An Application and Performance Evaluation of Twin Extreme Learning Machine Classifier for Intrusion Detection

D. Vivek, K. Selvanayaki, C. AnoorSelvi

Abstract---Network along with Security is most significant in the digitalized environment. It is necessary to secure data from hackers and intruders. A strategy involved in protection of information from hackers will be termed as Intrusion Detection System (IDS).By taking into nature of attack or the usual conduct of user, investigation along with forecasting activities of the clients will be performed by mentioned system.Variousstrategies are utilized for the intrusion detection system. For the purpose of identification of hacking activity, utilization of machine learning based approach might be considered as novel strategy.In this paper, for identification of the hacking activity will be carried out by Twin Extreme Learning Machines (TELM).Employing the concept of Twin Support Vector Machine with the fundamental structure of Extreme Learning Machine is considered in the establishment of Twin Extreme Learning Machine (TELM).Also, its performance and accuracy are compared with the other intrusion detection techniques.

I. INTRODUCTION

Identification of hacking activity will be performed by Intrusion Detection system which is involved in supervising the traffic in the framework for unfaithful activity and concerns alerts when anintruder is identified. While anirregularityidentification and intimating to the concerned authority is the most prominent function, some intrusion detection systems are ableto takeproper decisions when harmful activity or irregular traffic is identified, that may be due to stoppage of traffic transmitted from suspicious IP addresses.Even though intrusion detection systems supervise networks for possibleharmful activity, they are also subjected to false alarms (false positives). Therefore, organizations required to adjust their IDS products when they first place them. That means properly arranging their intrusion detection systems to understand about the normal traffic on their network seemsto be compared to harmful activity.An Intrusion Prevention System(IPS) also supervises network packets for possibleharmful network traffic. But where an intrusion detection system acts to harmful traffic by retaining the traffic and broadcastingalarm notifications, intrusion prevention systems act to such traffic by stopping the possibleharmful packets.

Revised Manuscript Received on July 05, 2019

Dr. D. Vivek, Sri Krishna College of Engineering and Technology, Coimbatore.
Dr. K.Selvanayaki, Tamilnadu College of Engineering, Coimbatore.
C. AnoorSelvi, VSB College of Engineering, Karur.

Intrusion detection systems provides companies a number of advantages, starting with the capacity to discover security occurrences. An IDS can be utilized to aidexploring the quantity and types of strikes, and companies can utilize this information to alter their security systems or install more efficientpreventive mechanisms. An intrusion detection system can also stoporganization todiscoverinfectionsworries with their network device arrangement.

In this paper, Intrusion Detection is done by using Twin Extreme Learning Machines (TELM). Then this performance is compared with other Intrusion Detection techniques.Arrangement of balance work will be presented as succeeding. Section 2 involves study of various researches done with respect to the Intrusion Detection Systems. Section 3 establishesIntrusion Detection utilizing Twin Extreme Learning Machines (TELM). Section 4contains experimental outcomes. Lastly, Conclusion of proposed experimentation is presented in Section 5 along with the cited references that will be listed.

II. RELATED WORKS

Online Sequence Extreme Learning Machine (OS-ELM) was established **Li et al (2018)**which was involved in the framework for identification of hacking activity with respect to smart grid-based circumstance.The mentioned strategy was utilized in identification of having activity with respect to Advanced Metering infrastructure. Experimental investigation might be carried out by means of relating with additional strategies. Obtained outcomes demonstrated the effectiveness of proposed approach along with providing superior outcomes in terms of computing swiftness along with exactness will be established by relating with additional approaches involved in identification of hacking activity. Establishment of hacking activity identification system utilizing Support Vector Machine in combination with Particle Swarm Optimization was recommended by **Manekar and Waghmare (2014).**For the purpose of providing the optimization of parameter factor employment of Particle Swarm Optimization was carried out which results in the accomplishment of best value for C (cost) along with g (gamma parameter). Subsequently optimizing the selected features was performed utilizing Particle Swarm Optimization. SVM was provided with optimized parameters along with features that were obtained with the processing utilizing Particle Swarm Optimization for the purpose of classification.

mentioned strategy provided the improved exactness. NSL-KDD dataset was utilized for performing the experiments.

