SADI International Journal of Science, Engineering and Technology
ISSN: 2837-1941| Impact Factor: 8.27
Volume. 12, Number 3; July - September, 2025;
Published By: Scientific and Academic Development Institute (SADI)
8933 Willis AveLos Angeles, California
https://sadijournals.org/index.php/sijset|editorial@sadijournals.org

INTELLIGENT INTRUSION DETECTION SYSTEM USING MULTILAYERED TECHNIQUE

B. I. Ele, D. O. Egete and E. O. Omini
Department of Computer Science, University of Calabar, Calabar, Nigeria.
Email: mydays2020@gmail.com, / davidoboboho@gmail.com, / ominiebri77@gmail.com
Phone: +234(0)8064451381 / +234(0)8037204626 / +234(0)8172649857
DOI: https://doi.org/10.5281/zenodo.16894969

Abstract: Network users, administrators, and security professionals continue to express grave concern over the slowness, accuracy, and high false alarm rates of current network security systems. Therefore, immediate action is required to address these issues. Thus, this study aims to develop a more effective model of a network intrusion detection system for virtual local area networks using a multi-layered technique with radial basis functions (RBF) and support vector machines (SVM). The SSADM was used in this study to design the security system. The designed system was successfully implemented using JavaScript and Python programming languages with the vue.js, node.js, and express.js frameworks and tested with the NSL-KDD dataset with a virtual local area network. The developed system has a detection accuracy of 99% compared with the existing individual RBF and SVM systems with 76% and 87%, respectively. The ability of this system to accurately and quickly identify network-based attacks will be crucial in limiting the actions of intruders. This study's outcome was an improved NIDS that would proactively address potential security vulnerabilities by reliably and effectively detecting attacks and security policy violations in virtual LANs. Therefore, its use in the 21st-century security-conscious environment is inevitable.

Keywords: Intelligent, Network, Intrusion detection system, Radial basis, function, Support vector machine, Multilayered technique

1. Introduction

When designing a network, the specialists, who are occasionally known as network administrators, design and maintain the computer networks, repairing them when they malfunction. They teach users how to operate every network's hardware and software and update their security permits. Establishing a flexible and adaptable security-oriented approach is extremely difficult because of the increasing security risks to the Internet and computer networks and the constant emergence of new attack types. To safeguard target systems and networks against hostile activities, the multi-layered intrusion detection technique has become an invaluable technological tool.

Ele, Alo, Mbam, and Ofem (2016) opined that network intrusion detection systems (NIDSs) are assigned the critical role of monitoring the security state of the network; therefore, the NIDS itself is a primary target of attack. The NIDS must be able to operate in a hostile computing environment and exhibit a high degree of fault tolerance,

allowing for graceful degradation. Humans walking out with data on a memory stick or sharing proprietary information with social engineering hackers are also prone to insecurity, whereas network security, a subset of cybersecurity, covers what that user does on the network itself.

According to Ele and Mbam (2014), various sources of security threats for any network system are authenticity, access control, confidentiality, integrity, availability, and non-repudiation. Intrusion detection techniques are continuously evolving to improve the security and protection of networks and computer infrastructures. Despite the promising nature of multi-layered-based intrusion detection systems, as well as their relatively long existence, several security issues still exist.

Intrusion detection systems (IDS) are security tools that, like other measures such as antivirus software, firewalls, and access control schemes, are intended to strengthen the security of information and communication systems (Garcia-Teodoro, et al., 2019).

An X-ray by Agana and Ele (2019) shows that cybercrimes can threaten a nation's security and financial health. Computer system vulnerabilities persist worldwide, and the random cyber-attacks that plague computers on the Internet remain largely unknown. They further opined that cyberspace has become an environment where the most lucrative and safest crime This is partly due to inadequate awareness by Internet users, inadequate security restrictions to Internet access, inadequate cyber user identification/detection techniques, and loose cyber regulations on the prosecution of the culprits.

Unfortunately, keeping a network safe from intrusion is one of the most vital aspects of system and network security. A malicious attacker can penetrate a network and cause massive losses for any company, including potential downtime, data breaches, and loss of customer and client trust. Organizations have adopted the use of network systems to increase service efficiency and revenue. Moreover, some studies have shown how attackers can use this fact to hide their exploits by overloading a NIDS with extraneous information while executing an attack. Most intrusion detection systems perform poorly in defending themselves from attacks (Ele et al., 2016).

Recent research has focused on network intrusion detection using rule-based approaches and machine learning algorithms. The radial basis function (RBF) network is one of the most popular machine learning algorithms used in intrusion detection, which combines multiple input variables to create a series of predictions regarding potential exploits. RBF networks are also commonly employed in intrusion detection systems to identify and classify malicious traffic. RBF networks are frequently applied to networks that contain a variety of data, such as proxy servers. RBF networks use the data contained within the proxy server's logs to generate a series of predictions about potential cyber-attacks when used in such scenarios. These predictions include the attack source, attack type, and attack target. By combining this data with other frequently used IDS metrics, such as system vulnerability scans, RBF networks can generate accurate and timely predictions about potential cyber-attacks (Wang, et al., 2020).

Recently, the use of RBF networks for intrusion detection on computers and network systems has become increasingly popular. This is due to their ability to accurately classify malicious traffic and identify patterns in attackers' behavior. However, there are also some limitations to using RBF networks. For example, it is difficult to accurately detect new attacks because they do not have the same patterns as previously seen attacks. In addition, RBF networks can be computationally expensive, making them impractical for large-scale networks (Lee et al., 2020).

Machine learning (ML) techniques have gained wide interest in intrusion detection tasks. ML-IDSs are based on the definition of models that allow the classification of the analyzed information (Wang, et al., 2020). Support

vector machine (SVM) is one of the most attractive ML techniques (Burges, 2018). An SVM is a classification technique that has proven to be effective in a wide variety of problems, such as image processing (Hai & Thuy, 2022), often providing considerable improvement over competing methods.

Network layering limits access to devices, data, and applications and restricts communications between networks. Layering also separates and protects operational technology in network layers to ensure that industrial and other critical processes function as intended. Properly implemented decentralized networks and customized firewalls can prevent malicious actors from attempting to access high-value assets by shielding the network from unauthorized access.

2. Problem Statement

Network intrusion detection systems (NIDS) exist in varying forms and have several performance and effectiveness limitations. These limitations arise from problems associated with the traditional placement of the NIDS within any given network infrastructure. Despite the deployment of advanced security methodologies, several loopholes have not been filled. Data theft in industries is growing worldwide. Cybercrime depresses trade and investor confidence in companies. Apart from economic loss, internet fraud, credit card fraud, insurance fraud, tax evasion, financial fraud, securities fraud, insider attacks, money laundering, and embezzlement, as well as copyright and trade secret theft, constitute major problems to network systems. While it is not possible to completely protect industries from data theft, steps can be taken to protect industries from potential harm and attacks. However, information transmission over such networks can be compromised, and security breaches, such as viruses, denial of service, and unauthorized access, prevail. This research proposes an effective multi-layered technique for augmenting the functionalities of network security technologies because attacks are still bound to occur irrespective of the type of access control being employed.

