Journal of Information Systems Engineering and Management
2025, 10(53s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Enhancing Network Security through Multiclass SVM-Based Intrusion Detection Systems

Nisha Bhati [1], Shredha Parmar[2], Ajaj Khan[3], Jyotsana Goyal[4], Ranu Dixit[5], Deepesh Bhati[6]
[1,2,3,4]*Assistant Professor, Computer Science and Engineering, Medicaps University Indore, India*
[5]*Assistant Professor, Computer Science and Engineering, Sage University Indore, India*
[6]*Assistant Professor, Electrical and Electronics Engineering, IPSA IES, Indore, India*

ARTICLE INFO

Received: 31 Dec 2024

Revised: 20 Feb 2025

Accepted: 28 Feb 2025

ABSTRACT

This paper provides an intrusion detection system based on support vector machines (SVMs) for internet-based attacks on computer networks. The purpose of intrusion detection systems (IDS) is to anticipate and stop present and potential threats. SVMs are employed to detect and forecast anomalous system activity. The DARPA and KDD'99 intrusion detection evaluation datasets provided the training and testing data. Real-world data experimentation revealed encouraging outcomes for multiclass support vector machine intrusion detection systems.

Keywords: KDD'99, Defense Advanced Research Projects Agency (DARPA), Support Vector Machine (SVM), Intrusion Detection System (IDS).

INTRODUCTION

The evolution of business and the global economy are significantly influenced by the internet and enterprise networks. However, the range of network attacks and their ever-evolving nature can make achieving a secure network challenging. It is necessary to have adaptable security strategies that can swiftly examine vast amounts of network traffic and precisely identify various attack types.

Anomaly-based intrusion detection systems (IDSs) are useful tools in network security for detecting known and unknown (new) threats. IDSs that are trained to continuously observe typical patterns of behavior and identify any deviations from those patterns are known as anomaly-based IDSs [1]. The presence of an anomaly can yield vital information in anomaly-based intrusion detection systems. Unusual network traffic patterns, for instance, may indicate that a server is being attacked and that data is being transferred to an unauthorized location. Not only can network traffic anomalies reveal existing assaults, they also reveal novel attack patterns.

In many situations, though, abnormalities may just represent typical behaviors that haven't been recognized yet. Therefore, anomaly-based NIDSs must be

modified often to incorporate new network protocols and behaviors. High false alarm rates and poor detection accuracy against unknown assaults continue to plague many IDS techniques. Deep learning is a type of machine learning technique that has become more and more popular in recent years for pattern detection and categorization. To create a deep model, deep learning employs a hierarchical design with multiple input processing layers. Deep learning differs from traditional machine learning.

learning due to its capacity to identify the best features in unprocessed data by means of a series of nonlinear transformations, each of which reaches a greater degree of complexity and abstraction [2]. Deep learning techniques have been successfully used in a variety of research domains, including signal recognition, speech recognition, natural language processing, and medical image processing.

Convolutional neural networks (CNNs) outperformed other deep learning techniques in computer vision tasks including object and face identification. CNNs are a type of neural network that differs from conventional neural networks in that they include convolution and pooling layers rather than the fully linked hidden layers.

Journal of Information Systems Engineering and Management
2025, 10(53s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

INTRUSION DETECTION SYSTEMS

Intrusion Detection Systems (IDS) keep an eye out for any odd activity on the network to see whether it has been compromised. A host-based ID is different from a network-based ID. One machine power a host-based intrusion detection system, which keeps an eye on its own traffic for threats. An autonomous computer that monitors network traffic is home to a network-based intrusion detection system [3]. Two distinct techniques are available for detecting intrusions: anomaly intrusion detection and misuse intrusion detection. The more popular method, known as knowledge-based or misuse intrusion detection, compares network traffic to a database of known attacks. When an event in the database matches the signature of an attack, an alarm is triggered.

intrusion detection that is behavior-based examines network data for any deviation from the typical or

anticipated system behavior. After that, it absorbs the knowledge and adjusts accordingly. The accuracy and low false positive rate of misuse intrusion detection are two benefits. When an intrusion detection system mistakenly believes that regular traffic is an attack, this is known as a false positive. Keeping the database current with routine maintenance is a drawback of misuse intrusion detection. The anomalous intrusion detection system's primary drawback is its high false positive rate. Its capacity to evolve and adapt over time is the cause of this. One of its benefits, however, is its capacity to "detect attempts to exploit new and unforeseen vulnerabilities," even helping to uncover novel attacks.

