Intrusion Detection using IP Binding in Real Network

Vishakha R. Deshmukh[1], Dr. Sheetal. S. Dhande-Dandge[2]

[1]*Student, Department of Computer Science and Engineering, SIPNA COET, Amravati, Maharashtra, India*
[2]*Professor, Department of Computer Science and Engineering, SIPNA COET, Amravati, Maharashtra, India*

---***---

Abstract - *In the era of big data, with the increasing number of audit data features, human- centered 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.

***Key Words*: Genetic Algorithm, Support Vector Machine, SHA Algorithm, AES Algorithm, IPs, Nodes, Users.**

1. 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 defense 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. Having IDS to complement a firewall can provide an extra layer of protection to a system such as-

- Identify attacks that firewall legitimately allow through (such as HTTP attacks against web servers)
- Identify attempts such as port scan
- Notice inside hacking
- Provides additional checks for holes/ports opened through firewalls intentionally or unintentionally. Intrusion Detection is a set of techniques and methods that are used to detect suspicious activity both at the network and host level. Using Intrusion Detection, we can collect and use information from known types of attacks and find out if someone is trying to attack our network or particular hosts. The information helps us to harden our network security, as well as for legal purposes.

1.1 What is Intruder?

An intruder is a person who attempts to gain unauthorized access to a system or network to damage that system or network. This person attempts to violet security by interfering with system availability, data integrity or data confidentiality.

Intruder always trying to gain access to a system or network with his criminal intentions. Once he gains access to that system or a network he will corrupt or steal the complete data from the system or network and imbalance the environment of a network

Types of Intruder:

There are two types of intruders:

➢ **Outside Intruder (Masquerader):** Pretend to be someone one is not an individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account. Outside intruder actually not having any authorized access to the system or to the network therefore this intruder is always try to gain the access using different techniques like, stealing credentials or break the credentials of a systems or network and once intruder gets that credentials then with the help of that credentials intruder can easily enter inside the system or network and can penetrate to that system or network.

- **Inside Intruder (Misfeasor):** Authentic user doing unauthorized actions. A legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges. Inside intruder having some having some authorized access to the system or to the network but with some restrictions. Some privileges and resources are provided to that intruder and by using this privileges and resources intruder provides the confidential information or the data from the system or network to the other network. Inside intruder is more harmful than outside intruder because it is very difficult to identify inside user.

1.2 What is Intrusion?

Intrusion is unauthorized access by intruder or misuses of computer system or a network. In other word we can say that, intrusion is a harmful action taken by intruder with the criminal intention that is what the intrusion is. The intrusion is done by particular intruder. And this intrusion we have to detect using IDS.

1.3 What is IDS?

IDS stands for Intrusion Detection System which is a device or an application used to do the surveillance of network or systems for any insecure activity. A report is made that is sent to the administrator by the application or the information is collected and stored in the event management system. IDS mainly monitor network traffic so that Malicious activity can be spotted easily. It scans the network or the system to check the policy breaching and informs the concerned authorities or applications.

An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. Any intrusion activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system combines outputs from multiple sources and uses alarm filtering techniques to distinguish malicious activity from false alarms.

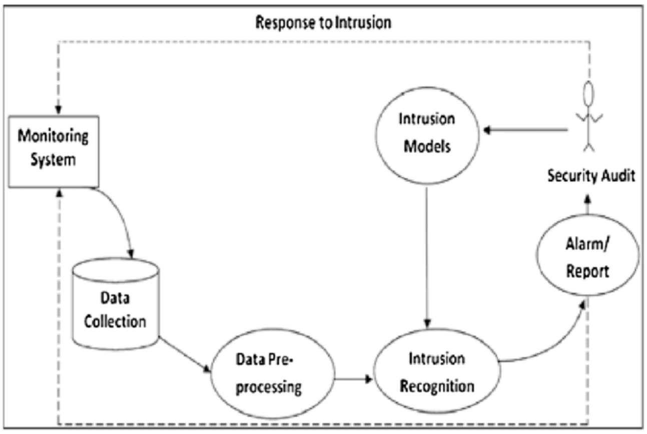

Fig -1: Overall Structure of IDS

However, the existing IDS often has a lower detection rate under new attacks and has a high overhead when working with audit data.