3. Aim and Objectives of the Research

The main aim of this research is to develop an INIDS using a multi-layered approach that can detect and prevent intrusions and to integrate the same on networks to secure them. This will provide a solution that can secure the networked systems of industries from any potential threats and attacks. The specific objectives of the study are as follows:

i) To review related works and functionalities of existing intrusion detection systems to identify their shortfalls;
ii) To design a multi-layered network intrusion detection system using different machine learning techniques per layer, specifically RBF, SVM, and hybrid of RBF and SVM;
iii) Use the system to detect varying levels of intrusion that might tend to bypass a single-layer intrusion detection system;
iv) Implement the designed multi-layered system using Python programming language; and
v) To test using the NSL dataset and denial of service, remote-to-user, user-to-root, and probing attacks, and to evaluate the efficiency of the proposed system using a virtual local area network in comparison to existing systems.

4. Overview of the Intrusion Detection System

An intrusion is the act of intruding or the state of being intruded, especially the act of wrongfully entering upon, seizing, or taking possession of another's property. An intrusion occurs as soon as an intruder attempts to gain unauthorized access to or abuse a computing device. The intrusion detection system (IDS) is the mechanism for identifying intrusions. A network IDS will persistently monitor network packets and attempt to detect any attempt

to forcefully gain unauthorized access to the system. An intrusion detection system comprises processes for identifying, detecting, and reacting to intrusions.

Confidentiality, integrity, availability, and vulnerability (also known as the CIAV triad) are the four fundamental concepts of information security. A cyber-attack (or an intrusion) is defined as any unauthorized activity that compromises one, two, or all three components of an information system (Agana & Ele, 2019).

Intrusion detection **(**ID**)** methods are security frameworks designed to safeguard network information systems. The strength of an intrusion detection method depends on the robustness of the feature selection method (Joseph, et al., 2023).

The SANS Institute (2017) defined intrusion detection as the act of detecting inappropriate, inaccurate, or anomalous activity. The mechanism responsible for this task is called the intrusion detection system. Agana and Ele (2019) defined intrusion as a group of events that attempt conceding privacy, honesty, and accessibility of facilities.

IDS can be host- or network-based subject to the source of data for attack detection and signature- or behavior-based subject to the method of intrusion identification (Ele & Mbam, 2014).

In addition, some IDSs are passive, whereas others are reactive. IDS that simply identifies intrusion and generates alerts to the appropriate personnel, who will determine the next action, is called passive IDS. Reactive IDSs are IDSs that identify intrusion, generate alerts, and take reactive actions against the detected intrusion. An IDS is a strategically deployed network software system that regularly monitors network traffic and alerts the user or network administrator of any traffic anomalies (Hodo, 2018).

Furthermore, a complete network security mechanism must have the following modules:

i) **The intrusion detection module** differentiates possible attacks from normal network processes.
ii) **Protection module** that defends the security mechanism against network attacks;
iii) **The reaction subsystem** is the component that generates an alert and subsequently counters the detected intrusion.
iv) **The audit subsystem** is a thin subsystem where components can send their audit messages. The audit subsystem watches file accesses, monitors system calls, records user commands, records security events, searches for events, and runs summary reports.

Ele et al. (2016) opined that IDS is a vital part of the network security domain, and security is usually implemented as a multi-layer structure. The distinct techniques used to offer security are classified into six areas:

i) Attack Deterrence: According to Tao, Christopher, and Kotagiri (2012), attack deterrence is a process of convincing an intruder not to initiate intrusion by raising the professed danger of adverse penalties for the intruder. A robust legal system can be supportive in preventing attacks. Nevertheless, robust evidence against the intruder is needed in case an attack is initiated.

ii) Attack Prevention: William and Steven (2014) stated that attack prevention is a means of preventing intrusions by obstructing them before they reach their target. Nonetheless, it is difficult to avoid all intrusions because the systems require full knowledge of all potential attacks together with complete information of all permissible normal activities, which are not always available. Firewalls are examples of intrusion prevention systems.

iii) Attack Deflection: This implies fooling an intruder by making the intruder believe that the intrusion is fruitful, whereas the intruder was stuck by the system and intentionally made to disclose the intrusive intention. Honey pots are examples of attack deflection systems (Bace & Mell, 2018).

iv) Attack avoidance: Ele and Mabm (2014) asserted that attack avoidance is used to make a resource unworkable to the intruder even if the resource is illegally accessible. Cryptography is an example of an attack avoidance system. Data encryption makes data unusable by the intruder, thus preventing potential threats.

v) Attack Detection: This implies identifying intrusions that are on the way or that happened in the past. The basic reasons for identifying an attack are as follows: (i) the system must recuperate from the impairment caused by the intrusion and (ii) to allow the system to take measures to avoid upcoming comparable intrusions.

vi) **Attack Reaction and Recovery:** This is a process of reacting to an attack once it is detected and carrying out the recovery procedures as specified. IDSs are available tools for intrusion identification and subsequent response and retrieval procedures.

5. Review of Related Studies

There has been a lot of research into intrusion detection systems, and some of them have used machine learning and data mining techniques. Decision trees, neural networks, clustering, and Bayesian parameter estimation are some techniques that have been used to detect any intrusive behavior in a computer network.

Amor, Benferhat and Elouedi (2014) used naive Bayes classifiers to detect intrusions. Nonetheless, naive Bayes classifiers generate stringent independence postulation among the observation characteristics, leading to low accuracy of intrusion identification once these attributes are interrelated.

Kruegel, Mutz, Robertson, and Valeur (2013) asserted that intrusions can be detected using a Bayesian network. However, using a Bayesian network to detect intrusions tends to be intrusion-specific and form a decision network using intrusion-specific features. Therefore, the scope of the Bayesian network expands rapidly as the characteristics and nature of the intrusions modeled by it increase.

Wu, Foo, Mei, and Bagchi (2013) proposed a framework known as the Collaborative Intrusion Detection System (CIDS), which defines how host- and network-based intrusion detection systems are collaborative to overcome the flaw of a single intrusion detection system. The principal component analysis and naive Bayes classifier were employed by Panda and Patra (2017) to provide a method of detecting intrusion using machine learning algorithms. These experiments were conducted on the KDD'99 cup dataset, which is an intrusion detection dataset. The dimensionality of the dataset was reduced using principal component analysis, as well as the Naïve Bayes classifier classification of the dataset. This was performed in both the normal and attack classes. They concluded that the approach they used was a description of a network intrusion detection system framework that used two algorithms, naive Bayes and PCA. The results showed that their approach was faster than some of the other existing systems.

Chandolikar and Nandavadekar (2012) utilized the J48 intelligent algorithm in the experiments they did to make IDS. Their results show that J48 is an effective and efficient classification algorithm for the KDD CUP1999 dataset.