MULTI-CLASS SVM

Despite being a binary classifier, academics are trying to expand the SVM model to address multi-class classification issues. The one versus all (one versus rest) method is the first attempt. Assuming a total of c classes and n training data in the form of (xi, yi), we must construct c binary SVM models. After training the SVM model, we define class J as favorable and the other classes as unfavorable. This subproblem is an unbalanced binary classification problem if there is an equal amount of training data in each class. It may be expressed as ;

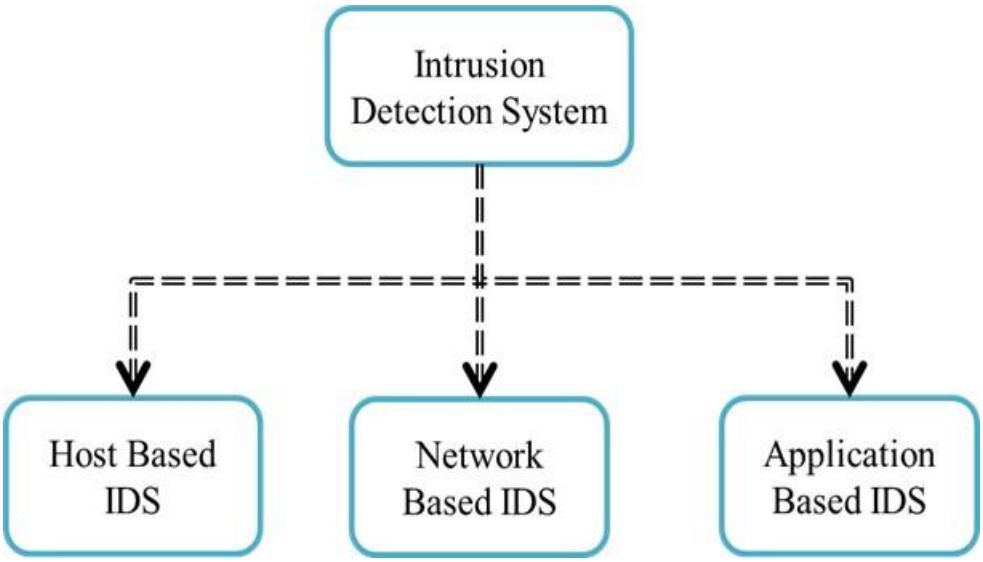


Fig.1 Multi class SVM structure

Despite being a binary classifier, academics are trying to expand the SVM model to address multi-class classification issues. The one versus all (one versus rest) method is the first attempt. Assuming a total of c classes and n training data in the form of (xi, yi), we must construct c binary SVM models. After training the SVM model, we define class J as favorable and the other classes as unfavorable. This subproblem is an unbalanced binary classification problem if there is an equal amount of training data in each class. It may be expressed as,

Journal of Information Systems Engineering and Management
2025, 10(53s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

$$\min_{w_j, b_j} \frac{1}{2}\|w_j\|_2^2 + C\sum_{i=1}^{n} \varepsilon_i^j w_j^T x_j + b_j \le 1 + \varepsilon_i^j, \ \text{if } y_i \ne j \ s.t\ w_j^T x_j + b_j \ge 1 - \varepsilon_i^j, \ \text{if } y_i = j$$

As previously stated, this strategy's primary flaw is that each binary classification is out of balance. This characteristic could influence how well one technique performs in comparison to the others on a multi-class classification issue. This issue is resolved by a one-versus-one technique that involves training more binary SVM models. With this approach, we will train a single binary SVM model for every two classes, totaling c(c−1)/2 models. The following problems can be used to learn that the maximum-margin hyperplane between classes j and k is wjkxi + bjk = 0.