And thus machine learning methods have been widely applied in intrusion detection. Two algorithms are useful for detecting the intruders that are, SVM (Support Vector Machine) and GA (Genetic Algorithm).

Compared with other classification algorithms, SVM can better solve the problems of small samples, nonlinearity and high dimensionality. However, with the advent of the era of big data, SVM encounters the problem of long training and testing times, high error rates and low true positive rates, which limit the use of SVM in network intrusion detection. Therefore, SVM feature selection, feature weighting and SVM parameter setting are critical to improved detection performance. GA shows excellent global optimization ability via population search strategies and information exchange between individuals. Different from the traditional multi-point search algorithm, GA can easily avoid local optima GA and SVM are used to select the optimal feature subset and optimize the SVM parameters and feature weights to improve the performance of the network intrusion detection system.

For these reasons, the combination of the genetic algorithm (GA) with support vector machine (SVM). First, we optimize the crossover probability and mutation probability of GA, generate the population to speed up the search in the early evolution of the population and accelerate the convergence of the algorithm in the later evolution of the population.

In the stage of optimal feature set selection, a new fitness function is proposed to decrease the error rate while increasing the true positive rate. Finally, the feature weights and parameters of SVM are optimized simultaneously. And the robustness of SVM is improved. To address the problems, we use GA technology to supply fast and accurate optimization that can enable IDS to find the optimal detection model based on SVM.

2. Literature Survey

As network attacks continue to raise, better forms of intrusion detection and prevention are needed. Intruder Detection System has become standard component in security infrastructure as they allow administrator to detect policy violations.

Zhixin Sun [1] presented the intrusion detection has become the most important topic in security infrastructure. This paper makes effective use of the GA population search strategy and the capability of information exchange between individuals by optimizing the crossover probability and mutation probability of GA. The convergence of the algorithm is accelerated, and the training speed of the SVM is improved. To distinguish between attack and normal network access, different machine learning methods are applied in IDS, including fuzzy logic [3], K nearest neighbor (KNN) [4], support vector machine (SVM), artificial neural network (ANN) [5], and artificial immune system (AIM) approaches [6]. SVM showed better performance than traditional classification techniques [7], and several researchers proposed SVM-based IDS [8–10]. Although SVM-based IDS can improve IDS performance in terms of detection rate and learning speed compared with traditional algorithms (such as neural networks), room for improvement still exists. As the number of features of the audit data becomes larger, the performance of IDS degrades in terms of training time and classification accuracy. To address these problems, we use GA technology to supply fast and accurate optimization that can enable IDS to find the optimal detection model based on SVM. In [11], the genetic algorithm (GA) was proposed to improve the intrusion detection system (IDS) based on support vector machine (SVM), and the optimal feature subset was selected for SVM. However, the error rate of SVM was not considered. In [12], an intrusion detection method based on wavelet kernel least square was designed to improve the detection capability of SVM in complex nonlinear systems. However, the training and testing time of the algorithm is relatively long. In [13], the heuristic genetic algorithm was applied to optimize the SVM kernel parameters. The genetic operator is dynamically adjusted via a heuristic strategy, and the classification accuracy of the model is taken as the objective function to realize parameter optimization of the Gaussian kernel-based SVM classification model. However, this approach did not consider the impact of feature weighting on SVM detection accuracy. In [14], the coarse-grained parallel genetic algorithm (CGPGA) was presented to simultaneously optimize the feature subsets and parameters of SVM. A new fitness function was proposed that includes the classification accuracy, the number of features and the number of support vectors, but it required a long time to train the SVM. In [15], GA was selected as one of the most powerful tools to search in a large space with the potential to find the best solution in the search space. However, in the later evolution of the population, a larger crossover and mutation probability might result in the loss of good genes and delayed convergence of the algorithm.

3. Analysis of Problem

3.1 Earlier System

In the existing system of intruder detection the predefined data-set is used for the evaluation in which not exact detection is applicable and it is time consuming because in GA and SVM record evaluation get performed on huge amount of data-set and server log so that it is necessary to go with system which will make the detection possible in live way and help the users to be safe in all mode.

In earlier system, many SVM-based intrusion detection algorithms have been widely used to identify the intrusion quickly and accurately. 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. But in this earlier system, it does not keep the data about transaction of files or packets from one network to another. And here no IP concept is used. This system detects the intruder on the basis of fitness value which is generated with by genetic algorithm.