Bhavsar and Waghmare (2013) proposed IDS that uses a SVM as a data mining technique. Notably, SVM is a very popular classification algorithm. However, they highlighted the main drawback, which is that SVM takes a very long time to train the neural network. These experiments were performed using the improved version of the NSL-KDD Cup'99 dataset of the KDD Cup'99 dataset. They used the Gaussian RBF as the kernel function and a 10-fold cross validation as the test option parameter that was used for SVM. In addition, they pointed out that the proposed method-based SVM could increase the accuracy of intrusion detection and reduce the time taken to build this classification model.

Ektefa et al. (2020) used data mining techniques, including SVM and the IDS classification tree. The results reveal that the C4.5 algorithm is better than the SVM at detecting any network intrusions. These experiments were performed on a KDD CUP 99 dataset. Das and Nayak (2022) examined the IDS at its preprocessing level, which is the level before the classification process, and proposed a D&C algorithm. This study aims to reduce the feature set from the large KDD 99 dataset. The proposed algorithm successfully reduced the overhead of IDS for analyzing the entire KDD dataset. This was done by selecting the vital features and then classifying them all with a maximum classification rate. It was a generic algorithm that could be applied to any dataset. The authors used LDA, KNN, C4.5, SVM, and some classification algorithms to classify the obtained feature sets.

Lee and Stolfo (2016) and Lee et al. (2019, 2020) are the most closely related works to this study. The authors consider a data mining method for determining frequent episodes as well as mining association rules and compute the guidelines' backing and sureness distinctly. However, in this study, features are selected from the observations as well as from the previous labels and then sequence labeling is performed through conditional-random-fields to tag each attribute in the observation. This situation is adequate for modeling the relationship among the observation's varied characteristics. This study was also compared with that of Gu, McCallum, and Towsley (2015), in their research titled "Detecting Anomalies in Network Traffic Using Maximum Entropy Estimation" that defines application of Maximum Entropy principles for identifying abnormal activity in the network. The main distinction between the study by Gu et al. (2015) and this study is the high rate of false alarms generated by their system, whereas the system developed in this study will drastically reduce the false alarms to the barest minimum, if not completely eliminated. Furthermore, the system developed by Gu et al. (2015) cannot replicate distant dependence in the observations, and this can be easily replicated by the system developed in this study. This study also integrates the multi-layered approach with radial basis functions and a support vector machine to obtain the benefits of computing effectiveness and high accuracy of attack identification in a single system.

Based on the foregoing, this study employed the efficiency of radial basis functions (RBFs) and support vector machines (SVMs) for building a strong network intrusion detection system (NIDS) and a multi-layered approach to achieve high operation efficiency.

6. Methodology

In this study, both the prototyping methodology and the SSADM were employed. Both methodologies were employed to provide a detailed description of the system and provide an avenue for easy modification of the system as the need may arise in the future to produce an effective and efficient system. SSADM is suitable for analyzing and designing large systems, such as the MLNIDS, as it gives out a clearer view and representation of the modules, procedures, and functions with their respective relationships, and the representation of the objects (data and processes) as contained in the MLNIDS, as such giving the designers a complete analysis for the development of an efficient system that meets specifications as contained in the specification documents. Prototyping methodology was adopted because of its suitability for building fast, cost effective, reliable, and quality systems such as MLNIDS.

7. Justification of the new system

i) The new security system uses IP addresses for intrusion detection and management because the IP address is assigned to a single computer in the network. If active, no other computer can use that source IP address in the network.

ii) The new system can identify distributed denial of service (DDoS) intrusions by monitoring unusual packet size and unauthorized packet transmission.

iii) The new system is designed to function in three layers, i.e., if an intruder bypasses Layer 1, Layer 2, or Layer 3, the intruder can be detected. Thus, the proposed system incorporates attack layer segmentation.

iv) The new security system is an automated network monitoring system designed with network monitoring techniques that help to increase the performance and functionality of the network by detecting and alerting intrusions in the network efficiently and effectively.

v) The new security system is designed with a real-time response mechanism that can promptly launch a reaction process when an intrusion is identified.

8. Design of the new system

The new system is designed using the following tools: algorithm, flowchart, use case diagram, architectural framework, and dataflow diagram.

8.1 Algorithm for the hybrid RBF and SVM model

1. **RBF network preprocessing:**

   i) An RBF network is used as a preprocessing step to transform the input data into a higher-dimensional space where it is more linearly separable.

   ii) Train the RBF network using the data and adjust its parameters (e.g., number of neurons, spread) to effectively capture the underlying patterns in the data.

2. **Feature Extraction:**

   i) Features are extracted from the RBF network output. These features represent the transformed data in a higher-dimensional space.

3. **SVM Training:**

   i) The extracted features are used as input to train an SVM classifier; and

   ii) Choose an appropriate kernel for the SVM, such as linear, polynomial, or RBF kernel, depending on the problem and data characteristics.

4. **Model Evaluation:**

   i) The combined RBF-SVM model is evaluated using standard evaluation metrics to assess its performance on a validation dataset.

   ii) Fine-tune hyper-parameters as needed to optimize performance.

5. **Detection:**

   i) Given new input data, preprocess it using the trained RBF network.

   ii) Features are extracted from the RBF-transformed data.

   iii) The SVM classifier is used to predict the class label or outcome for the input data.

6. **Post-processing:**

i) Any necessary post-processing steps, such as threshold adjustment or probability calibration, are applied to refine the model's predictions.

8.2 Flowchart of the new security system

Figure 1 shows the flowchart of the new system.