Designing of system which performs the identification of hacking activity with respect to network utilizing approaches relied with Machine learning strategies was established by**Das et al (2010).**For the purpose of identification of hacking activity with respect to strategies such asRough Set Theory (RST) along with Support Vector Machine (SVM) was employed. After capturing the packets from the network, RST was utilized in pre-analyzing the information along with minimization of size was carried out subsequent to retaining of packets.Providing the input to Support Vector Machine will be performed by utilizing the chosen features with the help of RST procedure.For minimizing the compactness of information, the mentioned strategy provided the competent solution.Investigational analysis was carried out by relating with additional strategies such as Principal Component Analysis. Superiority of accomplished outcomes was assured that might be involved in minimization of false positivesalong with enhancing exactness.

Utilization of machine learning approaches was suggested by **Zamani and Movahedi (2013)** in identification of hacking activity. Investigational analysis was performed utilizing various arrangement along with relating the functionality of entire selected approaches. Categorization of strategies into traditionalArtificial Intelligence (AI) along with approaches dependent withComputational Intelligence (CI). Numerous features involved in computational intelligence strategies was explained and might be involved in developing competent strategy that performs the process of identification of hacking activity.

Study of numerous involved in Identification of hacking activity with the help of Machine Learning approaches was performedby **Singh and Nene (2013)**.Consideration of numerous strategies comprised soft-computing along with machine learning strategies was established in construction of automated identification of hacking activity.The performed study proposes a solid fundamental for designing the system that performs the identification of hacking activity and provides the protection of system from hacking in a competent manner.

III. INTRUSION DETECTION USING TWIN EXTREME LEARNING MACHINES (TELM)

Selection of dataset, pre-analyzing the selected dataset, classification along with prediction of outcomes in addition with investigation of accomplished outcomes are the prominent stages involved in the suggested strategy.Providing the authenticity to everystage along with consideration of every stage as significant one. Enforcing the strategy of Twin Extreme Leaning Machine for performing the process of identification of hacking activity will be prominent concentration of suggested work.To assure the superiority of the suggested strategy, outcomes obtained will be analyzed with the outcomes obtained by using additional classifiers such as Support Vector Machine, Twin Support Vector Machine along with Extreme Learning Machine.

3.1. Extreme Learning Machines

An innovative strategy utilized for the purpose of classification of provided strategy by employing solitary layer feed forward neural network strategy is termed as Extreme Learning Machine (ELM). Mentioned strategy will be involved in mitigating the sluggish nature of learning with provided data set along with alleviating the challenges with respect to over-fitting.Requirement of solitary step for providing the training process with data set using ELM that depends with minimization of experimentalerrors. Circumventing the numerous steps along with restricted reduction is observed in Extreme Learning Machine.Due to the improved simplification capacity strength, regulating along with rapid training duration is utilized in numerous arenas of applications.

3.2. Twin Extreme Learning Machines

A progress in the strategy of Extreme Learning Machine termed as Twin Extreme Learning Machines (TELM) considered in this paper. Implementation of the concept that was used in the Twin Support Vector Machine inside the organization of Extreme Learning Machine, subsequently emergence of fresh strategy called as Twin Extreme Learning Machine is established.Benefits observed in the techniques Twin Support Vector Machine along with Extreme Learning Machine will be exploited in TELM technique.Improved prediction accuracy along with variables contained least conditions involved in the determination of best solutions is observed in TELM while relating with TSVM.With the aim of providing the training by utilizing selected characterization for categorization of data, utilization of two non-concurrent isolation hyperplane is observed in the operation of Twin Extreme Learning Machine utilizes.Minimization of distance with respect to any category out of available two category is the prominent operation of TELM along with it requires the placement the selected category farther with respect to additional category with in each hyperplane. Permission provided by TELM with respect to consideration of tolerable fault occurrence with the help of reducing the formularization variable combinedly while performing the process of training with the motivation of mitigating the challenges related to over fitting.Minimization of faults occurred during the process of training along with addition of squares with respect to distance pertaining to hyper place and any of categories will be the prominent objective of TELM. With the motivation of determining the best solutions, concurrent training of two Extreme Learning Machine at single instance by combinedly exploiting the advantages of both ELM along with TSVM.

