Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Development of Intrusion Detection & Prevention System (IDPS) Using SVM Model with New Kernel Function for Security Solutions

Itfaq Ahmad Mir[1], Anwaar Ahmad Wani[2]

[1]Sher-i-Kashmir University of Agriculture Science & Technology, Kashmir, UT-J&K.
[2]Mewar University, Chittorgarh, Rajasthan.

In digital era, every aspect has an online presence. Almost all the activities whether communication, financial transactions, shopping, social networking etc are carried out digitally. All these activities involve sharing of sensitive data and information, hence securing information has become inevitable for almost all agencies whether public or private. Confidentiality of information must be maintained for integrity of data, various studies have been proposed, to prevent the intrusion and cyber-attacks. Despite this, the hackers succeed in breaking the barriers and can access the data unauthentically. The proposed research study has produced a versatile Intrusion Detection and Prevention System (IDPS) to detect and prevent the intrusion of hackers in the web. To further enhance the performance of the proposed IDPS, SVM (Support Vector Machine) classification model, along with a linear kernel is used to classify the intruders, by using probability concepts in the SVM kernel function, which uses probability concepts to classify intruders and authenticated web users, suggested IDS is tuned for accuracy by using SVM classification model. An innovative SVM classification algorithm along with a new kernel function is used to develop and implement the new IDPS. This research work provides the overview on current active cyber-attacks (intrusions) as well as available intrusion detection and prevention methods.

Keywords: Intrusion, Cyber-attacks, Intrusion Detection System, Intrusion Detection and Prevent System, SVM, Kernel Functions.

1. Introduction

Intrusion Detection System (IDS)

An attempt to bypassing the network security of computer system is intrusion [1, 2]. An IDS is a device or a software application that monitors a network and systems (host) for malicious activity and policy violations [3].The malicious activities are reported to the system administrator or stored in security information and event management systems (SIEM). The IDS play an important role by preventing the network from malicious attacks and alerts the organizations networking system during unauthenticated intrusion by the hackers [4, 5].

IDS is classified into following four categories as under [6]:

1. Network Intrusion Detection System – The system which monitors the incoming traffic in a networking environment.

2. Host Based Intrusion Detection System – The system, which monitors the internal files of an operating system.

3. Anomaly Based Intrusion Detection System – This system is used in Machine Learning process, identifying the deviation of models from their normal behaviour.

4. Signature Based Intrusion Detection System – This system is uses to identify the malwares.

Intrusion Detection and Prevention System (IDPS)

IDPS is extension of IDS. It performs dual roles of identifying and preventing the networking systems from unauthenticated malwares or intruders [7]. These systems prevent the network from further invasion of malicious attacks. IDPS identifies malicious attacks, records their logs and try to block them from further invasion [8]. The main difference between IDS and IDPS is, IDS only detect the intrusion and send alert to the users whereas, IDPS prevents the networks and hosts from the intrusions after detecting of intrusions. The IDPS sends an alarm to the networking environment, if it identifies an intrusion, further stopping the traffic flow and blocking the offended IP address of the intruder [9].

IDPS are classified into following four categories [10]:

1. Host Based Intrusion Prevention System (HIPS) - This system monitors special software used to monitor the host behavior, by analyzing events occurring in the host or by analyzing the event log of the host.

2. Network Based Intrusion Prevention System (NIPS) - This system monitors the entire network and prevents from intrusion attacks by analyzing the protocol activity.

3. Wireless Intrusion Prevention System (WIPS) - This system analyses the wireless network protocols to monitor the suspicious activities in wireless networks.

4. Network Behavior Analysis - This system monitors and analyses the behavior of the networks. It analyses the unusual behavior of traffic flow such as distributed denial of services, violation in networking policies, malware attacks etc.

