redundant attributes are excluded to reduce dimensionality, improving computational efficiency and predictive accuracy.

3.4 Baseline Model – Multinomial Naive Bayes (MNB) MNB is implemented as a reference model. It assumes conditional independence among features and estimates posterior probabilities for each attack category.

Equation (Bayes' Theorem):

$$P(C \mid X) = \frac{P(X \mid C) \cdot P(C)}{P(X)}$$

where $P(C \mid X)$is the posterior probability of class Cgiven features X.

3.5 Proposed Model – Decision Tree + Linear SVC Voting A hybrid ensemble integrates Decision Tree and Linear Support Vector Classifier (SVC). The Decision Tree captures non-linear feature interactions,

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X ww.ijdim.com Original Research Paper

while Linear SVC maximizes separation in high-dimensional space. Predictions are combined using a voting mechanism.

Equation (Entropy for Decision Tree Splitting):

$$H(S) = -\sum_{i=1}^{n} p_i \log_2 p_i$$

where $p_i$is the proportion of samples belonging to class i.

Equation (SVC Optimization):

$$\min_{w,b} \frac{1}{2} \| w \|^2 \text{ subject to } y_i(w \cdot x_i + b) \geq 1$$

ensuring maximum margin separation between classes.

3.6 Performance Evaluation Models are evaluated using accuracy, precision, recall, and F1-score. Special emphasis is placed on minority attack classes (R2L, U2R).

4. DESIGN AND CONSTRUCTION

The design of the proposed cyber-security threat detection system is centered on building a robust intrusion detection framework using machine learning. The system architecture begins with the KDD Cup 1999 dataset, which provides a comprehensive representation of network traffic through 41 features. These features are categorized into basic, content-based, time-based, and host-based attributes, ensuring that the system captures both short-term and long-term attack behaviors.

Preprocessing plays a crucial role in the construction phase. Categorical attributes such as protocol type, service, and flag are encoded into numerical values to make them suitable for machine learning algorithms. Attack labels are consolidated into five major categories—Normal, DoS, Probe, R2L, and U2R—reducing complexity and improving generalization. Data cleaning ensures consistency, while train-test splitting provides reliable evaluation of model performance.

The baseline model is constructed using the Multinomial Naive Bayes classifier. This probabilistic model serves as a reference point, offering fast training and low computational cost. However, its limitations in handling correlated features and imbalanced classes highlight the need for a more advanced approach.

The proposed system integrates a Decision Tree classifier with a Linear Support Vector Classifier (SVC) through a voting mechanism. The Decision Tree captures non-linear feature interactions and provides

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X ww.ijdim.com Original Research Paper

interpretability, while Linear SVC ensures robust separation in high-dimensional data. The voting mechanism combines their predictions, reducing bias and improving detection accuracy, particularly for minority attack categories such as R2L and U2R.

For deployment, the trained models are embedded into a Flask-based web interface. This interface allows real-time preprocessing of incoming network packets, classification into attack categories, and generation of alerts when anomalies are detected. Predictions are returned in JSON format, making the system lightweight and adaptable for integration into enterprise or government networks.

5 RESULTS AND DISCUSSION

The experimental evaluation was conducted using the KDD Cup 1999 dataset, which contains diverse attack categories mapped into five major classes: Normal, DoS, Probe, R2L, and U2R. The baseline Multinomial Naive Bayes classifier demonstrated reasonable performance for majority classes such as Normal and DoS but struggled significantly with minority classes like R2L and U2R due to its independence assumption and sensitivity to class imbalance.



Fig 2: AI-Based Cyber Threat Detection Interface

The interface demonstrates an AI-powered cyber threat detection system capable of analyzing datasets, labeled and unlabeled data, and performing DDoS analysis. It allows manual data input and graphical visualization of suspicious activity, including malicious URLs. This design highlights the system's adaptability in identifying threats and providing real-time security insights.



Fig 3: Cyber Threat Detection Data Interface

The interface illustrates an AI-driven cyber threat detection system that analyzes datasets and suspicious URLs. It provides

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

options for dataset analysis, manual data entry, labeled and unlabeled data handling, DDoS analysis, and graphical visualization. The displayed URLs represent potential threats, showcasing the system's capability to identify malicious links and enhance network security.



Fig 4: AI-Driven DDoS Threat Detection Interface

The interface illustrates malware detection and network traffic analysis alongside a diagram of a DDoS attack. It identifies threats such as TCP-based and Ping of Death attacks, mapping their positions in traffic. The DDoS visualization shows attacker commands directing zombie PCs to overwhelm a victim website, highlighting AI's role in proactive defense.



Fig 5: AI-Based Malware Analysis

In the Graphical Analysis section, the Column Chart provides a vertical comparative visualization of the system's findings, highlighting the relative volume of various data categories. This specific chart indicates that Unlabeled Data represents the vast majority of the dataset at 38.00%, significantly outperforming the detected attack volumes. The identified threats are categorized into three distinct columns: Ip Fragment Attack (2.00%), TCP Based Attack (2.00%), and Ping of Death Attack (1.00%). This vertical alignment makes it easy for an analyst to see that while the network is currently processing a high volume of raw data, the active, identified attacks remain at a low but measurable percentage.

6. CONCLUSION

This research presents a machine learning–based cyber attack detection framework using the KDD Cup intrusion detection dataset. Network traffic data was analyzed, categorical attributes encoded, and multi-class attack labels reduced into five categories. Multinomial Naive Bayes served as a baseline, revealing limitations in

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X ww.ijdim.com Original Research Paper

accuracy and minority class detection due to feature dependency and imbalance. To address these issues, a hybrid algorithm combining Decision Tree and LinearSVC with a voting mechanism was developed. The Decision Tree captured non-linear interactions, while LinearSVC improved generalization. The voting strategy enhanced robustness reduced false positives, and improved detection of rare attacks. Performance evaluation confirmed superior results, and deployment via a Flask-based web application validated real-time applicability for modern network environments.

FUTURE SCOPE:

Future work can enhance the system by integrating advanced ensemble and deep learning models such as XG Boost, CNN, and LSTM to improve detection accuracy and robustness. Real-time processing using big data frameworks and deployment in cloud or edge environments can improve scalability and performance. Additionally, handling class imbalance and incorporating explainable AI will increase reliability, transparency, and real-world applicability.

REFERENCES

[1] P. Sornsuwit and S. Jaiyen, "A new hybrid machine learning approach for cybersecurity threat detection based on adaptive boosting," Applied Artificial Intelligence, vol. 33, no. 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," in Proceedings of the IEEE International Conference on Cyber Warfare and Security, IEEE, Oct. 2020, pp. 1–6.

[3] Q. H. Vu, D. Ruta, and L. Cen, "Gradient boosting decision trees for cybersecurity threat detection based on network event logs," in Proceedings of the IEEE International Conference on Big Data (Big Data), IEEE, Dec. 2019, 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

International Journal of

DATA SCIENCE AND IOT MANAGEMENT SYSTEM

Peer Reviewed, Referred & Indexed Journal

ISSN: 3068-272X ww.ijdim.com Original Research Paper

Engineering, vol. 19, no. 12, pp. 1462–1474,
2018.