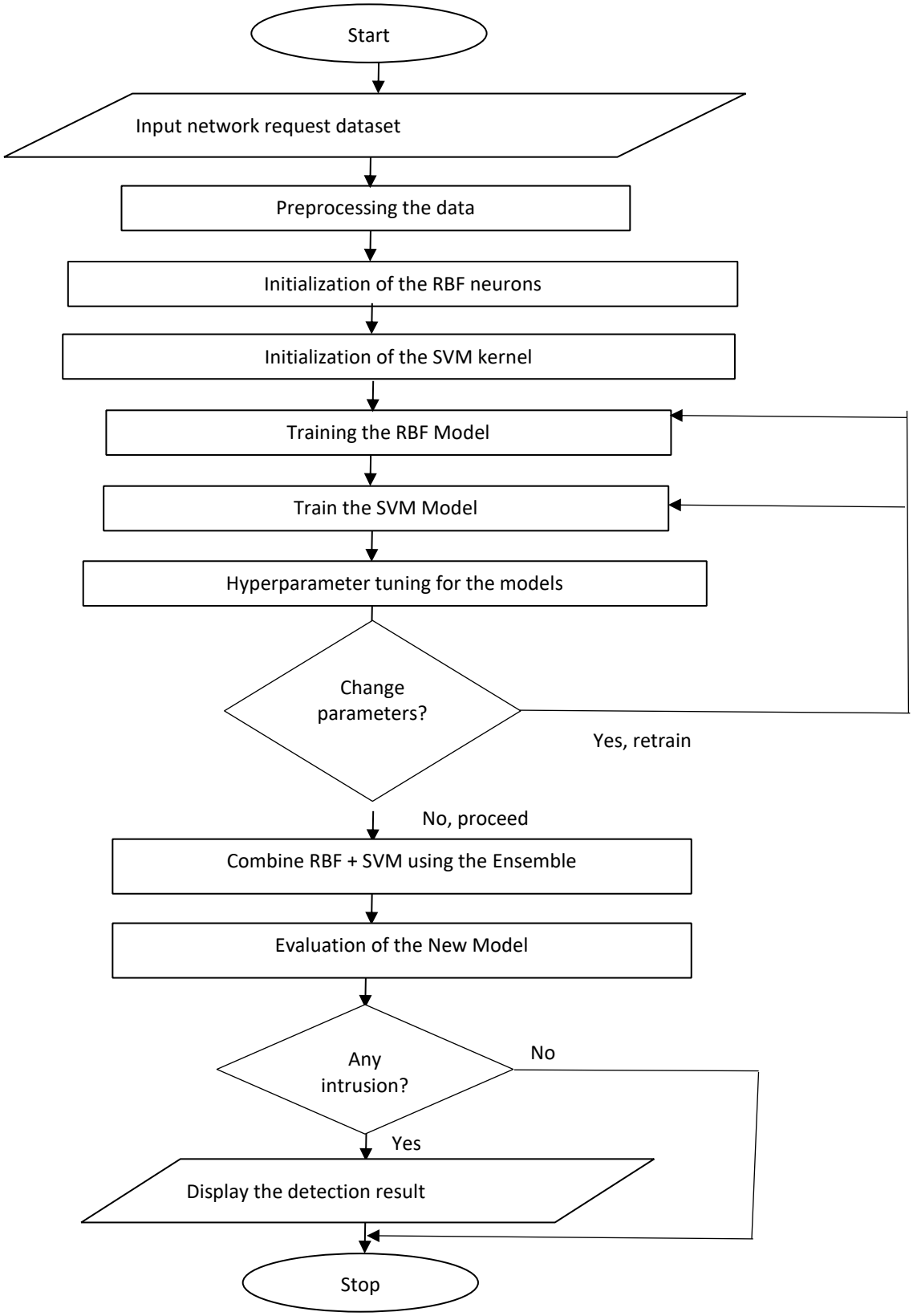

Figure 1: Flowchart of the new security system

8.2 Use Case Diagram of the New System

The use case diagram in Figure 2 indicates that the user (attacker) monitors the network performance and sends a network request to the server, which is then intercepted by the proxy server to determine whether it is a valid request. The admin monitors the users to determine where the malicious request originates and can then decide whether to block or filter such a user.