To implement the Intrusion Detection System following seven factors need to be analyzed :

- The way, information is collected (e.g. sensor alert, Application logs).
- Type of network on which IDS can be implemented.
- The strategy may be used to detect the intrusions (e.g. Anomaly or Misuse).
- Time aspects for implementing the IDS (e.g. Real or offline).
- The architecture (e.g. Centralized, Distributed, Heterogeneous).
- Activeness (active or passive).

- How the data need be monitored.

The complete IDS taxonomy is described by Aleksandar Lazarevi et al [11] and Zibusiso Dewa et al [12] as shown in figure 1.

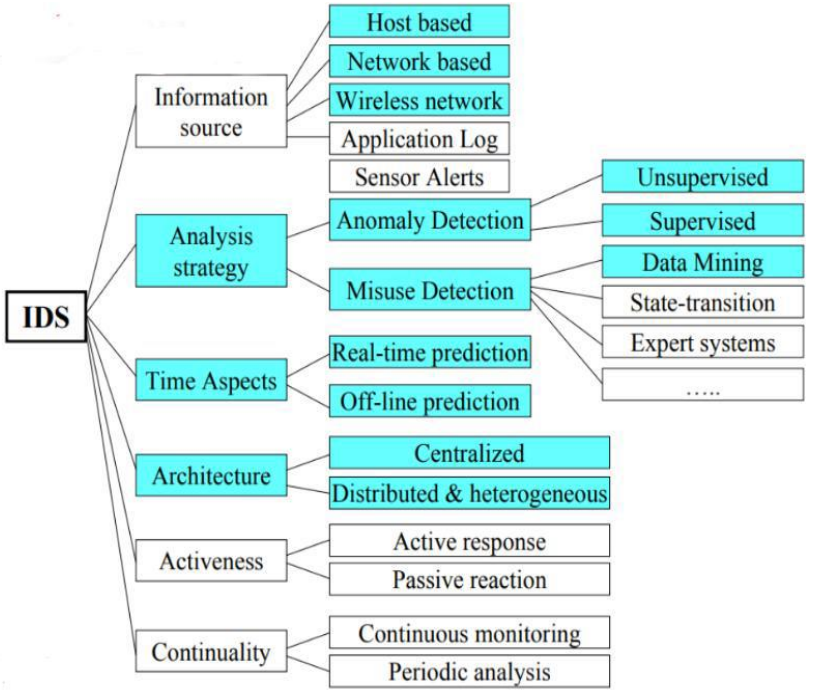

Figure 1: IDS Taxonomy

Intrusion Detection and other security technologies such as authentication, data integrity, cryptography etc have increasingly gained importance due to changing behavior of attacks [10]. Till now the existing intrusion detection systems are not able to detect the attacks and prevent the networks from the attacks perfectly. In case of emergency, the signature-based attacks cannot be detected in real time. Hence application of data mining has been explored as an alternative by the researchers in the field of intrusion detection.

SVM Classification Model

Features of this model are used in this research to classify the authenticated users from intruders quickly. SVM classification algorithm can be used for following:

I). Linear data. II). Non-linear data.

It uses a nonlinear mapping to transform the original training data into a higher dimension. Within this new dimension it searches for the linear optimal separating hyper plane a decision boundary separating the tuples of one class from other. With an appropriate nonlinear mapping to a sufficiently high dimension, data from two classes can always be separated by a hyper plane.

Following are the advantages of SVM:

a) Easy to implement.

b) SVM kernel helps to classify nonlinear data.

c) Provides unique solution.

d) SVM can be robust even if the sample data has bias.

Following are limitations of SVM :

a) Lack of transparency of results.

b) Accuracy drops for larger data sets.

c) Proper selection of kernel for better performance.

d) Extensive memory requirements for QP in large scale tasks.

2. Literature Review:

In today‘s world, securing web data from attackers is a challenging task. Researchers are still in progress to find an efficient solution, to detect and prevent the web intruders [13]. Due to varying in profile and different types of web attacks, finding a reliable intrusion detection and prevention solution is still a major problem [14]. Various researchers have attempted to design and develop efficient Intrusion Detection System (IDS) and Intrusion Detection and Prevention System (IDPS) in various areas and domains [15].