3.2.1. Complete TELM Algorithm:

Summarized technique involved in operation of TELM approach is provided in the succeeding section

TELM Approach:

Provided the group of elements for performing the Training process $X = \{(x_i, t_i) | x_i \in \mathbb{R}^d,\ t_i = \{+1, -1\}, i = 1, \ldots N\}$, Operational Objective$G(\boldsymbol{x})$, along withquantity of concealedelements will be L.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

Step 1: Prepare the ELM frameworkby means*L* concealedelements utilizingarbitrary weight w_I along withbias$b$i,provided as input

Step 2: Develop A*and* ***B*** matrices that might be considered as input. Subsequently computation of concealed stage matrices U*and* ***V*** correspondingly with respect to proportional Twin Extreme Learning Machine, computation of matrices***R*** *and* ***S***, correspondingly in accordance with nonproportionalTwin Extreme Learning Machine

Step 3:

a) Development of convex Quadratic Permutation Polynomial with respect to proportional Twin Extreme Learning Machine

$$\max_{\alpha} e_2^T\alpha - \frac{1}{2}\alpha^T V(U^T U + \epsilon 1)^{-1}V^T\alpha$$
$$s.t.\, 0 \le \alpha_i \le c_1, i = 1, \dots m_2.$$

In addition, with

$$\max_{\gamma} e_1^T\gamma - \frac{1}{2}\gamma^T V(U^T U + \epsilon 1)^{-1}V^T\gamma$$
$$s.t.\, 0 \le \gamma_i \le c_2, i = 1, \dots m_1,$$

b) Development of convex Quadratic Permutation Polynomial with respect to non-proportional Twin Extreme Learning Machine

$$\max_{\alpha} e_2^T\alpha - \frac{1}{2}\alpha^T S(R^T R + \epsilon 1)^{-1}S^T\alpha$$
$$s.t.\, 0 \le \alpha_i \le c_1, i = 1, \dots m_2.$$

In addition with

$$\max_{\gamma} e_1^T\gamma - \frac{1}{2}\gamma^T R(S^T S + \epsilon 1)^{-1}R^T\gamma$$
$$s.t.\, 0 \le \gamma_i \le c_2, i = 1, 2 \dots m_1$$

Step 4: With the help of determining the solutions for two Quadratic Permutation Polynomial Acquire Lagrange multipliers α along with γ

Step 5:

a) Computation of weights β1 along with β2 corresponding to outputs with respect to proportional Twin Extreme Learning Machine

$$\beta_1 = -(U^T U + \in I)^{-1}V^T\alpha., \beta_2 = -(V^T V + \in I)^{-1}U^T\gamma\,.$$

b) Computation of weights μ1 along with μ2 corresponding to outputs with respect to non-proportional Twin Extreme Learning Machine

$$\mu_1 = -(R^T R + \in I)^{-1} S\alpha.\quad, \mu_2 = -(S^T S + \epsilon I)^{-1}R^T\gamma\,.$$

Step 6: Compute vertical distance pertaining to data point ***x*** with respect to isolating hyperplane

$$f(x) = \arg\min_{r=1,2} d_r(x) = \arg\min_{r=1,2} |\beta_r^T h(x)|,$$

Subsequently allocate x to category (*i*- +1, −1).

IV. EXPERIMENTAL RESULTS

NSL-KDD dataset is utilized for performing the experiments. 65535 samples contained in complete dataset 65,535 samples along with 100%, 50% and 25% of the samples are applied for the evaluation. There are 65535 samples in the original dataset, 50% of the samples are 32767 and 25% samples of original dataset are 18383 are used for the evaluation. Consideration of parameter which will involve in deciding the performance of suggested approach exactness, meticulousness along with recall will be listed as performance measures to evaluate the performance as described by the **Ahmad et al.** The entire dataset split in to two parts, randomly 80% of the samples are used tolearnin addition withbalance 20% of the illustrationswill beutilized inscrutinizing. The proposed TELM compared with the TSVM, SVM and Traditional ELM methods for performance evaluation.

