IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, May 2023

Intruder Detection System

Nidhi Ganorkar, Reetika Vaidya, Sakshi Kapile, Yelisha Ingale, Prof. Z. I. Khan
Department of Computer Science Engineering
P.R. Pote College of Engineering and Management, Amravati

Abstract: *In the era of big data, with the increasing number of audit data features,* ***human-centred smart intrusion detection system (IDS)*** *performance is decreasing in training time and classification accuracy, and many SVM-based intrusion detection algorithms have been widely used to identify an intrusion quickly and accurately. This paper proposes the FWP-SVM-GA (feature selection, weight, and parameter optimization of support vector machine based on the genetic algorithm) algorithm based on the characteristics of the genetic algorithm (GA) and the* ***support vector machine (SVM)*** *algorithm. The algorithm first optimizes the crossover probability and mutation probability of GA according to the population evolution algebra and fitness value; then, it subsequently uses a feature selection method based on the genetic algorithm with an innovation in the fitness function that decreases the SVM error rate and increases the true positive rate. Finally, according to the optimal feature subset, the feature weights and parameters of SVM are simultaneously optimized. The simulation results show that the algorithm accelerates the algorithm convergence, increases the true positive rate, decreases the error rate, and shortens the classification time. Compared with other SVM- based intrusion detection algorithms, the detection rate is higher and the false positive and false negative rates are lower.*

Keywords: Human-centred smart intrusion detection system, support vector machine (SVM)

I. INTRODUCTION

In the last few years, with the rapid popularization of internet, network has become a very important and essential method of user's accomplishing relative business. However, as the great advantage that the rapid development of network technology has brought to our social life, the network economy is facing a not optimistic present situation.

With the development and popularization of information and network technologies, network information security is becoming more and more important. Compared with traditional network defences technology (such as firewalls), It is a common misunderstanding that firewalls can recognize and block intruders. A firewall is simply a fence around a network. A fence has neither the capability of detecting somebody trying to break in (such as digging a hole underneath or jumping over it), nor can differentiate somebody carry through the gate is allowed in. A firewall simply restricts access to the designated points in the network.

Intrusion Detection System is configured to respond to predefined suspicious activities. An IDS does not replace firewalls. Firewalls are must in any corporate security foundations. Intrusion Detection Systems identify attacks against networks or a host that firewalls is unable to see.

II. MOTIVATION

An Intrusion Detection System is used to detect all types of malicious network traffic and computer usage that can't be detected by a conventional firewall. This includes network attacks against vulnerable services, data driven attacks on applications, host-based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and malware (viruses, trojan horses, and worms). An IDS is composed of the following three components: Sensors: - which sense the network traffic or system activity and generate events. Console: - to monitor events and alerts and control the sensors, Detection Engine: - that records events logged by the sensors in a database and uses a system of rules to generate alerts from the received security events. There are several ways to categorize an IDS depending on the type and location of the sensors and the methodology used by the engine to generate alerts. In many simple IDS implementations, all three components are combined in a single device or appliance.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, May 2023

III. AIM

Intrusion detection allows organizations to protect their systems from the threats that come with increasing network connectivity and reliance on information systems. Given the level and nature of modern network security threats, the question for security professionals should not be whether to use intrusion detection, but which intrusion detection features and capabilities to use. IDSs have gained acceptance as a necessary addition to every organization's security infrastructure. Despite the documented contributions intrusion detection technologies make to system security, in many organizations one must still justify the acquisition of IDSs. There are several compelling reasons to acquire and use IDSs.

IV. PROPOSED WORK

To improve the accuracy as well as to reduce the risk of intrusion for the network or system this proposed system uses the concept of IP binding. In this apropos mechanism technique in which the regular IP address in the network will be consider in which the regular authentication system will get workout with network evaluation for the determination of the intruder. The undefined IP determination technique is used to speed up the intruder detection system by implementing the SVM verification with Meta data verification. The SVM algorithm first optimizes the crossover probability and mutation probability of GA according to the population evolution algebra and fitness value, then it subsequently uses a feature selection method based on genetic algorithm with an innovation in the fitness function that decreases SVM error rates and increases the true positive rates with highly configured authentication techniques. To perform evaluation mechanism in authentication of nodes and live performer evaluation and detection system implementation.

4.1 Proposed Concept

In this system there are number of nodes, this number of nodes are nothing but the networks. And the numbers of users, users are also known as systems which are connected into networks. All the users have IP address and all the nodes have their own ID. All nodes stores the IP address of their users into database. If any user send the message or any kind of data to another users from other network then their IP address will get check as well as all the data of that user will be verified for ex. Their transaction history. If IP address of the user is not match then there is risk factor for the network.

The data or message send by user to other user, that data will be send by encrypted manner. For the encryption AES i.e. Advanced Encryption Standard algorithm is used and for the decryption Secure Hash Algorithm i.e. SHA algorithm is used to increase the security. In the existing system, there was not any encryption and decryption concept of data. If the user has done so many transactions then by applying GA and SVM algorithm the fitness value will be calculated. On the basis of transactions and the fitness value the intruder will get detected. Fitness value is calculated by GA i.e. Genetic Algorithm. Fitness function is simply defined as a function which takes a candidate solution to the problem as input and produces as output.