3.2 Proposed Design

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. 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. System Design

System implementation by using GA-SVM algorithms. The below diagram shows the architecture of Proposed system.

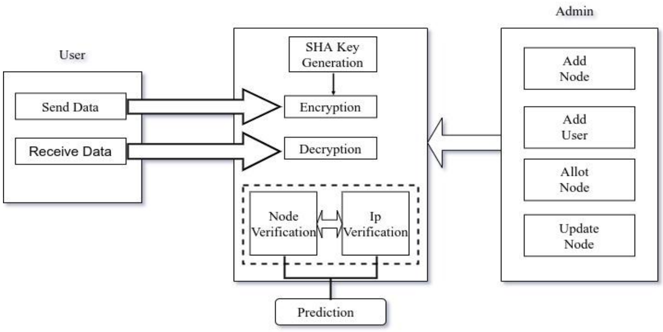

Fig -2: Proposed system Architecture

It is observe 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.

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.

4.1 Methodology

There are some algorithms which are used in current system:

GA (Genetic Algorithm): Genetic Algorithm is belongs 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.

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 consider 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.

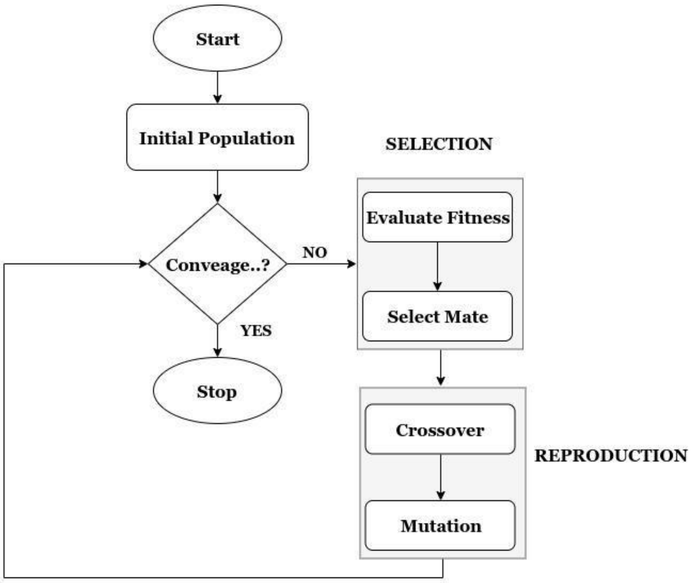

Fig -3: Flow chart of GA

SVM (Support Vector Machine): "Support Vector Machine" (SVM) is a supervised machine learning algorithm which can be used for both classification and regression challenges. However, it is mostly used in classification problems. In this algorithm, we plot each data item as a point in n-dimensional space (where n is number of features you have) with the value of each feature being the value of a particular coordinate. Then, we perform classification by finding the hyper-plane that differentiate the two classes very well.

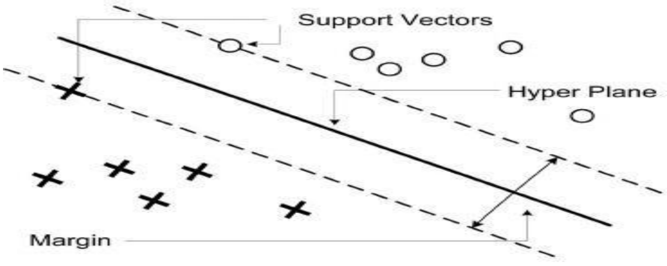

Fig -4: Support Vector Machine

Support Vectors are simply the co-ordinates of individual observation. Support Vector Machine is a frontier which best segregates the two classes i.e. Hyper-plane. Here, maximizing the distances between nearest data point (either class) and hyper-plane will help us to decide the right hyper-plane. This distance is called as Margin.

AES (Advanced Encryption Standard): The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES), it treats every 128 bits of blocks into a 16-byte segment. Every 16-byte segment gets settled as 4 and 4 bytes matrix. The length of the key determines the number of rounds involved.