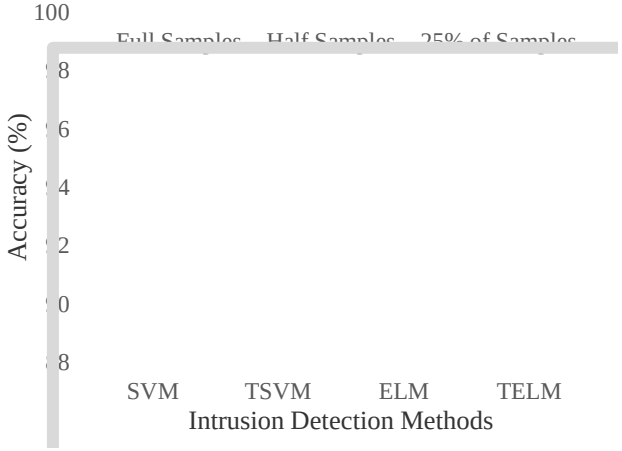

Fig 1. Accuracy Evaluation

The obtained accuracy values are plotted in the graph shown in Figure 1. It is observed the accuracy value of the proposed TELM is higher than the ELM, TSVM and SVM. Similarly, the obtained precision values are plotted in the Figure 2. It is observed the Proposed TELM gives better precision than ELM, TSVM and SVM for all the testing samples.

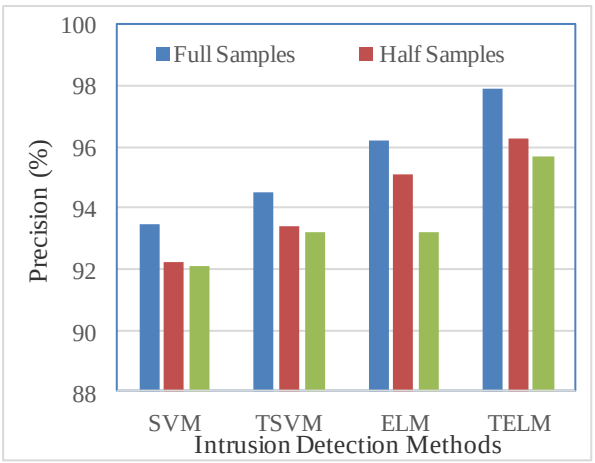

Fig 2. Precision for the Test Samples

The obtained recall value for the proposed TELM, ELM, TSVM and SVM are shown the Figure 3. It is observed that the TELM obtained the greater precision value than the other standard classifiers. From the evaluation results, superior functioning by utilizing Twin Extreme Learning Machine is observed when compared

with additional techniques such as Extreme Learning Machine Learning, Twin Support Vector Machine along with Support Vector Machine. The proposed TELM is one of the best alternative classification algorithms for the Intrusion Detection systems.