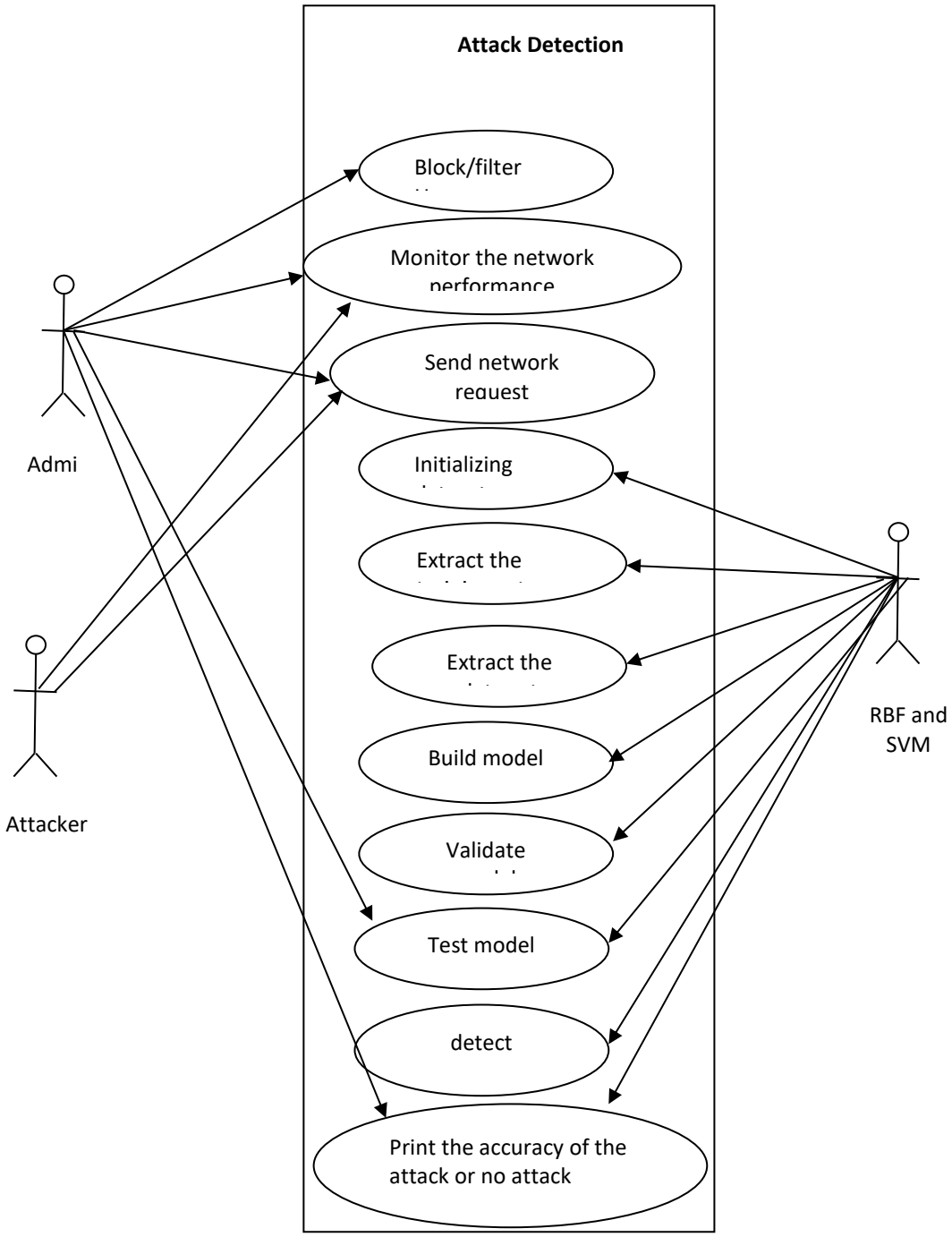

Figure 2: Use case diagram of the new system

8.3 Architectural framework of the new security system

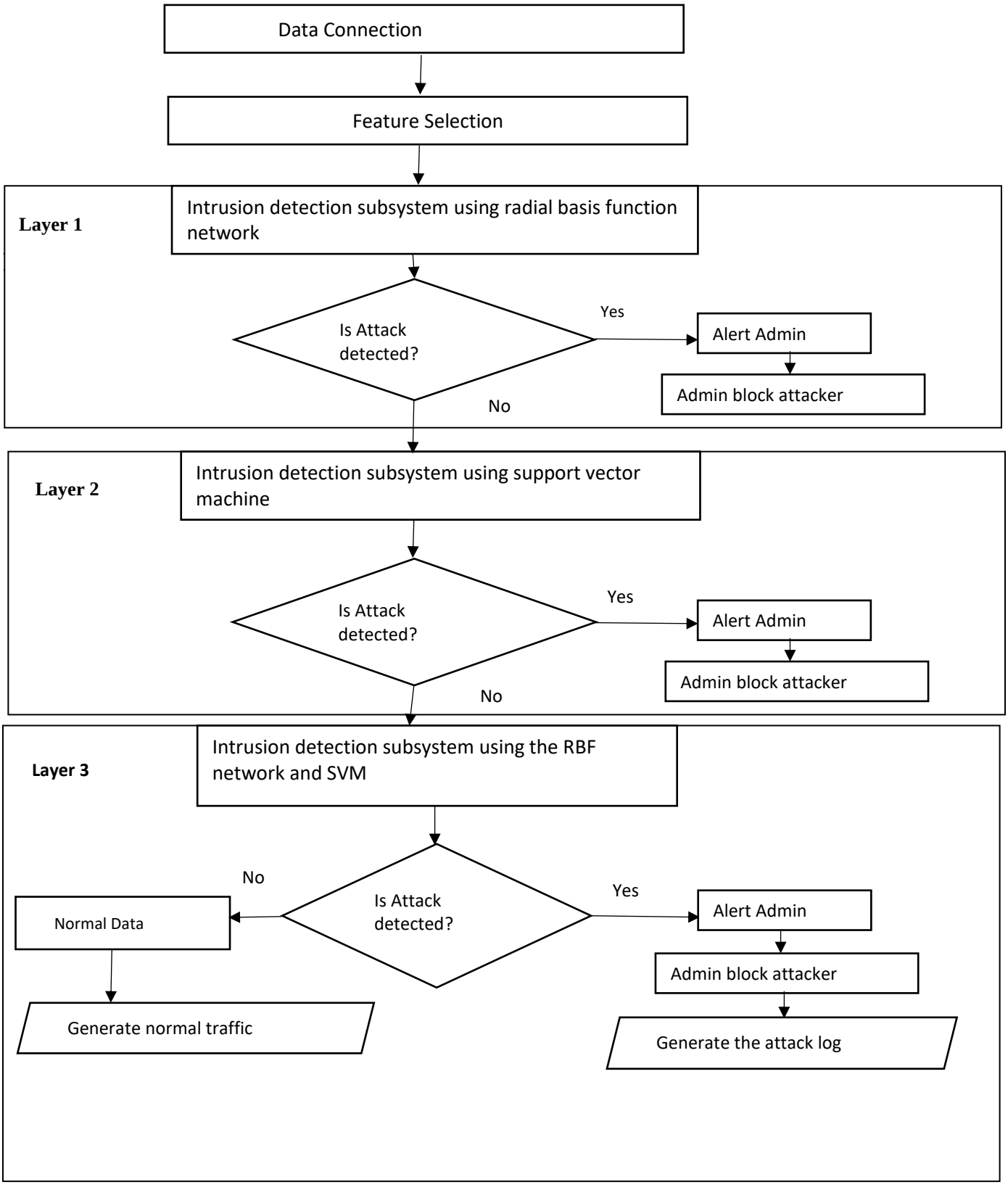

Figure 3: New system architecture

Figure 3 represents a **"3"** layer system where each layer in itself is a sub-intrusion detection module using different machine learning techniques that are specially trained to identify intrusions, such as remote-to-user, user-to-root, and probing attacks. These subsystems are then deployed consecutively in sequence, which will help to effectively detect attacks.

8.4 Overall data flow diagram of the new security system

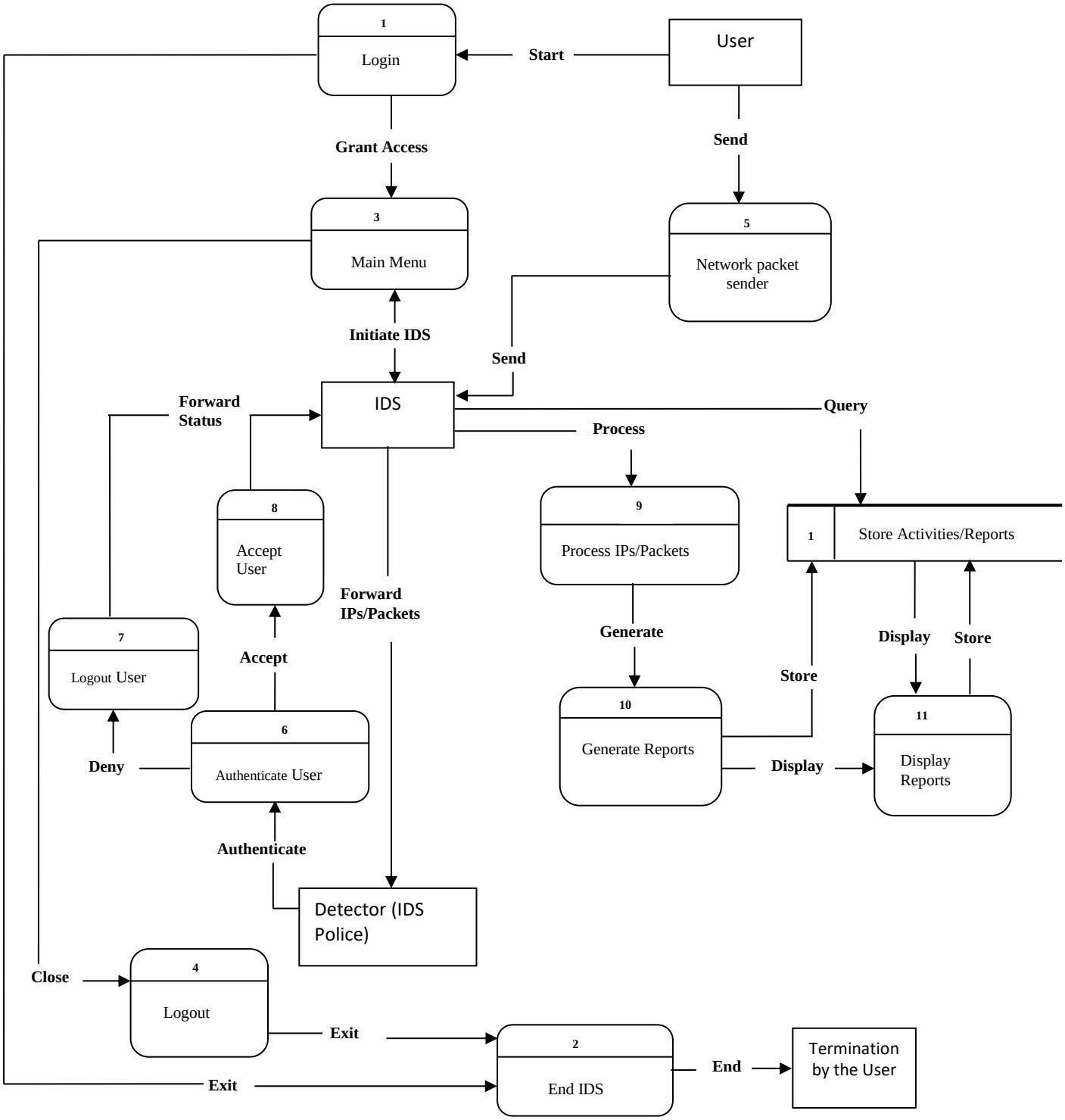

Figure 4: Overall data flow diagram of the new security system

Figure 4 shows the overall data flow diagram of the new security system. The overall data flow diagram explains the flow of data in the system in detail and depicts all the system's key procedures and their inputs or outputs.