Being the Advanced Encryption Standard (AES), a key standard for cryptography is in the process of data encryption and privacy. Advanced Encryption Standard acts as the most popular cipher and used for a wide range of applications comprising even the US Government use AES for ensuring data privacy and security. Advanced Encryption Standard(AES) is that is symmetrical and stands away from the stream cipher where each character is encrypted one at a moment. symetricity means the same kind of keys is used in the encryption process. It is also very robust for hackers because of its large key sizes. The key sizes used here are very higher as like 128, 192 and 256 bits for encryption. Commercially his cipher protocol is among the most widely used ones all around the world.

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations). Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix.

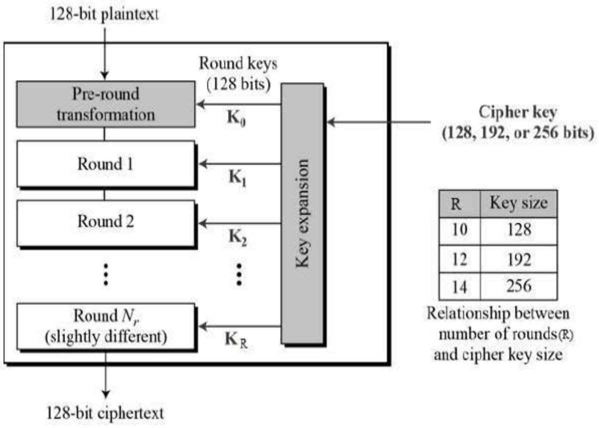

Fig -5: AES Structure

SHA (Secure Hash Algorithm): Secure Hash Algorithms. Secure Hash Algorithms, also known as SHA, are a family of cryptographic functions designed to keep data secured. It works by transforming the data using a hash function: an algorithm that consists of bitwise operations, modular additions, and compression functions.

SHA algorithm is Secure Hash algorithm developed by National Institute of Standards and Technology along with NSA, previously released as a Federal Information Processing Standard, later in 1995, it was named as SHA algorithm, design to modify the MD4, in other words, we can say that the SHA algorithm is the modified version of MD4. SHA is designed to obtain the original message, given its message digest and to find the message producing the same message digest.

In the field of cryptography and crypt analytics, the SHA-1 algorithm is a crypt-formatted hash function that is used to take a smaller input and produces a string which is 160 bits also known as 20-byte hash value long. The hash value therefore generated is known as a message digest which is typically rendered and produced as a hexadecimal number which is specifically 40 digits long.

The SHA or secured hash algorithm is aimed to provide an additional level of security to the increasing and the massive data you have to deal with. Hackers and attackers will keep finding vulnerability in all the newer forms of hashing techniques being used. We just have to ensure that we are prompt enough to be more secure than letting our data fall prey to it. Hope you liked our article. Stay tuned for more articles like these.

5. Implementation

Flow diagram of implementation is as follows:

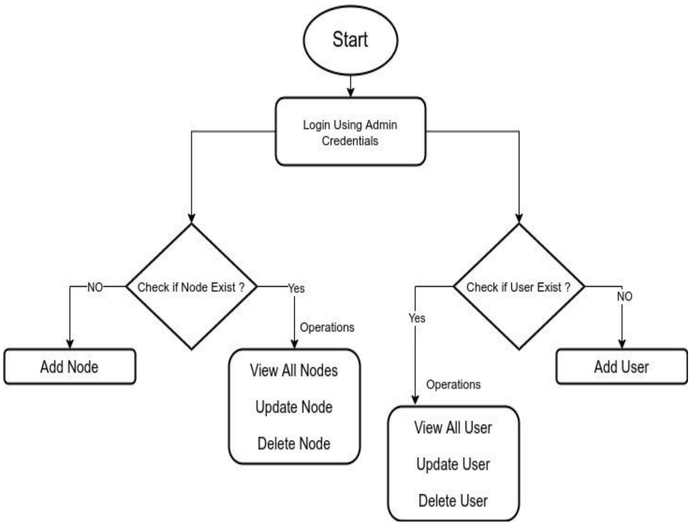

Fig -6: Flow chart of Admin

The above flow chart shows the flow of project where the admin first login with their credentials i.e. username and password. Then admin check whether the nodes are available or not. Node is nothing but the network. If there are no any nodes available then admin creates the new node or add the new node.

If the nodes are available then admin perform some operation with the present node. The operations which are performed by admin on the nodes are, update node where admin change the information about node and store that updated information. Next operation is, delete node where the node get removed permanently. Also admin can check all the information about node.