$$\min_{w_{jk}, b_{jk}} \frac{1}{2}\|w_{jk}\|_2^2 + C\sum_{i=1}^{n} \varepsilon_i^{jk} s.t\ w_{jk}^T x_j + b_{jk} \ge 1 - \varepsilon_i^{jk}, \ \text{if } y_i = j \ w_{jk}^T x_j + b_{jk} \le 1 + \varepsilon_i^{jk}, \ \text{if } y_i \ne k \ \varepsilon_i^j \ge 0$$

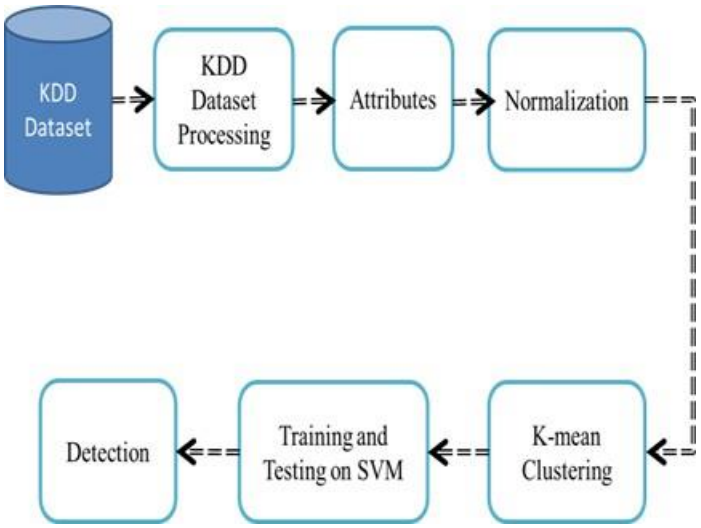
KDD'99 AND DARPA EVALUATION

MIT Lincoln Labs developed and oversaw the 1998 DARPA Intrusion Detection Evaluation Program, which created an environment to collect raw TCP dump data for nine weeks for a local-area network (LAN) that mimicked a normal LAN in the United States Air Force. They launched numerous attacks on the LAN while running it like a real Air Force setting. Four gigabytes of compressed binary TCP dump data and seven weeks' worth of network activity made up the raw training data. Approximately five million connection records were created from this. There were about two million connection records from the two weeks of test data. There was only one type of attack assigned to each connection record (about 100 bytes), which may be classified as normal or as an attack. The audit was conducted using a standard set of data that contained a wide range of intrusions that were mimicked in a military network environment. A variant of this dataset was used in the 1999 KDD intrusion detection challenge. 10% of the training and test datasets were tagged for this study. The test dataset has 37 attack types, which can be divided into 4 categories: Probe, DOS, U2R, and R2L. The training dataset has 22 attack types. Furthermore, there are patterns in both datasets that are indicative of typical behavior.

RESULT ANALYSIS

Using support vector machines, this study offers a comprehensive approach for choosing the optimal collection of KDD dataset features that effectively describe typical traffic and differentiate it from anomalous traffic. The hybrid feature selection method used in this study combines the filter and wrapper models. This method uses the information gain ratio, an independent metric, to rank features. The prediction accuracy of the k-means classifier is utilized to determine the ideal set of

the attributes displayed in Figure 2 that optimize the SVM classifier's detection accuracy.



Journal of Information Systems Engineering and Management
2025, 10(53s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Fig. 2 System Block Diagram

The IDS system uses a training dataset and five attributes to categorize network attacks. To carry out all of these tasks, a graphical user interface (GUI) has been created; Figure 3 illustrates this GUI.