9. Results and Discussion

9.1 Results

In this study, a multi-layered network intrusion detection system (MLNIDS) using radial basis functions (RBF) and support vector machine (SVM) was developed as a web application, as shown in the following figures.

The web application starts by showing a list of all the network cards present in the target device and allows one to monitor network traffic based on a specific network device (Figure 7). To test out different attacks for experimentation and evaluation, a provision in the code enables a network administrator to launch an attack on the target system. In displaying the attacks, the system displays the time, IP address, and type of attacks.

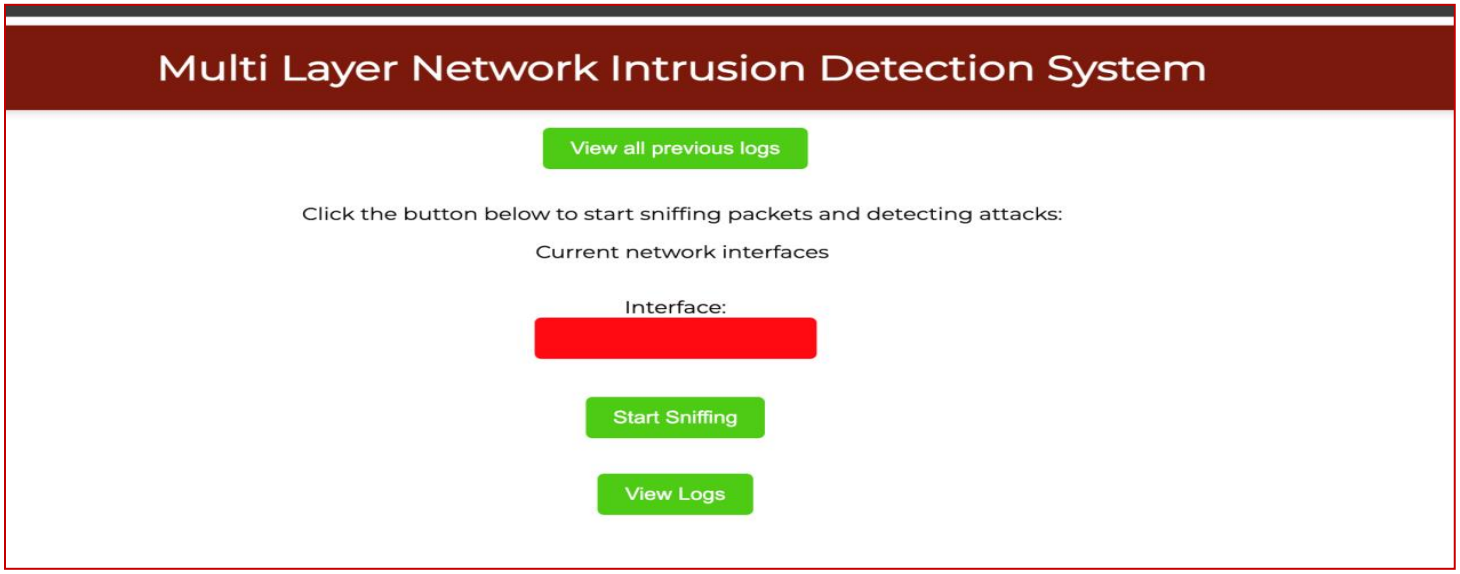

Figure 5: Main interface of the new system

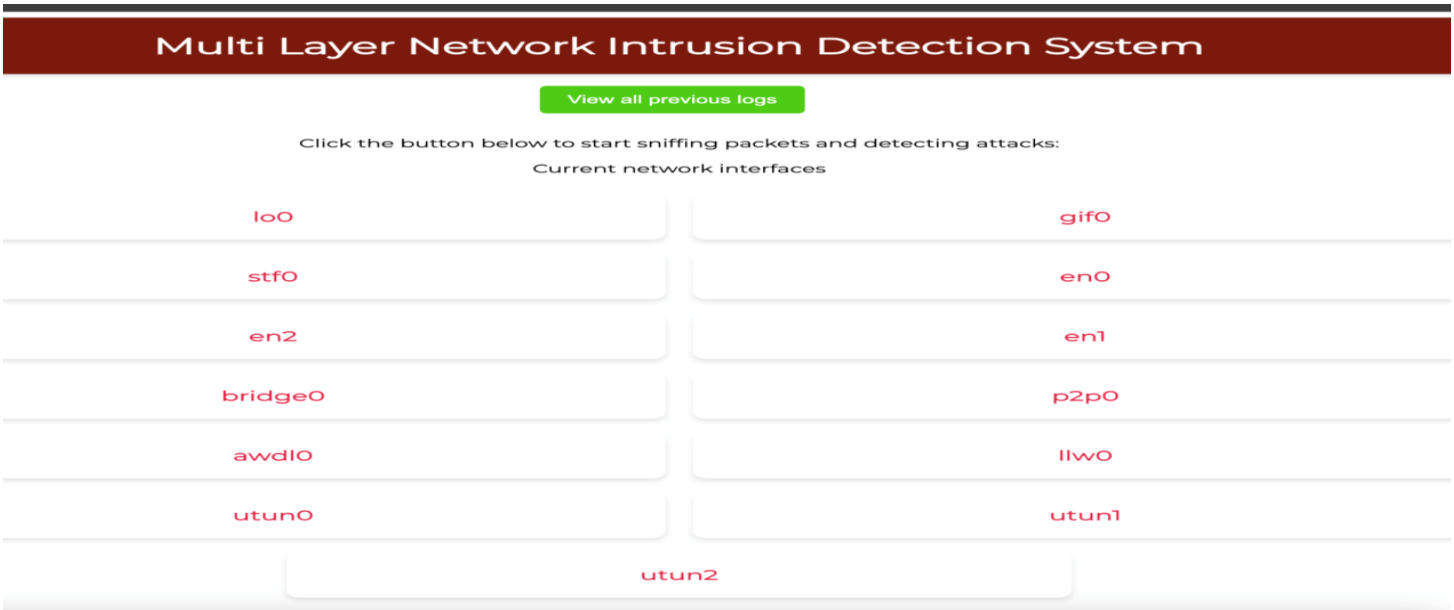

Figure 6: Interface showing the list of all network cards

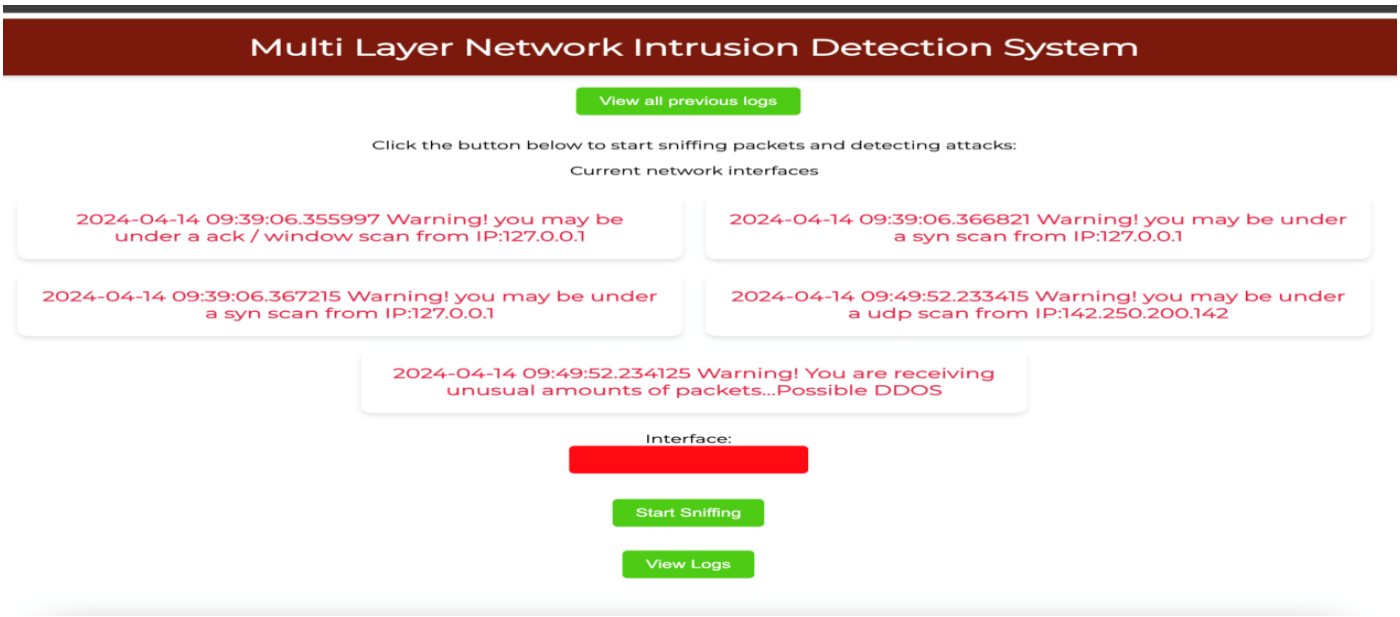

Figure 7: Interface showing the date/time, type of attack, and IP address

Figures 5, 6, 7, and 8 show the results of the machine learning run (as well as the Web Graphical Interface output).

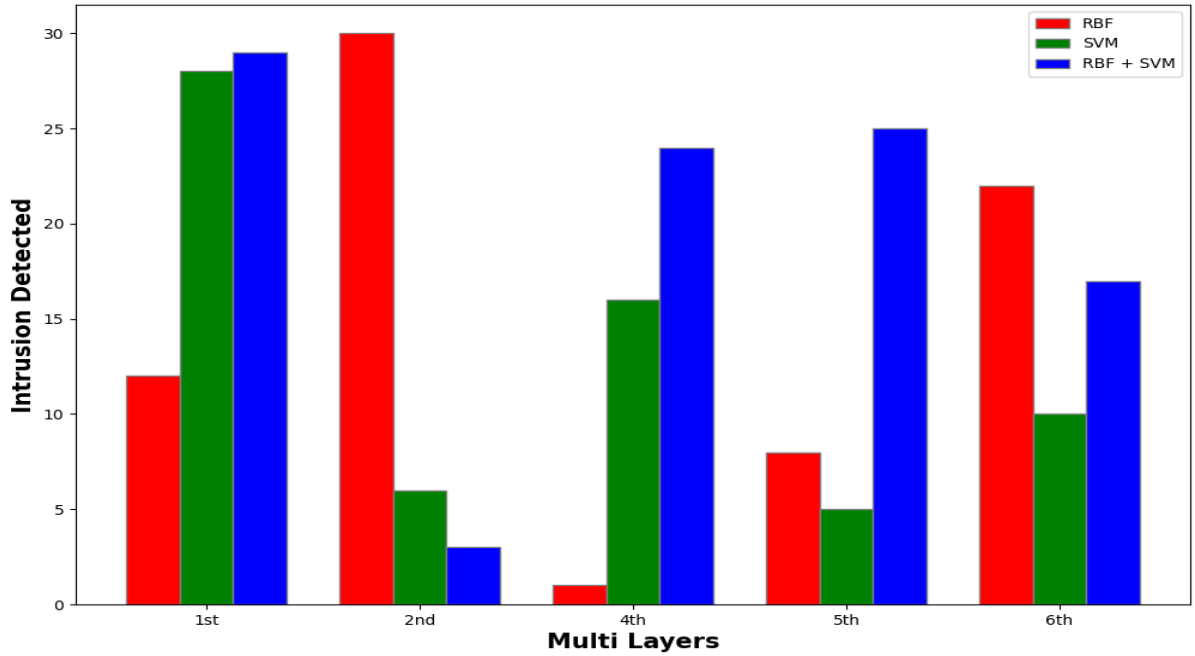

Figure 8: Bar chart showing the detection levels of various techniques

The bar chart in Figure 8 shows how the RBF, SVM, and RBF + SVM algorithms detect network intrusion in groups of bars. As shown in each bar group, Blue represents the combined algorithm, while Red and Green represent RBF and SVM,, respectively. The bar chart shows that the combined algorithm is more effective in detecting network intrusions than the individual RBF and SVM algorithms.

9.2 Discussion

Based on the network services included in the NSL dataset, the results in this study were calculated and examined using the new multilayer model (RBF and SVM). The bar charts show that the majority of daily network usage uses the http(s) network protocol, which contributes to a significant number of malware infections. A close

examination of the charts reveals that assaults are also being made against other types of network traffic. This suggests that attackers are looking for several avenues to access a user's system (some of which succeed, some of which fail).

From a network administrator's standpoint, the combination of protocol, flag, and service ought to provide a wealth of information about the type of traffic we have. However, we can better understand how the new multi-layer machine learning model anticipated the assaults across the various types of network traffic if we additionally consider the length of a connection and the volume of data in that connection. During the analysis, it was discovered that the multilayer approach to network intrusion detection makes it easier to identify and isolate various types of network intrusions.

