An Intelligent Approach to Cyber Attack Detection in Networks using Machine Learning Techniques

Mr. N. SaiKiran[1], Kommuri Vamsi Naga Jagadeesh[2]

[1]Associate Professor, Dept. of Computer Science and Engineering, MNSK College of Engineering and Technology, Tamil Nadu, India

[2]Final Year (B. Tech), Dept. of Computer Science and Engineering, MNSK College of Engineering and Technology, Tamil Nadu, India

DOI: https://doi.org/10.51584/IJRIAS.2025.100800117

Received: 06 August 2025; Accepted: 11 August 2025; Published: 19 September 2025

ABSTRACT

The escalating sophistication and volume of cyber threats have made the development of effective security techniques an urgent and paramount demand within the cybersecurity community. Traditional signature-based detection methods are increasingly challenged by novel and evasive attack vectors, necessitating a paradigm shift in defines strategies. In this context, machine learning (ML) has emerged as a field of profound importance for cybersecurity. Its inherent ability to identify complex patterns, adapt to evolving threats, and automate analytical processes has demonstrated significant promise in addressing various cybersecurity challenges.

Typically, machine learning applications in cybersecurity involve the automatic collection and aggregation of vast amounts of data from diverse system and network sources. This raw information is then meticulously analysed by ML algorithms to pinpoint potential security problems, ranging from malware identification to anomaly detection. However, the application of machine learning to the critical task of intrusion detection presents unique and fundamental challenges that differentiate it from other, perhaps more straightforward, ML applications. The dynamic, adversarial nature of cyber-attacks, coupled with the constantly shifting landscape of network environments, makes the effective employment of machine learning for intrusion detection significantly harder. This paper aims to delve into these complexities and explore robust machine learning approaches to overcome the inherent difficulties in accurately and efficiently detecting cyber-attacks within network infrastructures.

INTRODUCTION

In an increasingly interconnected world, cyber-crime is proliferating at an alarming rate, continuously exploiting every conceivable vulnerability within the computing environment. This pervasive threat necessitates an urgent and evolving response from the cybersecurity community. While ethical hackers diligently work to assess system weaknesses and recommend robust mitigation methodologies, the dynamic and intricate nature of modern cyber-attacks consistently challenges the efficacy of conventional defense mechanisms.Traditional Intrusion Detection Systems (IDS), which have long formed a cornerstone of network security, often struggle to cope with the sheer volume, velocity, and sophistication of contemporary threats. Their reliance on predefined signatures and rule sets renders them less effective against novel, zero-day attacks and polymorphic malware that mutate to evade detection. Amidst this challenging landscape, machine learning (ML) has emerged as a profoundly important discipline for enhancing cybersecurity. The inherent ability of ML algorithms to learn from vast datasets, identify intricate patterns, and adapt to evolving threats offers a promising avenue for developing more resilient and proactive security solutions. Technological advancements in computing power and communication networks have further amplified the potential of ML, allowing for the analysis of massive data streams generated by diverse systems and network sources to pinpoint potential security anomalies and malicious activities.

However, the proliferation of technology also brings with it significant challenges, particularly concerning the protection of sensitive information, the security of stored data platforms, and the continuous availability of critical services. These concerns are exacerbated by the rise of cyber-terrorism, which poses one of the most significant threats in this digital age. Cyber-terrorism, perpetrated by various groups including criminal organizations, highly skilled individuals, and cyber activists, has reached a level that can severely undermine open societies and national security by targeting critical infrastructure and essential services. It is precisely to address these multifaceted and evolving threats that Intrusion Detection Systems (IDS) have been developed. However, as previously highlighted, the task of effectively finding and identifying cyber-attacks is fundamentally different and significantly harder for the intrusion detection community when employing machine learning compared to other general-purpose ML applications. This distinction arises from factors such as the adversarial nature of attacks, the constantly shifting normal behaviour of networks, and the inherent imbalance in cybersecurity datasets. This paper seeks to explore and contribute to the development of advanced machine learning techniques specifically tailored to overcome these challenges, thereby improving the accuracy and efficiency of cyber-attack detection in dynamic network environments.