4.2 System Architecture /Design

System implementation by using GA-SVM algorithms. The below diagram (fig.:01) shows the architecture of Proposed system.

It is observed that, there is two main modules Admin and User. Admin can create the nodes that is networks. And in that network admin added the users these users are noting but the systems which are present into the networks. When the users are registered itself admin allotted the nodes to that user. Also admin can update the node as well as users.

Now the Most important second module is user. User is a system which is present into node i.e. network. The user can send the data or message to another user that user can be within network or out of network. And the user received the data this received data is encrypted form, to encrypt the data AES algorithm is used. To decrypt that message SHA algorithm is used. By applying SHA algorithm message is decrypted and user gets the original message. After receiving message to check whether the message is received from intruder or not user can apply the GA-SVM algorithm on that message that verify the node as well as IPs to generate the prediction.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, May 2023

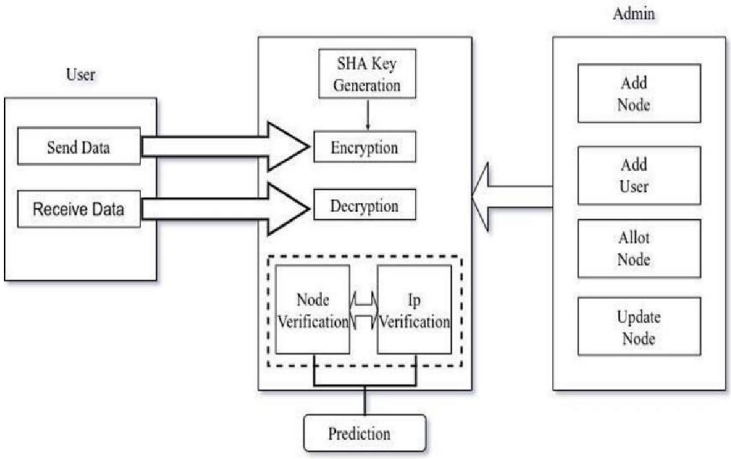


Fig. 01Architecture of Proposed system

With the help of GA-SVM algorithm the user can apply multiple functions like, initial population, initial population shows received message from which node and its IPs. Apply classification and mutation, this function shows on which node data is received also their network status that means weather the message is received from same network or different network. The another function is crossover and mutation, this function is used for to indicate node which send the message also there number of transaction in other words, it shows that ,how many transactions happens from same nodes and calculate its fitness value. The last option is IP filtration, IP filtration is used to check the IPs of a system and verify that weather this IP is stored in our database if yes then how many transactions are happened from the same IP and calculate its fitness value. On the basis of that fitness value this algorithm gives the final prediction that this is risk detected or safe.

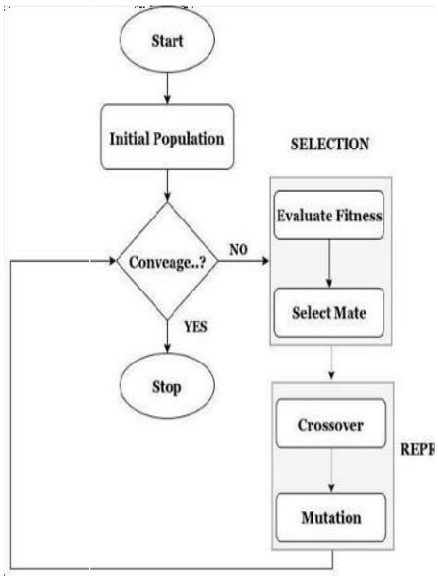
On the basis of GA-SVM algorithm all the details about the message and the nodes is shown. And can predict that, whether there is any risk from that message or not.

4.3 Working of proposed system

There are some algorithms which are used into the current system.

GA (Genetic Algorithm):

Genetic Algorithm is belonging to evolutionary algorithm. GA is an adaptive heuristic search algorithm which means this algorithm is adapted with respect to the changing environment. The most important thing about the GA is, this algorithm is based on genetics and natural selection.



IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, May 2023

The actual working of the GA is, it is used to generate the high-quality solution for optimization problem. This algorithm generates the best optima of any search problem. There are two main terms of a GA is population and individuals. Individuals is just considered as a possible solution for the given problem by GA. And the collection of individuals is called as population and such a population of a individuals is maintain within a search space.
There are four operators of GA. First is selection, selection operator is used for to select the fittest individual for the mating process. Second is crossover, this operator is used to reproduction to generate the new offspring. Third operator is mutation, mutation is used to alter some gene. And the last operator is encoding.