Martin Roesch (2006), proposed a light weighted intrusion detection system called Snort. Snort analyses the TCP/IP networking packets to identify malicious packets. The framework gave alert messages and caution to the network administrators, when any intrusions are detected [16]. A broad study done by Chih-Fong (2009) on various types of classifiers like single, hybrid and ensemble, which were used to classify the intruders from web log dataset. The study gave valuable information regarding, how classification models are effectively used to detect intruders [17]. An efficient framework for intrusion detection and prevention is suggested by Roam Fekolkin (2012). He has developed two IDPS engines namely Snort and Suricata, to detect and prevent the attackers. Snort called Single Threaded Signature based network. The model reads and compares the networking packets with known patterns of attacks. If the packets match the known packets, they are treated as intruders. Similar to Snort, Suricata, is another IDPS framework, based on predefined set of rules. It uses confusion matrix techniques like false negatives and false positive metrics to identify threats [18]. Intrusion detection in MANETs is proposed by Ehsan Amiri et al (2014). They have suggested a pioneering methodology, to prevent intrusion in dynamic networking nodes. They have proposed an IDS engine, which is used to detect local intrusions using local audit data. Along with the IDS engine they have also proposed an IDS watermarking technique, used to protect related data that are exchanged between nodes [19]. A study done by S. Vijayarani (2015) on various types of IDS in networking system, life cycle and various tools used for IDS. They also discussed about misuse detection as well as anomaly detection approach and suggested for future work to be done to enhance the classification-based IDS [20]. An approach suggested by Amrutha Ambre et al (2015) helped to approach the IDS in different perception. They used probability concepts to detect the intruder. Frequency of occurrence of events is

calculated, and the events which occur in lesser frequency are taken into consideration [21]. Classification of cancer genes using microarrays study done by X. W. Chen (2011), gave a broad view, how SVM can be implemented in various domains and suggested the wide area of its application.

3. Proposed System:

Our proposed IDPS using SVM model is efficient, quick and capacity to handle large datasets. The basic idea of the proposed model was derived from the finite Newton method for classification problems. The proposed SVM model uses incremental methodology to classify datasets and uses the new proposed RBF kernel function. Two new factors namely the gradient and hessian factors are introduced. Based on the values obtained, the proposed SVM classifies the dataset.

SVM based algorithms along with their supporting kernels, have become more popular in recent years, due to its simplicity and the powerful logic behind its execution [22]. There are certain drawbacks, which has to be overcome in the SVM model. SVM model operates on Quadratic Programming (QP) logic, which doubles the number of the training tuple during classification, which increases the memory and reduces the efficiency of the SVM model. As a result, SVM model lacks in handling large datasets. Therefore, SVM model requires scaling up, to operate in smaller PCs with moderate system configuration. The QP programming is divided into smaller executable problems. Concepts of incremental learning, parallel and distributed computing are used to solve these problems. Instead of considering the whole dataset for classification, subsets of data points are selected as training tuples for SVM model.

The following notations are used to build the proposed SVM model.

i. T – Transpose of row vector

ii. S(x.y) – inner dot products of two vectors

iii. ||x|| - second normal form of vector (x)

iv. A[m x n] – (m) data points

v. D[m x n] – diagonal matrix of value ±

The graphical representation of the proposed SVM model is illustrated in Figure 2.

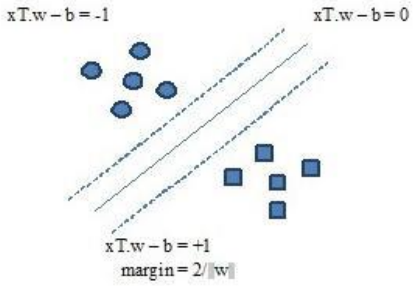

Figure 2: New SVM Algorithm

The hyper plane separates two classes of either of values ±. The condition, separating the two classes is xT.w – b = ± 1. The positively classified tuples has the value of +1 for the function and non-classfifed tuples has =1 vale for the function. The distance between the margins of the, separating the hyper planes is calculated from the values obtained from the equation 2/||w||. Maximum the margin distance, more the clarity and accuracy in classification.