Data security remains a paramount concern, particularly when transmitting information across networked systems, and numerous solutions have been proposed within the existing literature to address this challenge. Among these, cryptography stands as a fundamental method for enciphering data, employing either symmetric or asymmetric key algorithms. While asymmetric key cryptography is generally considered highly secure due to its use of distinct keys for encryption and decryption, its key generation process is notably resource-intensive, consuming significant computational power and storage space [4].Existing cryptographic proposals present various trade-offs. For instance, the Advanced Encryption Standard (AES) is widely recognized as a high-security approach for data encryption [5]. Another method, the Shamir Secret Sharing Scheme, is also utilized for secure data distribution [6]. Furthermore, some approaches, like the one described in [7], encrypt sensitive data by performing an XOR operation with a random number, subsequently splitting and distributing the resulting shares across multiple cloud environments to enhance security and availability. Despite these advancements, the ongoing need for more efficient and robust data security solutions persists in an increasingly complex digital landscape.

LITERATURE SURVEY

The rate of attacks against networked systems has increased melodramatically, and the strategies used by the attackers are continuing to evolve. For example, the privacy of important information, security of stored data platforms, availability of knowledge, etc. Depending on these problems, cyber terrorism is one of the most important issues in today's world. Cyber terror, which caused a lot of problems to individuals and institutions, has reached a level that could threaten public and country security by various groups such as criminal organizations, professional persons, and cyber activists. Intrusion detection is one of the solutions to these attacks. A free and effective approach for designing Intrusion Detection Systems (IDS) is Machine Learning. In this study, deep learning and support vector machine (SVM) algorithms were used to detect port scan attempts based on the new CICIDS2017 dataset Introduction Network Intrusion Detection System (IDS) is a software-based application or a hardware device that is used to identify malicious behaviour in the network [1,2]. Based on the detection technique, intrusion detection is classified into anomaly-based and signature-based. IDS developers employ various techniques for intrusion detection. Information security is the process of protecting 12 information from unauthorized access, usage, disclosure, destruction, modification, or damage. The terms" Information security"," computer security" and" information insurance" are often used interchangeably.

Existing System:

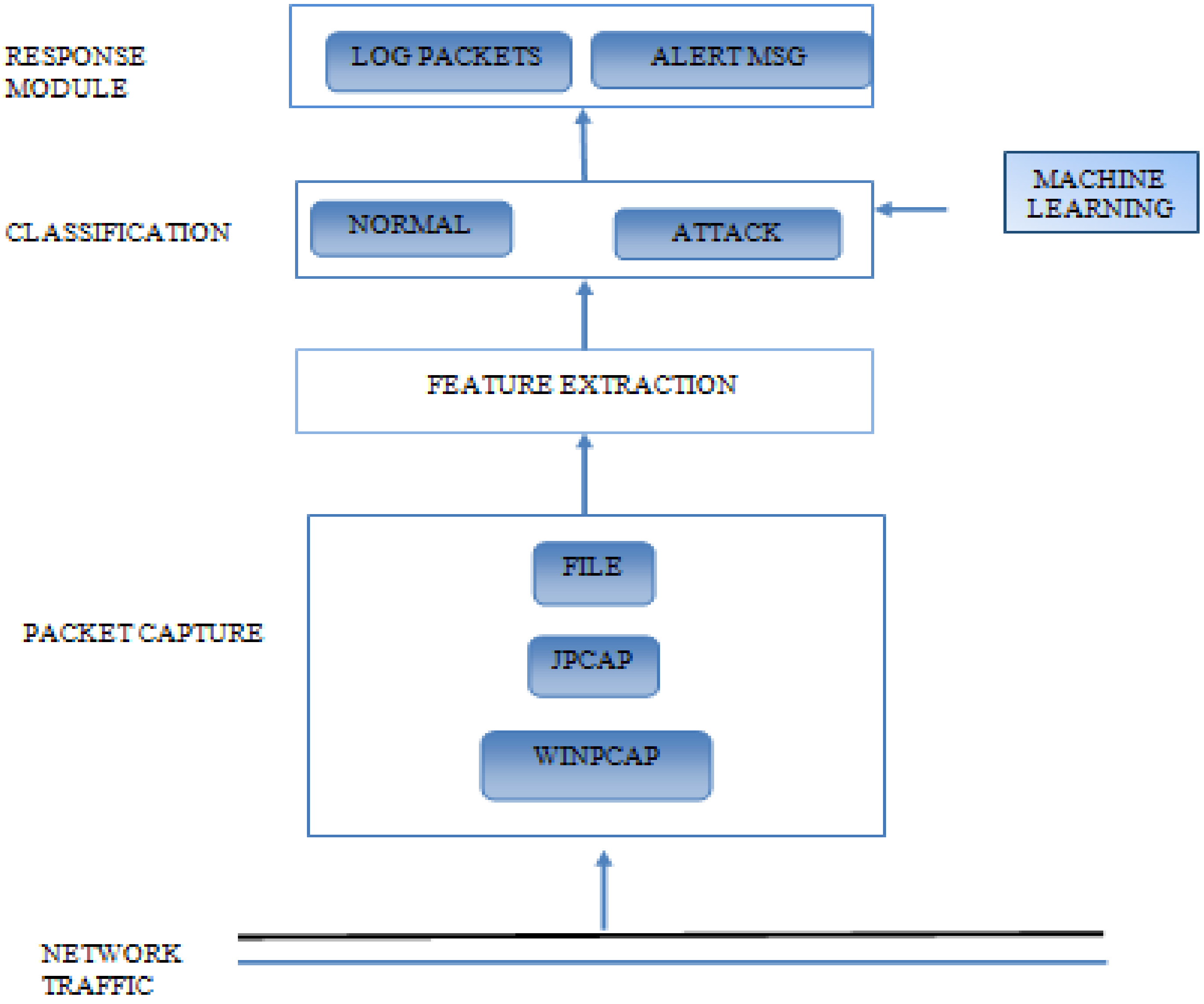
While Intrusion Detection Systems (IDS) are a foundational component of network security, most current techniques struggle to cope with the dynamic and complex nature of modern cyber-attacks. These limitations are particularly concerning as threats increasingly leverage encryption, which renders IDS incapable of inspecting packet contents, allowing intruders to slip deeper into the network unnoticed. A significant challenge for existing IDS deployments is their propensity for generating high volumes of false positives, often outnumbering actual threats. This saturation of alerts can lead to "alert fatigue," where legitimate attacks are either missed or ignored amidst the noise, leaving systems vulnerable until an intrusion is discovered.

Upon detecting suspicious activity, an IDS typically reports violations to a Security Information and Event

Management (SIEM) system. It is within the SIEM that real threats are ultimately distinguished from benign traffic abnormalities and other false alarms. However, this multi-stage process inherently introduces delays; the longer it takes to identify and confirm a genuine threat, the greater the potential for damage. While IDS are immensely valuable for continuous network monitoring, their overall effectiveness is contingent on subsequent human intervention. Since these detection tools do not inherently block or resolve potential issues, they are ineffective as a standalone security layer unless an organization possesses the requisite skilled personnel and robust policies to administer them and act decisively upon detected threats.

An IDS often fails to register intrusions until they have penetrated deeper into the network, thereby leaving systems vulnerable for an extended period until the breach is finally discovered. This delayed detection is a growing concern, particularly as encryption becomes increasingly prevalent for securing data, making it harder for traditional IDS to inspect packet contents. A significant drawback of current IDS implementations is their tendency to generate frequent false positives, often outnumbering actual security threats. While an IDS can be tuned to reduce these erroneous alerts, security engineers are still required to dedicate substantial time to investigating them. Consequently, if these false positives are not meticulously monitored and managed, there is a substantial risk that legitimate attacks may be overlooked or entirely ignored.