The next task or the work of admin is, admin can perform some operation with users as well.

After the admin login, admin checks is there any users are available or not. Users are nothing but the systems which are connected or present into networks i.e. node. If there is no any users are present then admin can add the new users and the users are get added with their proper registration i.e. by filling the complete information about new user and then add this user.

And if there is already users are available then admin can perform some operation on the available users. The operation performed by admin with users are, first is add user this operation is for adding the new users. Next operation is update user where the admin can change the information about user. Also admin can remove the user as well. After updating, deleting and adding new user admin can view the information of users. The most important thing about admin is, after the admin login any operation can perform by admin i.e. admin can perform the operations first with either user or node.

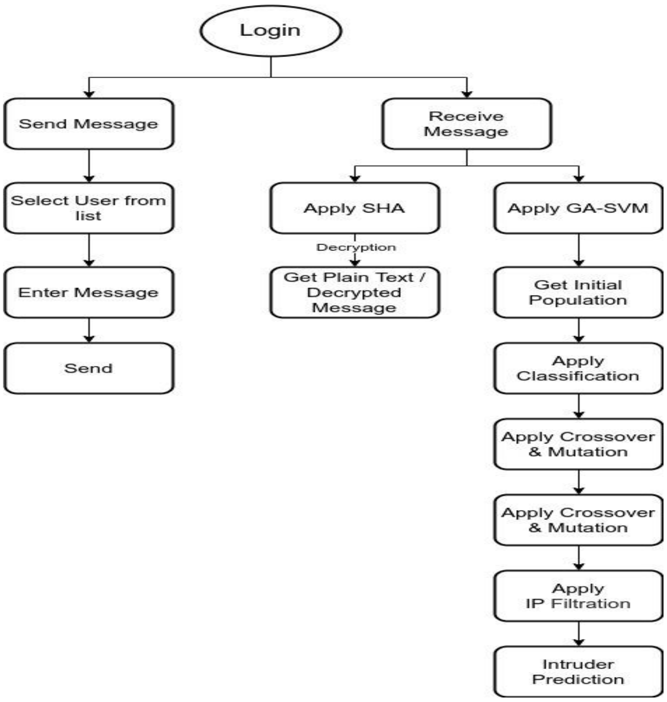

Fig -7: Flow chart of User

The above flow chart shows the flowchart of user where describes the complete working of user. After the logout of admin, user can login with their credentials that is user ID and password. After the user login the main task which can perform by users are, user can send the messages to the other users or can check the messages which are received from other users.

If user wants to send the message to the other user then first user who is sender must select the other user from the list to whom sender wants to send the message or any other data. After selecting user, sender type the message or enter the data and then click on the below button so that the data should send to the receiver or the selected user this is the complete process of sending message or data from one user to another.

The next most important task of user is received message, the data or message received by user then we can called this user is receiver the data or message received by receiver which is encrypted form. Then receiver can perform many operations on received message such as, apply SHA for decryption and get the plain text from encrypted message or data and then receiver can read the plain text.

Now the most important thing is, when receiver wants to check that, the message or data which received the receiver is send by intruder or not, for that verification receiver apply the very important function on that received message is GA with SVM.

GA with SVM can apply on the received message or data which will shows the initial population where receiver can check the sender's node and the sender's IP. After initial population the next function is classification, this function is used to show the node ID of sender, network status i.e. the sender is belonging from same network of receiver or not. If the sender and receiver having same node then the network status will be in-network. And if the sender and receiver both are belonging from different node then the network status will be out-network.

After classification the next function is crossover and mutation. After applying the crossover and mutation function the result will be node name of a sender, number of transactions that is how many messages received from same node, then calculate the fitness value which is calculated as, the total messages sent from node divided by total transaction done till. And on the basis of fitness value prediction is occur that is risk is detected or not. Next function is IP-filtration this is the last function provided by GA-SVM in this project.

After applying the IP-filtration function IPs of a user's will be filtered or we can say the IPs will be verified so that it will gives the final prediction that is the message is received is detect risk or not.