The Poison distribution value is also added along with the notations. If value obtained is greater than or almost equal to one; the users are classified, else users will not be classified. Classified users are authenticated and allowed to access the system. OTP is send to the non-classified users, to evaluate them.

Proposed RBF Kernel Function

The proposed RBF kernel function implemented as the activation function for the SVM algorithm. The notations used in the proposed RBF kernel function is shown in Table 1.1.

Table 1.1: Illustrates the Various Notations Used in the Proposed RBF Kernel Function

f = function representing the kernel function
w = coefficient of hyper plane
b =scalar variable
z = slag variable
A = m x n matrix
D = diagonal matrix denoting class labels
PDval = Probability distribution value
C = constant

Modified IDS Architect Using New SVM Algorithm

The IDS proposed previously is further modified to improve the efficiency of the IDS using new SVM algorithm. Figure 3 illustrates the flow of the modified IDS architect using proposed SVM classification algorithm. At the first step, the input url from the web user is fed into the proposed UUI algorithm. If it is a new user, Poison distribution of the variable along with the frequency of occurrence is calculated from the previous history.

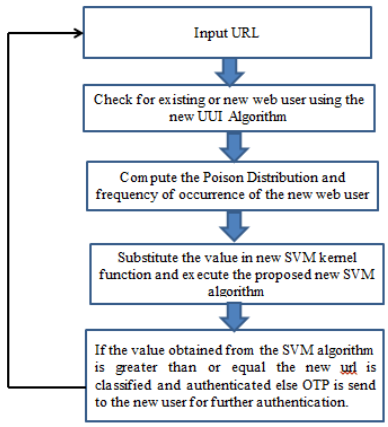

Figure 3: Modified IDS Architect using Proposed SVM Algorithm

The Poison distribution value is substituted in the proposed SVM kernel function, and the new SVM classification model is executed to classify the new user. If the value obtained from the SVM is greater than or equal to one, the web user is classified, or the user is authenticated to access the system. An OTP generated by the system is send to the non-classified web user for authentication. If the user responds to the OTP in time, authentication is provided to the user to access the system. Else the user is blocked from accessing the system.

Pseudo Code for the Proposed SVM Model for Intrusion Detection

Step 1: Input training data (new users) set represented by A and D matrices

Step 2: Starting with u0 € Rn+I and initializing i to 0

f(u) = (C/2)‖(1- e– DHu) * PDval

Step 3: Repeat

Step 4: ui+1 = ui - ∂2f(ui)-1-Δf(ui)

Step 5: If (ui+1) ≥ 1 then

Step 6: Classified valid user Else

Step 7: Send OTP to the new user

Step 8: If no response in time

Step 9: Non classified user

Step 10: i = i + 1

Step 11: Until Δf(ui) = 0

Step12: Return ui // New class generated from the algorithm.

Step wise Illustration of SVM Algorithm:-

I. The array of new users is taken as input for the proposed SVM algorithm in the first step.

II. In the second step the new user is initialized and cross checked whether it belongs to the new user array.

III. In the third step, the first order derivative of the proposed kernel function namely gradient and the second order derivative of the kernel function hessian are calculated from the new kernel function.

IV. Step four computes the difference between the value of the proposed kernel function along with the difference between the gradient and hessian are calculated.

V. Step six checks the value of step five. If the value is greater than or equal to one then the new user is classified and authenticated to access the system, which is represented in step six.