System Architecture:



Network traffic represents the aggregate data volume traversing a network at any given moment, primarily encapsulated within network packets that form the network's load. The meticulous analysis of this traffic is fundamental for effective network management, control, and simulation, offering significant benefits to organizations. Proper network traffic analysis enables the identification of **network bottlenecks**, pinpointing users or applications that consume excessive bandwidth and devising solutions to mitigate these issues. Crucially, it plays a vital role in **network security**, as anomalous traffic patterns can often signal a cyber attack. Comprehensive network traffic reports provide invaluable insights that are instrumental in preventing such incursions. Furthermore, insights derived from traffic analysis are essential for **network engineering**, allowing for the accurate assessment of current usage levels and the proactive planning for future network requirements.

Packet capture is a critical networking technique involving the interception of data packets at a specific point within a network as they transit. Once captured in real-time, these packets are temporarily stored for detailed analysis before being downloaded, archived, or discarded. The examination of captured packets is indispensable for diagnosing and resolving a wide array of network issues. This includes **identifying security threats** by scrutinizing malicious packet activity, **troubleshooting undesirable network behaviors**, detecting instances of **network congestion**, pinpointing **data/packet loss**, and performing **forensic network analysis** to reconstruct security incidents.

Classification is a widely utilized supervised machine learning task with extensive applications in cybersecurity. A prime example is the successful implementation of ML-based classifiers for **spam detection**, where models are trained to accurately discriminate between legitimate and unwanted email messages. These spam filter models effectively separate spam from non-spam communications, demonstrating the power of machine learning in identifying and categorizing threats. Machine learning techniques employed for classification tasks include, but are not limited to, Logistic Regression, among others Regression, K-Nearest Neighbors, Support Vector Machine, Naïve Bayes, Decision Tree, Random Forest Classification

This detailed description provides an excellent foundation for an "Implementation Details" or "Methodology" section of a research paper. Here's a structured and refined version, integrating all your points.

Machine Learning Algorithms for Cyber Attack Detection

The system leverages several prominent machine learning algorithms for securing confidential information and detecting cyber-attacks, each offering distinct characteristics:

1. Artificial Neural Network (ANN)

The design philosophy behind Artificial Neural Networks (ANNs) draws inspiration from the functioning of the human brain. An ANN typically comprises an input layer, one or more hidden layers, and an output layer, with units in neighbouring layers being fully interconnected. ANNs consist of a vast number of interconnected units, theoretically enabling them to approximate arbitrary functions. Consequently, they possess strong fitting capabilities, particularly effective for modelling complex, non-linear relationships within data. However, due to their intricate architectural design, the training process for ANNs can be computationally intensive and time-consuming.

2. Support Vector Machine (SVM)

The fundamental principle of Support Vector Machines (SVMs) is to identify a maximum margin separation hyperplane within an n-dimensional feature space. SVMs are capable of achieving satisfactory results even with relatively limited training datasets, primarily because the optimal separation hyperplane is determined by only a few crucial support vectors. A drawback, however, is that SVMs can be sensitive to noise present in data points located near the decision hyperplane.

3. K-Nearest Neighbor (KNN)

The core idea of the K-Nearest Neighbor (KNN) algorithm is rooted in the manifold hypothesis. It posits that if the majority of an example's neighbors belong to the same class, then that example has a high probability of also belonging to that class. Therefore, the classification outcome is directly influenced by the top-k closest neighbors. The choice of the parameter 'k' significantly impacts the performance of KNN models. A smaller 'k' tends to create a more complex model, increasing the risk of overfitting, whereas a larger 'k' results in a simpler model with potentially weaker fitting capabilities.

Proposed System Approach

The proposed system employs machine learning algorithms to train models capable of detecting cyber-attacks in network traffic. Upon the successful detection of an attack, an automated email notification is dispatched to relevant security engineers or users, ensuring prompt awareness. Any suitable classification algorithm can be utilized to categorize the detected incident, for instance, determining if it constitutes a Denial of Service (DoS) or Distributed Denial of Service (DDoS) attack. Support Vector Machine (SVM), as a supervised learning method that analyzes data and recognizes patterns, serves as a prime example of such a classification algorithm that can be leveraged.