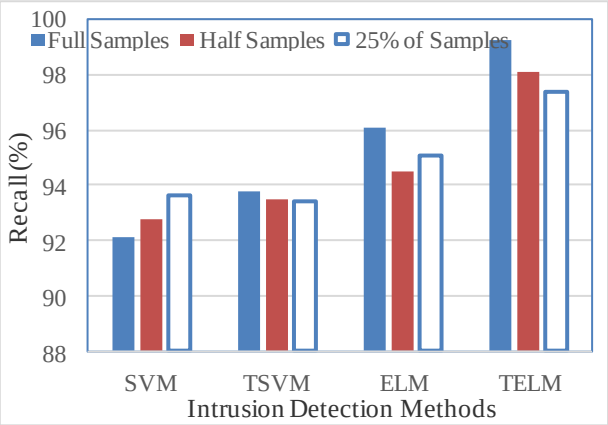

Fig 3. Recall Value Obtained for the Test Samples

V. CONCLUSION

Now a days Intrusions are very common in network systems. So, it is very important in securing the communication and data networks. In this paper, for identification of hacking activity pertaining to network suggestion of pattern classification algorithm termed as Twin Extreme Learning Machine was established. Several literatures have been proposed for intrusion detection on the other hand strategies that works with the principle of machine learning approachesprovided special attention as far as consideration of research.in this research. For the purpose of establishing the superiority of suggested system of Twin Extreme Learning Machine that performs the process of identification of hacking activity, comparison will be performed with certain standard machine learning classifiers namely, Support Vector Machine (SVM), Extreme Learning Machine (ELM) and Twin Support Vector Machine (TSVM). It is observed from the obtained results the proposed TELM classifier is one of the best alternative pattern classifiers for Intrusion detection systems. The performance can be further enhanced by optimizing the weights in the secondary layer during the learning phase of the classifier.

REFERENCES

1. Ahmad, I., Basheri, M., Iqbal, M.J. and Raheem, A., 2018. Performance comparison of support vector machine, random forest, and extreme learning machine for intrusion detection. IEEE Access.
2. Li, Y., Qiu, R. and Jing, S., 2018. Intrusion detection system using Online Sequence Extreme Learning Machine (OS-ELM) in advanced metering infrastructure of smart grid. PloS one, 13(2), p.e0192216.
3. Manekar, V. and Waghmare, K., 2014. Intrusion detection system using support vector machine (SVM) and particle swarm optimization (PSO). International Journal of Advanced Computer Research, 4(3), p.808.
4. Das, V., Pathak, V., Sharma, S., Srikanth, M.V.V.N.S., Kumar, G. and Nadu, T., 2010. Network intrusion detection system based on machine learning algorithms.
5. Zamani, M. and Movahedi, M., 2013. Machine learning techniques for intrusion detection. arXiv preprint arXiv:1312.2177.
6. Singh, J. and Nene, M.J., 2013. A survey on machine learning techniques for intrusion detection systems. International Journal of Advanced Research in Computer and Communication Engineering, 2(11), pp.4349-4355.
7. Mohammed, M.N. and Sulaiman, N., 2012. Intrusion detection system based on SVM for WLAN. Procedia Technology, 1, pp.313-317.
8. Hamid, Y., Sugumaran, M. and Journaux, L., 2016, August. Machine learning techniques for intrusion detection: a comparative analysis. In Proceedings of the International Conference on Informatics and Analytics (p. 53). ACM.
9. Yao, J., Zhao, S. and Fan, L., 2006, July. An enhanced support vector machine model for intrusion detection. In International Conference on Rough Sets and Knowledge Technology (pp. 538-543). Springer, Berlin, Heidelberg.
10. Mulay, S.A., Devale, P.R. and Garje, G.V., 2010. Intrusion detection system using support vector machine and decision tree. International Journal of Computer Applications, 3(3), pp.40-43.

AUTHORS PROFILE

Vivek Deivasigamani working as Assistant professor in science and humanities at Sri Krishna College of Engineering and Technology, Coimbatore
VivekDeivasigamani received the M.C.A and ME degrees in Computer Applications and Computer science and engineering from Anna University, Chennai, India,in 2008 and 2015, respectively. In2018, he received the PhD degree in computer Applications from Anna University, Chennai,India.His current research interests include Network Security,MachineLearning,software engineering and Data mining.He has organised and attended various national and international conferences.

Dr.K. Selvanayaki is working as an assistant professor in Master of Computer Applications,Tamilnadu College of Engineering. She Receivedher Master of philosophy from Alagappa university, Karaikudi, Tamilnadu, India and received her Master of Computer Application from BharathiyarUniversity,Coimbatore.Currently she is working as a lecturer in MCA Department,Tamilnadu College of Engineering, Coimbatore.

AnoorSelvi.C working as Assistant professor in Computer Science and Engineering at VSB College of Engineering, Karur. AnoorSelvi.C received the BE and ME degrees in Computer science and engineering from Anna University, Chennai, India,in 2009 and 2011, respectively. Her current research interests include Network Security, Machine Learning, software engineering and Data mining. She has organized and attended various national and international conferences.