VI. Steps seven, eight and nine, depicts the detection of an intruder.

VII. In step ten next users from the array is validated.

VIII. The process in repeated until the gradient value is equal to zero.

Our proposed IDPS uses the concepts of SVM model. A new RBF kernel is developed. The new user table is used as the input for the kernel, along with the Poison distribution value of the new user. If the output of the kernel function is one, then the tuple is classified, means the user is valid, and allowed to access the system. If the output of the SVM model is minus one, then appropriate preventions are made by the system to validate the users. An alert and an OTP is send to the user. If the user responds the OTP in time, they are valid, else their IP address are blocked from accessing the system.

4. Experiment & Result Analysis:

Performance Analysis of Proposed SVM Model and Kernel Function

Different SVM kernel functions and the modified proposed kernel function implemented using proposed SVM model are tested for its accuracy and efficiency by the applications developed in MATLAB. Accuracy is calculated using confusion matrix techniques and efficiency is calculated by the time taken by the model to classify.

The proposed SVM kernel function is compared with other popular SVM kernel functions for the performance evaluation of proposed SVM kernel function shown in Table 1.2.

S.No	DatabaseUsed	Kernel Function	Data Size	Accuracy(%)	Time to Classify(s)
1	Fisher IrisDataset	Gaussian Function	10^{12}	52.25	4.725
2		Polynomial Function	10^{12}	89.11	3.89
3		Radial Basis Function	10^{12}	90.21	3.79
4		Fisher Function	10^{12}	92.67	3.25
5		Graph Function	10^{12}	91.25	3.62
6		String Function	10^{12}	90.01	3.77
7		Proposed SVM Kernel	10^{12}	94.32	2.66
1	Ionosphere Dataset	Gaussian Function	10^{12}	56.32	4.68
2		Polynomial Function	10^{12}	91.25	3.27
3		Radial Basis Function	10^{12}	89.42	3.64
4		Fisher Function	10^{12}	89.42	3.65
5		Graph Function	10^{12}	89.42	3.65
6		String Function	10^{12}	92.25	3.21
7		Proposed SVMKernel	10^{12}	94.78	2.90
1	Diabetic	Gaussian Function	10^{8}	72.34	3.62
2		Polynomial Function	10^{8}	80.25	3.12
3		Radial Basis Function	10^{8}	92.36	3.64
4		Fisher Function	10^{8}	90.21	3.65
5		Graph Function	10^{8}	92.77	3.65
6		String Function	10^{8}	92.25	3.21
7		Proposed SVM Kernel	10^{8}	96.78	2.87
1		Gaussian Function	10^{8}	81.67	3.52

2	Cancer	Polynomial Function	10^8	80.25	3.12
3		Radial Basis Function	10^8	92.36	3.64
4		Fisher Function	10^8	90.21	3.65
5		Graph Function	10^8	90.21	3.65
6		String Function	10^8	87.65	3.34
7		Proposed SVM Kernel	10^8	95.78	2.90

The information represented in the above table clearly shows the improved performance of the proposed SVM kernel function. With Fisher Iris dataset the accuracy level is 94.32, with ionosphere dataset the accuracy level is 94.78, with diabetic dataset the accuracy level is 96.78 and with cancer dataset the accuracy level is 95.78. There is no drop in the accuracy level even when the size of the database increases. This consistency level proves the efficiency and stability of the proposed SVM kernel and model. The results obtained also clearly depict the generalized performance of the models efficiently with different databases with their specific attributes.

The performance of the proposed SVM model compared with other popular classification models is shown in Table 1.3 and Figure 4.

DatabaseUsed	Data Size	Using Proposed SVM withproposed Kernel Function	Rule BasedClassifier	DecisionTree	Bayesian Classifier
	Accuracy (%)				
Fisher Iris	10^8	94.32	89.23	90.11	91.08
Ionosphere	10^8	94.78	91.27	92.33	92.21
Diabetic	10^{12}	96.78	92.33	93.62	93.38
Cancer	10^{12}	95.78	90.21	92.11	93.01