Given that it is currently impossible to control when, where, or how a cyber-attack may manifest, and absolute prevention cannot yet be guaranteed, the paramount objective of this system is **early detection**. This proactive approach is crucial for mitigating the risk of irreparable damage that such incidents can inflict upon an organization's assets and operations. Organizations can either adopt existing solutions or develop their own to identify cyber-attacks at their nascent stages, thereby minimizing their overall impact. A system designed for minimal human intervention would be ideal in achieving this goal, providing a more autonomous and efficient defense mechanism.

It appears you've provided snippets that belong to different sections of a research paper or project report, specifically:

1. Problem Modelling (Network Admin functions)
2. System Analysis (Definitions)
3. Implementation (Software & SVM detail)

1. Problem Modelling

In the context of cybersecurity, the network administrator plays a crucial role in managing and monitoring network activity. The core functions of a network administrator, pertinent to this project's problem domain, involve:

- **Intercepting network traffic:** Continuously capturing data flowing through the network.
- **Reading and storing data packet information:** Extracting and archiving relevant details from intercepted packets for subsequent analysis.
- **Monitoring and responding to cyber-attack alerts:** Vigilantly checking for notifications regarding suspicious activities and potential cyber threats detected within the network.

2. System Analysis

The development of a robust cyber-attack detection system necessitates a thorough understanding of its constituent elements and operational principles.

a) System Definition

A system is formally defined as an orderly group of interdependent components linked together according to a predefined plan to achieve a specific objective. Its fundamental characteristics include a clear organizational structure, interactive components, mutual interdependence among these components, their seamless integration, and a unified central objective guiding their collective operation.

b) System Analysis Approach

System analysis involves applying a systematic approach to problem-solving, typically utilizing computational tools. To effectively reconstruct or design a system, an analyst must meticulously consider all its elements, including its expected outputs, necessary inputs, processing mechanisms, control measures, feedback loops, and the broader environmental context within which it operates. This holistic perspective ensures that all interdependencies and functional requirements are adequately addressed.

3. Implementation

Software Environment

The proposed system is implemented using **Anaconda**, which stands as the world's most popular data science platform. Anaconda serves as the foundational environment for modern machine learning development, providing the necessary tools, libraries, and package management capabilities for the project's execution.

Machine Learning Algorithms

Within the machine learning component of the system,

Support Vector Machines (SVMs) are utilized for classification tasks. The underlying principle of SVMs involves identifying a maximum-margin hyperplane that optimally separates data points into different classes within an n-dimensional feature space. SVMs are capable of achieving satisfactory classification outcomes even with relatively limited training sets because the decision hyperplane is primarily determined by a few critical data points known as support vectors. However, a known characteristic of SVMs is their sensitivity to noise in the data, particularly for instances located in close proximity to the decision hyperplane.

Software Requirements

Processor : Intel(R)Core (TM)I5 RAM : 2.00GB

System Type : 64Bit Operating System.

fundamentals of machine learning:

Support vector machine (SVM) is another widely used supervised machine learning model. SVM works to find hyperplane with most suitable dataset distribution by classifying the data into two classes on both sides of the hyperplane. Both sides of the hyperplane donate a separate class. The class of every data point depends on the side of the hyperplane it lands. Support vector machine has a high consumption of space and time to handle larger and noisier datasets . The computational complexity of SVM is O(n2) where n represents the number of instances . A matrix that is used to evaluate the performance of machine learning classifier is called a confusion matrix .

Cyber-attack detection techniques fall into two categories: signature-based and inconsistency-based. In both cases, machine learning techniques are used. The authors of improved the detection of Denial-of- Service (DoS) attacks. The Naive Bayes classifier was created based on the element vectors, which included different User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) bundles and their sizes. It has also been shown that Discrete Wavelet Transform and Matching Pursuit may successfully be used to calculate highlights depending on various organizational boundaries.

Error Rate:

The error rate (ERate) is a percentage of the total number of misclassified instances to all instances of the dataset.