Based on the evaluation of the system, the radial basis function (RBF) has a detection accuracy of 87%, the support vector machine (SVM) has a detection accuracy of 76%, and the hybrid model (RBF and SVM) has a detection accuracy of 99%, implying that the new system performs better than the individual RBF and SVM.

10. Conclusion

This study focused on the development of a multi-layered network intrusion detection system (MLNIDS) for virtual local area networks. In this study, the suitability of radial basis functions (RBF) network, support vector machine (SVM), and layered framework for building robust and efficient model of intrusion detection system for virtual local area networks was examined. In particular, a layered framework was introduced, and a multi-layered network intrusion detection system was developed and implemented to address the critical problems identified in Section 2 that severely affect the large-scale deployment of present intrusion detection systems in virtual local area networks.

This study observed that a layered framework can be used to build efficient intrusion detection systems. In addition, the framework offers ease of scalability for detecting various attacks and ease of customization by incorporating domain-specific knowledge. The framework also identifies the type of attack; hence, a specific intrusion response mechanism can be initiated, which helps minimize the attack's impact.

In this study, the multi-layered approach was compared with some well-known methods and found that most of the present methods for intrusion detection fail to reliably detect denial-of-service attacks, root-to-local attacks, and user-to-root attacks, whereas the integrated system developed in this study can effectively and efficiently detect such attacks. The developed system can help in identifying an attack once it is detected at a particular layer, which expedites the intrusion response mechanism, thus minimizing the impact of an attack. Finally, the developed system has the advantage that the number of layers can be increased or decreased depending on the environment in which the system is deployed, giving flexibility to the network administrators and security professionals to be flexible.

References

Agana, M. A. Ele, B. I. (2019). Cyber Crime and Security Vulnerabilities Awareness Information System Portal. International Journal of Natural and Applied Sciences, 12(Special Edition), 79–86.

Amor, N. B., Benferhat, S., & Elouedi, Z. (2014). Naive Bayes versus Decision trees in intrusion detection systems Proceedings of the ACM Symposium on Applied Computing (SAC '14), 420-424.

Bace, R. and Mell, P. (2018). Intrusion Detection Systems. Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology.

Bhavsar, Y. B. and Waghmare, K. C. (2013). Intrusion detection system using a data mining technique: SVM. International Journal of Emerging Technology and Advanced Engineering, 3(3), 581-586.

Burges, C. J. (2018). Tutorial on support vector machines for pattern recognition Data Mining and Knowledge Discovery, 2(2), 121-167.

Chandolikar, N. S., and V. D. Nandavadekar. 2012. Comparative Analysis of Two Intrusion Attack Classification Algorithms Using the KDD CUP Dataset International Journal of Computer Science and Engineering (IJCSE), 1(1), 81-88.

Das, A., & Nayak, R. B. (2022). A D&C feature reduction and feature selection algorithm in the KDD intrusion detection dataset. In Sustainable Energy and Intelligent Systems (SEISCON 2012), IET Chennai 3rd International on (1-4). IET.

Ektefa, M., Memar, S., Sidi, F., & Affendey, L. S. (2020). Intrusion detection using data mining techniques In Information Retrieval & Knowledge Management,(CAMP), 2010 International Conference on IEEE, 200-203.

Ele, B. I., Alo, U. R., Mbam, B. C. E. and Ofem, A. O. (2016). A Pragmatic Secure Intrusion Detection System Model for Local Area Networks British Journal of Mathematics and Computer Science, 13(2), 1–15.

Ele, B. I. and Mbam, B. C. E. (2014). Development of a Layered Conditional Random Field-Based Network Intrusion Detection System West African Journal of Industrial and Academic Research, 12(1), 3-20.

Garcia-Teodoro, P. Diaz-Verdejo, J. Macia-Fernandez, G. & Vazquez, E. (2019). Anomaly-based network intrusion detection: Techniques, systems and challenges. Computers & Security, 28(1), 18-28.

Gu, Y., McCallum, A. and Towsley, D. (2015). Anomalies in Network Traffic Detection Using Maximum Entropy Estimation Proceedings of Internet measurement Conference (IMC ’15), USENIX Association, 345-350.

Hai, T. S. & Thuy, N. T. (2022). Image classification using a support vector machine (SVM) and artificial neural network (ANN). International Journal of Information Technology and Computer Science (IJITCS), 4(5), 32-38.

Hodo, E. (2018). Machine Learning Approach for Detection of nonTor Traffic”. In: arXiv:1708.08725 [cs] (2017). URL: attp : //arxiv.org / abs/1708. 08725 (Retrieved on 07/02/2024).

Joseph, B. A., Femi, E. A., Ranjit, P., Amik, G., Akash, K. B. & Paolo, B. (2023). A Multilevel Random Forest Model-Based Intrusion Detection Using a Fuzzy Inference System for IoT Networks International Journal of Computational Intelligence Systems. 16-31,

Kruegel, C. Mutz, D. Robertson, W. and Valeur, F. (2013). Bayesian event classification for intrusion detection Proceedings of the 19th Annual Computer Security Applications Conference (ACSAC '03), pp. 14-23.

Lee, H., Song, J. & Park, D. (2019). An intrusion detection system based on multiclass SVM. In: Proceedings of the International Workshop on Rough Sets, Fuzzy Sets, Data Mining, and Granular-Soft Computing, pp. 511-519.

Lee, S., Kim, Y., Choi, H., & Kim, K. (2020). Detecting malicious traffic in web proxy logs using RBF networks. In Proceedings of the 8th International Conference on Computer Science & Information Technology (pp. 81-87).

Lee, W., and S. Stolfo. 2016. Data mining approaches for intrusion detection Proceedings of the Seventh USENIX Security Symposium. pp. 79-94.

Panda, M., & Patra, M. R. (2017). Network intrusion detection using naive Bayes algorithm International journal of computer science and network security(IJCSNS), 7(12), 258-263.

SANS Institute (2016). Intrusion Detection FAQ, http://www.sans.org/resources/idfaq/.

Tao, P.; Christopher, L.; Kotagiri, R. (2012). Adjusted Probabilistic Packet Marking for Technical Report CSE-96-11, Department of Computer Science, University of Technologies: Infrastructures for Collaborative Enterprises, 226-231.

Tombini, E., Debar, H., Me, L. and Ducasse, M. (2014). A Serial Combination of Anomaly and IDS Misuse Applied to HTTP Traffic Proceedings of the 20th Annual Computer Application Conference (ACSAC' 14), 428-437.

Wang, Y., Gao, M., Xu, J., & Wu, X. (2020). Detection and prediction of cyber-attacks on proxy servers and network systems using the RBF network. In Proceedings of the 11th International Conference on Information and Network Security, (53-60).

William R. C. and Steven M. B. (2014). Firewalls and Internet Security Addison-Wesley.

Wu, Y. S., Foo, B., Mei, Y., & Bagchi, S. (2013). "Collaborative Intrusion Detection System (CIDS): A Framework for Accurate and Efficient IDS." Proceedings of the 19th Annual Computer Security Applications Conference (ACSAC '03), pp. 234-244.