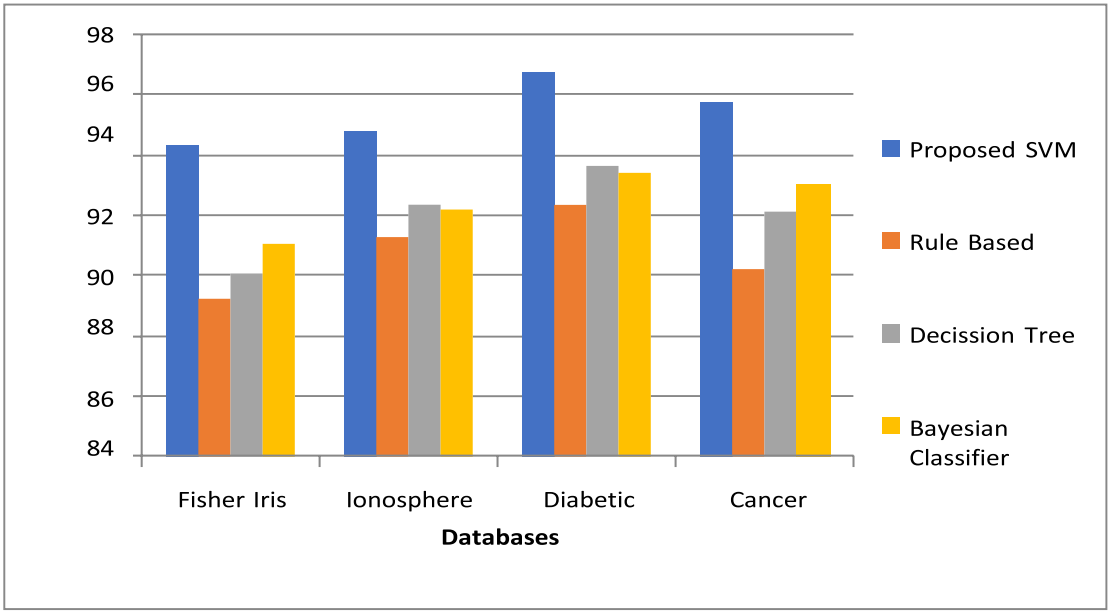

Figure 4: Performance Analysis of Different Classification Models with Different Datasets

The inference drawn from the Table 1.3 and figure 4 shows that the proposed SVM model has

produced better results than advanced classification models like Decision tree. Decision tree model had produced 90.11, 92.33, 93.62 and 92.11 percentage of accuracy for Fisher Iris, Ionosphere, Diabetic and Cancer datasets, whereas the proposed SVM model has produced 94.32, 94.78, 96.78 and 95.78 percentage of accuracy for the same datasets with same size. Thus, the tuning of the kernel function has substantially increased the performance of the proposed SVM model. The results also ensure the consistent performance of the proposed model for different datasets with their specific attributes.

The comparative accuracy results of the proposed SVM model along with the proposed kernel with the SVM model implemented with RBF kernel is shown in Table 1.4.

Table 1.4: Comparison Table of proposed SVM with Proposed Kernel Function and SVM with RBF Kernel

DatabaseUsed	Using Proposed SVM with proposed Kernel Function Accuracy (%)	DatabaseUsed	Using SVM with RBF KernelAccuracy (%)
Fisher Iris	94.32	Heart	89.23
Ionosphere	94.78	Diabetic	91.27
Diabetic	96.78	Satellite	92.33
Cancer	95.78	Shuttle	90.21

Comparing the models by taking the common datasets used in both the studies, the proposed SVM model has produced 96.78 percentage of accuracy for diabetic and 94.78 percentage of accuracy for ionosphere datasets, which is better than 91.27 percentage of accuracy for diabetic and 92.33 percentage of accuracy produced by the referred SVM model implemented with RBF kernel.

Performance Analysis of Modified IDS using Proposed SVM Algorithm

The performance comparison between IDS version 1.0 and IDS version 2.0 is shown in Table 1.5.