ERate = (FPositive + FNegative)/ (TNegative + FPositive + FNegative + TPositive)

Recall:

The recall is a percentage of correctly classified positive instances to the total number of positive instances classified in the dataset.

Recall = TPositive / (TPositive + FNegative)

Precision

The precision is a percentage of the total number of positive instances classified to the total number of positive instances.

Precision= TPositive / (TPositive + FPositive)

Modules:

classification Feature extraction detection evaluation

METHODOLOGY

SVM

In this algorithm, we plot each data item as a point in n-dimensional space (where n is number offeatures you have) with the value of each feature being the value of a particular coordinate.

RESULT

The experiments were conducted in Machine learning libraries like numpy, pandas, scikit learn. Python language is used to develop the application with jupyter notebook IDE. Predictions can be done by four algorithms like SVM,ANN, RF, CNN this paper helps to identify which algorithm predicts the best accuracy rates which helps to predict best results to identify the cyber-attacks happened or not. Fig: 2 Protocol Type Distribution.

CONCLUSION

At the present time, assessments of help vector machine, ANN, CNN, Random Forest and significant learning estimations reliant upon current CICIDS2017 dataset were presented moderately. Results show that the significant learning estimation performed generally best results over SVM, ANN, RFand CNN. We will use port scope attempts just as other attack types with AI and significant learning computations, a pache Hadoop and shimmer advancements together ward on this dataset later on. Every one of these estimation assists us with recognizing the digital assault in network. It occurs in the manner that when we think about long back a long time there might be such countless assaults occurred so when these assaults are perceived then the highlights at which esteems these assaults are going on will be put away in some datasets. So, by utilizing these datasets we will anticipate if digital assault is finished. These forecasts should be possible by four calculations like SVM,ANN, RF, CNN this paper assists with distinguishing which calculation predicts the best precision rates which assists with foreseeing best outcomes to recognize the digital assaults occurred or not.

REFERENCES

1. K. Graves, Ceh: Official certified ethical hacker review guide: Exam 312-50. John Wiley & Sons, 2007.
2. R. Christopher, “Port scanning techniques and the defense against them,” SANS Institute, 2001.
3. M. Baykara, R. Das¸, and I. Karado gan, “Bilgi g ¨uvenligisistemlerinde kullanilan arac¸ larin incelenmesi,” in 1st International Symposium on Digital Forensics and Security (ISDFS13), 2013, pp.231– 239.
4. RashmiT V. “Predicting the System Failures Using Machine LearningAlgorithms”.International Journal of Advanced Scientific Innovation,vol. 1, no. 1, Dec. 2020, doi:10.5281/zenodo.4641686.
5. S. Robertson, E. V. Siegel, M. Miller, and S. J. Stolfo, “Surveillance detection in high bandwidth environments,” in DARPA Information Survivability Conference and Exposition, 2003. Proceedings, vol. 1.IEEE, 2003, pp. 130– 138.

6. K. Ibrahimi and M. Ouaddane, “Management of intrusion detectionsystems based-kdd99: Analysis with lda and pca,” in Wireless Networks and Mobile Communications (WINCOM), 2017 International Conference on. IEEE, 2017, pp. 1
7. M. Thangamani, and Jafar Ali Ibrahim. S, "Knowledge Exploration in Image Text Data using Data Hiding Scheme," Lecture Notes in Engineering and Computer Science: Proceedings of The International MultiConference of Engineers and Computer Scientists 2018, 14-16 March, 2018, Hong Kong, pp352-357 http://www.iaeng.org/publication/IMECS2018/IMECS2018_pp352-357.pdf
8. Jeyaselvi, M., M. Sathya, S. Suchitra, S. Jafar Ali Ibrahim, and N. S. Kalyan Chakravarthy. "SVM-Based Cloning and Jamming Attack Detection in IoT Sensor Networks." Advances in Information Communication Technology and Computing, pp. 461-471. Springer, Singapore, 2022. https://link.springer.com/chapter/10.1007/978-981-19-0619-0_41