V. CONCLUSION

A system for intrusion detection is implemented which is based on genetic algorithm (GA) and support vector machine (SVM) for the use of human centered smart IDS. This system makes the effective use of genetic algorithm population search strategy and the capability of information exchange between two individuals by optimizing the crossover probability and mutation probability of GA. The convergence of the algorithm is accelerated and training speed of SVM is improved. A new fitness function is proposed that can decrease the SVM error rate and increase the true positive rate. On the basis of data transaction fitness value is calculated in proposed system and the prediction about intruder is generated and this prediction is alert the user so that any kind of attack will not occur. The results are discussed in result section and found satisfactory.
A system for intrusion detection is implemented which is based on genetic algorithm (GA) and support vector machine (SVM) for the use of human centred smart IDS. This system makes the effective use of genetic algorithm population search strategy and the capability of information exchange between two individuals by optimizing the crossover probability and mutation probability of GA.
The convergence of the algorithm is accelerated and training speed of SVM is improved. A new fitness function is proposed that can decrease the SVM error rate and increase the true positive rate. On the basis of data transaction fitness value is calculated in proposed system and the prediction about intruder is generated and this prediction is alert the user so that any kind of attack will not occur. The results are discussed in result section and found satisfactory.

ACKNOWLEDGMENT

It is my utmost duty and desire to express acknowledgement to the various torchbearers, who have rendered valuable guidance during the preparation of my seminar. First of all, I extend my deepest gratitude to respected Principal, Dr. D. T. Ingole without whose support, my seminar could not have been transformed into present form.
I am grateful to Dr. V. B. Kute Head, Computer Science and Engineering Department, and my guide Prof. Z. I. Khan for providing immense support and guidance. I am beholden for guiding me at every step in the seminar. He/she has honestly guided me throughout, never leaving me unanswered for any of my doubts. It was his/her constant persuasion, encouragement, inspiration and able guidance that helped me in completing my seminar successfully.

REFERENCES

[1] Zinxin Sun, Peiying Tao, Zhe Sun, "An Improved Intrusion Detection Algorithm Based On GA and SVM." DOI 10.1109/ACCESS.2018.2810198, IEEE Access.

[2] A. Chaudhari, V. Tiwari, and A. Kumar, "A novel Intrusion Detection System for ad hoc flooding attack using fuzzy logic in mobile ad hoc networks," in recent Advances and Innovations in Engineering (ICRAIE), 2014. IEEE, 2014, pp. 1-4.

[3] S. Malhotra, V. Bali, and K. Paliwal, "Genetic programming and K-nearest neighbour classifier-based intrusion detection model," in cloud computing, Data science & amp; Engineering-Confluence, 2017 7th International Conference on. IEEE, 2017, pp. 42-46.

[4] R. Sen, M. Chattopadhyay, and N. Sen, "An efficient approach to develope an intrusion detection system based on multi-layer back propagation neural network algorithm: Ids using bpnn algorithm," in proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research. ACM, 2015, pp. 105-108.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, May 2023

[5] M. Tabatabaefar, M. Miriestahbanati, and J.-C. Gregoire, "Network intrusion detection through artificial immune system," in Systems Conference (SysCon),2017 Annual IEEE International. IEEE, 2015, pp. 1-6.

[6] T. Mehmood and H. B. M. Rais, "SVM for network anomaly detection using aco feature subset," in Mathematical Science and Computing Research (iSMSC), International Symposium on. IEEE, 2015, pp. 121-126.

[7] N. Chand, P. Mishra, C. R. Krishna, E. S. Pilli, and M. Govil, "A comparative analysis of svm and its stacking with other classification algorithm for intrusion detection," in Advances in computing communication, & Automation (ICACCA)(Spring), International Conference on IEEE, 2016, pp. 1-6.

[8] R. Vijayanand, D. Devaraj, and B. Kannapiran, "Support vector machine based intrusion detection system with reduced input features for advanced metering infrastructure of smart grid," in Advanced Computing and Communication Systems (ICACCS), 2017 4th International Conference on, IEEE, 2017, pp. 17.

[9] Q. Yang, H. Fu, T. Zhu, "An optimization method for parameters of svm in network intrusion detection system," in Distributed Computing in Sensor Systems (DCOSS), 2016 International Conference on. IEEE, 2016, PP. 136-142.

[10] Y. Gaung and N. Min, "Anomaly intrusion detection based on wavelet kernel is-svm," in Computer Science and Network Technology (ICCSNT), 2013 3rd International Conference on. IEEE, 2013, pp. 434-437.

[11] T. Yerong, S. Sai, X. Ke, and L. Zhe, "Intrusion detection based on support vector machine using heuristic genetic algorithm," in Communication System and Network Technologies (CSNT), 2014 Fourth International Conference on. IEEE, 2014, pp. 681-684.

[12] Z. Chen, T. Lin, N. Tang and X. Xia, "A parallel genetic algorithm-based feature selection and parameter optimization for support vector machine," Scientific programming, vol. 2016, 2016.

[13] K. S. Desale and R. Ade,"Genetic algorithm based feature selection approach for effective intrusion detection system," in Computer Communication and informatics (ICCCI), 2015 International Conference on. IEEE, 2015, pp. 16.