Table 1.5: Performance Comparison between IDS Version 1.0 and IDS Version 2.0

Total Events	Unauthorized Access (ProposedIDS_version 1.0)	Unauthorized Access (ProposedIDS version 2.0)	Login Failed (IDS version 1.0 IDS_version 1.0)	Login Failed (Proposed IDSversion 2.0)
250	43	50	6	10
210	34	43	4	8
165	28	32	3	6
130	17	24	2	4
80	10	15	2	3
60	08	10	1	2

From the results depicted in Table 1.5, the number of unauthorized access and failed login access are comparatively more in IDS version 2.0 than IDS version 1.0. Hence the clarity and efficiency in identifying the intruders is apparently better in using the new SVM classification model along with the new kernel function.

Comparative Analysis of Proposed IDPS Algorithm

This section describes the comparative analysis of the proposed framework with other related studies. The referred studies use simulated environment, to evaluate the performance of their studies. Different studies use different datasets to evaluate the performance of their IDS. The

results obtain prove that the proposed IDS, performs better over the other referred studies.

Table 1.6: Comparative Analysis of Proposed IDPS vs other IDPS Models

		Naive Bayesian Model		Network intrusion system framework		Proposed IDPS	
30	20	15	75	17	85	19	95
45	30	27	90	29	96	30	100
60	40	34	85	36	90	39	97.5
80	50	45	90	47	94	49	98
100	60	57	95	58	96	60	100
120	70	65	92	66	94	69	98.5

The new IDS is compared with the previous version which is evaluated earlier, the new version IDS perform better over the previous version in terms of efficiency and accuracy.

5. Conclusion:

In today‘s cyber world, prevention of web information is a key factor. Maintaining confidentiality of web data is a challenging task to most of the organizations, normal and cloud-based data centres. Attackers try to intrude the areas where the confidential web data is stored. Attackers and intruders are changing their profile frequently. Hence a strong intrusion detection and prevention mechanism is needed to detect and prevent the intruders at the initial stage itself. Many innovative techniques and tools are available, but the hackers overcome all the new technologies and somehow intrude the networking system, to hack data. This is a challenging problem for the researchers to develop a strong technique to prevent the hackers in real time. The proposed IDPS algorithm performs dual work of detection and prevention of intruders. The idea of integrating SVM model to the new IDS, has widened the dimension of this study. New SVM model along with the new kernel, improves the efficiency and accuracy of the IDS. The time taken to classify intruders from larger datasets has been minimized. SVM consumes less system configuration when dealing with Quadratic Programming in large scale tasks.

The proposed IDPS framework may also help to many organizations to detect and prevent the intrusions and cyber-attacks automatically and may reduce the false positive alarms. Thus, the proposed system is more full-proof and can work in real time environment which will improve the safety and security of the networks. This study has also attempted to provide the framework of IDS/IDPS that can help the organizations to efficiently deal with the issues of network breaches proactively.

References

1. A. Lazarevi, J. Srivastava, V. Kumar, ―Data Mining for Intrusion Detection‖, Army High Performance Computing Research Centre Department of Computer Science University of Minnesota Tutorial on the Pacific-Asia Conference on Knowledge Discovery in Databases, 2003.
2. J. Pei, S. J. Upadhyaya, F. Farooq and V. Govindaraju, "Data mining for intrusion detection: techniques, applications and systems," In Proceedings of 20th International Conference on Data Engineering, Boston, MA, USA, pp. 877-877, 2004.
3. S.E. Smaha, __Haystack: An Intrusion Detection System,‘‘ Proc. IEEE Fourth Aerospace Computer Security Applications Conference, Orlando, FL, Dec. 1988.