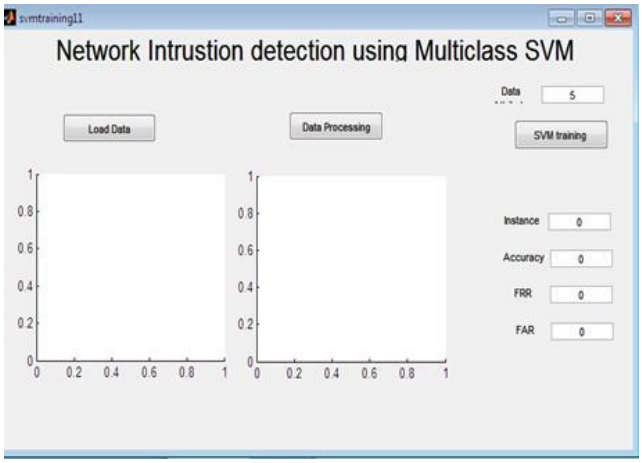


Fig. 3 GUI for SVM Network Intrusion

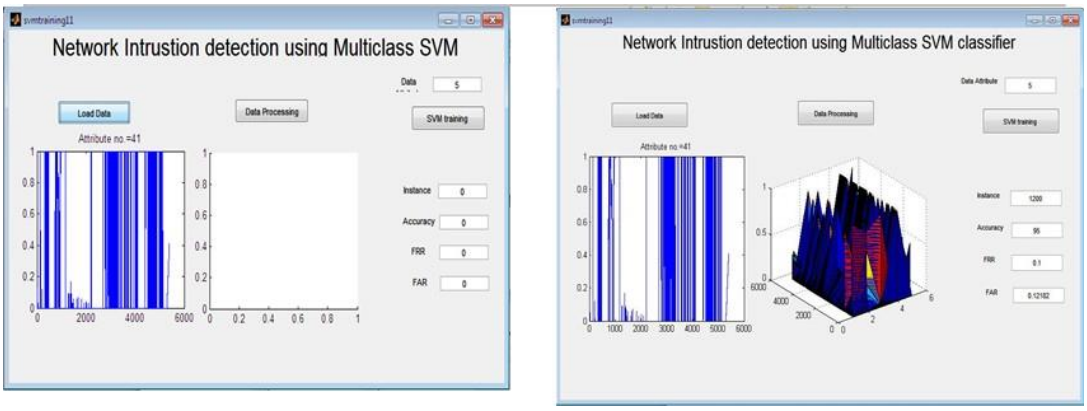


Fig 4 Load Training Data and SVM Training

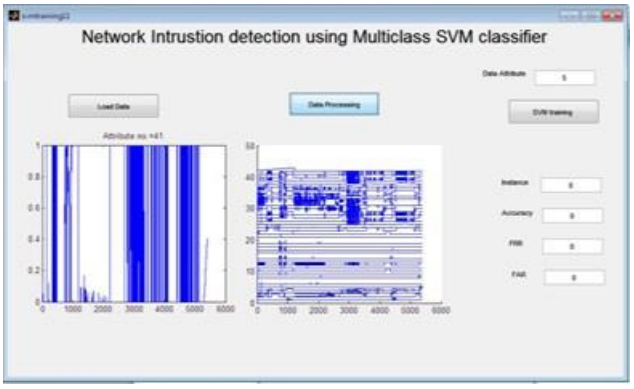


Fig 5 Data Processing

Journal of Information Systems Engineering and Management
2025, 10(53s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

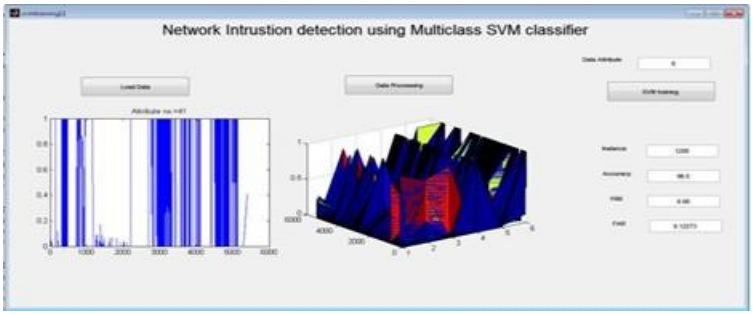


Fig 6 SVM Training with Data Attribute

The selection of attributes is a user-dependent parameter. To assess the algorithm's performance, the user can choose how many important attributes to include from the GUI and three distinct training datasets. The performance of the parameters is displayed in the table below.