4. K. Ilgun, R. A. Kemmerer and P. A. Porras, "State transition analysis: a rule-based intrusion detection approach," in IEEE Transactions on Software Engineering, vol. 21, no. 3, pp. 181-199, March 1995.
5. Wagner, David and P. Soto, "Mimicry Attacks on Host-Based Intrusion Detection Systems," In Proceedings of the 9th ACM Conference on Computer and Communications Security - CCS 02, 2002 pp. 255-264.
6. U A Sandhu, S Haider, S Naseer, O U A, ―A Survey of Intrusion Detection and Prevention Techniques‖, International Journal of Information and Education Technology, Vol. 1, No. 5, pp 426 -431, 2011.
7. R. P. Lippmann, D.J. Fried, I. Graf, J.W. Haines, K.R. Kendall, D. McClung, D. Weber, S.E. Webster, D. Wyschogrod, R.K. Cunningham, and M.A. Zissman, "Evaluating Intrusion Detection Systems: The 1998 DARPA Off-Line Intrusion Detection Evaluation," Proceedings of the 2000 DARPA Information Survivability Conference and Exposition, 2000, pp 12–26.
8. A. Borkar, A. Donode and A. Kumari, "A survey on Intrusion Detection System (IDS) and Internal Intrusion Detection and protection system (IIDPS)," 2017 International Conference on Inventive Computing and Informatics (ICICI), Coimbatore, 2017, pp. 949-953.
9. K. Scarfone and P Mell, ―Guide to intrusion detection and prevention systems (idps)‖. NIST special publication, 800, pp.94, 2007.
10. W. Bul'ajoul, A. James and M. Pannu, "Improving Network Intrusion Detection System Performance through Quality of Service Configuration and Parallel Technology," Journal of Computer and System Sciences, vol. 81, no. 6, pp. 981-999, 2015.
11. A. Lazarevi, J. Srivastava, V. Kumar, ―Data Mining for Intrusion Detection‖, Army High Performance Computing Research Centre Department of Computer Science University of Minnesota Tutorial on the Pacific-Asia Conference on Knowledge Discovery in Databases, 2003.
12. Z. Dewa and L. A. Maglaras, "Data Mining and Intrusion Detection Systems," International Journal of Advanced Computer Science and Applications, vol. 7, no. 1, pp. 33-42, 2016.
13. B. Manu, "A Survey on Secure Network: Intrusion Detection & amp; Prevention Approaches", American Journal of Information Systems, Vol. 4, No. 3, pp 69-88, 2016.
14. M. Azhagiri et. al, ―Intrusion Detection and Prevention System: Technologies and Challenges‖, International Journal of Computer Networks and Communications Security, Vol. 3, No. 10, pp 384–395, 2015.
15. Naresh kumar Harale, Dr. B.B.Meshram, • \Network Based Intrusion Detection and Prevention Systems: Attack Classification Methodologies and Tools., International Journal of Engineering and Science, Vol.6, Issue 5 ,pp 01-12, 2016.
16. M. Roesch,‖ Snort: Lightweight intrusion detection for networks‖, Proceedings of LISA, , Systems Administration Conference ,1999, Vol. 99, No.. 1, pp. 229-238.
17. C.-F. Tsai, H. YF, L. CY and L. WY, "Intrusion Detection by machine learning: A review," Expert Systems with Applications, Springer, vol.36, no. 10, pp 11994 – 12000, 2009.
18. Albin, Eugene, and Neil C. Rowe. "A realistic experimental comparison of the Suricata and Snort intrusion-detection systems." In Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on, IEEE, 2012, pp. 122-127.
19. E. Amiri, K. Hassan, H. Heidari, E. Mohamadi and M. Hossein, "Intrusion detection system in MANET: A Review", Procedia-Soc. Behav. Sci., Vol 129, pp 453–459, 2014.
20. S. Vijayarani and S. S. Maria, " Intrusion Detection System- A Study," IJSPTM, vol. 4, no. 1, pp. 31-44, 2015.
21. A. Ambre and N. Shekokar, "Insider Threat Detection Using Log analysis and Event," Procedia Computer Science, ELSEVIER, vol. 45, no. 12, pp. 436- 445, 2015.
22. Jayshree Jha and Leena Ragha, "Intrusion Detection System Using Support Vector Machine", International Journal of Applied Information Systems (HAIS), ISSN : 2249-0868, 2013.