Table 1: SVM Training Parameter Performance

S. No.	Parameter	Description		
1	Data Attribute	5	6	7
2	Instance	1200	1200	1200
3	Accuracy	95	96.8	97.83
4	FFR	0.1	0.08	0.02
5	FAR	0.12182	0.12273	0.12727

CONCLUSION

The various combination of training dataset has used for performance analysis. The multi-class support vector machine (SVM)algorithm has successfully used for development of intrusion detection system (IDS). The significant attributes is less than half of the total attributes which gives the performance above the 97.83%. This study demonstrates the effectiveness of using Multiclass Support Vector Machines (SVM) for network intrusion detection. By transforming the binary classification nature of traditional SVMs into a multiclass approach, the model is capable of accurately identifying and categorizing various types of network intrusions. The experimental results indicate that the multiclass SVM achieves high accuracy, precision, and recall across multiple intrusion categories, making it a robust choice for intrusion detection systems. Furthermore, the model shows good generalization performance on unseen data, highlighting its potential for real-time deployment in dynamic network environments. Future work may focus on integrating feature selection techniques and exploring hybrid models to enhance detection rates and computational efficiency.

REFERENCES

[1] Leila Mohammadpour, Teck Chaw Ling, Chee Sun Liewand ChunYongChong, “A Convolutional Neural Network forNetwork Intrusion Detection System”, Proceedings of the APAN, Research Workshop 2018.
[2] Witten, Ian H.; Frank, Eibe; Hall, Mark A., “Data mining Practical Machine Learning Tools and Techniques”, Third Edition. USA: Elsevier Inc, 2011.
[3] Wu, Xindong; Kumar, Vipin; Ross Quinlan, J.; Ghosh, Joydeep; Yang, Qiang; Motoda, Hiroshi; McLachlan, Geoffrey; Ng, Angus; Liu, Bing; Yu, Philip; Zhou, Zhi-Hua; Steinbach, Michael; Hand, David; Steinberg, Dan, “Top 10 algorithms in data mining”, Knowledge and Information Systems, 2008, Vol.14.
[4] Horng, Shi-Jinn, et al, ”A novel intrusion detection system based on hierarchical clustering and support vector machines”, Expert systems with Applications 38,1 2011.
[5] Gaspar, Paulo, Jaime Carbonell, and José Luís Oliveira, “On the parameter optimization of Support Vector Machines for binary classification”, 2012.

Journal of Information Systems Engineering and Management
2025, 10(53s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

[6] Hashem, Soukaena Hassan, "Efficiency of SVM and PCA to Enhance Intrusion Detection System", Journal of Asian Scientific Research, 2013.
[7] Waxman, Matthew C, "Cyber-Attacks and the Use of Force", Yale Journal of International Law. Vol. 36, 2011.
[8] Thomas, Ciza; Sharma, Vishwas; Balakrishnan, N. Dasarathy, Be- lur V., "Usefulness of DARPA dataset for intrusion detection system evaluation
[9] Tavallaee, Mahbod; Bagheri, Ebrahim; Lu, Wei; Ghorbani, Ali A., "A detailed analysis of the KDD CUP 99 data set", IEEE Symposium on Computational Intelligence for Security and De- fense Applications, July 2009.
[10] Asmaa Shaker Ashoor, Prof. Sharad Gore, "Importance of Intrusion Detection System", International Journal of Scientific & Engineering Research, Volume 2, Issue 1, January2011.
[11] Corinne Lawrence, "IPS The Future of Intrusion Detection", University of Auckland 26th October 2004.
[12] Anita K. Jones and Robert S. Sielken, "Computer System Intrusion Detection A Survey", International Journal of Computer Theory and Engineering, Vol.2, No.6, December, 2010