6. Result Analysis

In this project the data is encrypted with the help of AES algorithm. Encryption secures the information. Encryption is the process of converting the original representation of information, known as plain text into an alternative form which is known as cipher text. Only authorized person can decrypt the encrypted data into plain text and access the original information. The result of decryption where the encrypted data is converted into plain text so that the authorized user can access the original information.

The conversion of encrypted data into its original form is known as, decryption it is a reverse process of encryption. It decodes the encrypted information so that authorized user can only decrypt the data. In the current system SHA algorithm is used for the decryption process.

The final result of detecting intruder via node. Here the fitness value is calculated for every node so that we can identify that the intruder is belonging from which particular network. Fitness value is depend upon number of transaction occur from each node. If the transaction is more the fitness value of that node is greater. And on the basis of fitness value we can predict the intruder.

Fitness value calculation is as follow:

Fitness Value = *Total Number of Transaction from One Node / Total Number of Transaction from all Nodes*

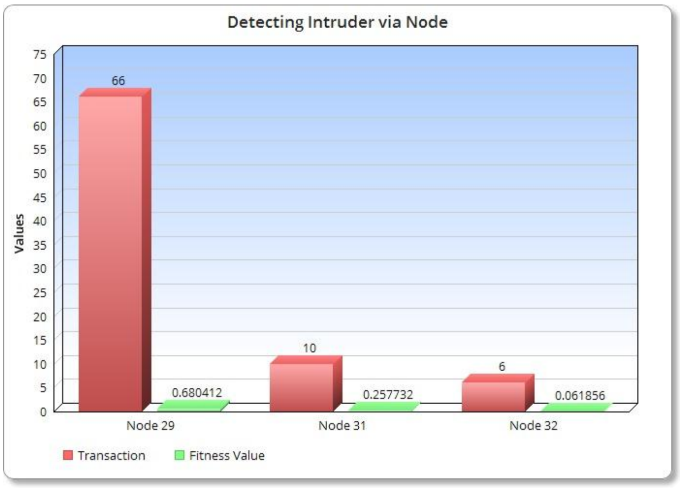

Fig -8: Graphical Analysis of Detecting Intruder via Node

Final result of detecting intruder via IP address. Each node contains number of users and every user contains unique ID. From every IP address there is some number of transactions is occurring. To detect the exact intruder we have to find the fitness value of each IP address.

If the transaction is more the fitness value of IP address is greater. And on the basis of fitness value we can predict the intruder.

Fitness value calculation is as follow:

Fitness Value = *Total Number of Transaction from One IP Address / Total Number of Transaction from all IPs from all Nodes*

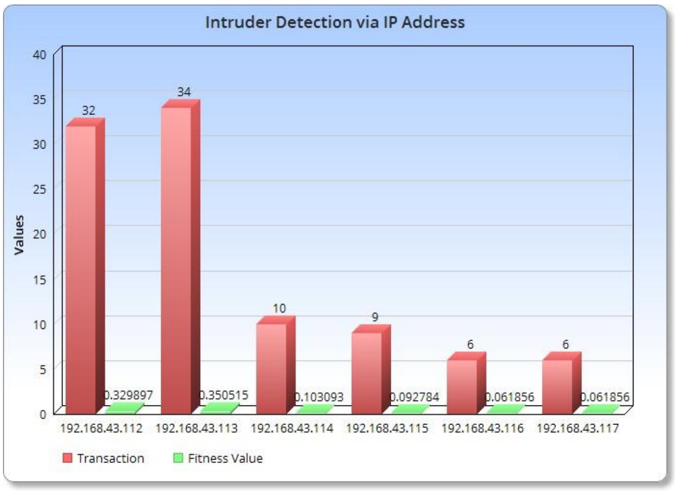

Fig -8: Graphical Analysis of Detecting Intruder via IP Address

7. 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.

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," 2014. IEEE, 2014,

[3] S. Malhotra, V. Bali, and K. Paliwal, Genetic programming and K-nearest neighbour classifier based intrusion detection model,"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.

[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, &amp; 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. 1-7.

[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. 1-6.

[14] W. Feng, Q. Zhang, G. HU and J. X. Huang, "Mining network data for intrusion detection through combining svms with ant colony networks," Future Generation Computer Systems, vol. 37, pp. 127-140, 2014.

[15] H. Gharaee and H. Hosseinvand, "A new feature selection ids based on genetic algorithm and svm," in Telecommunications (IST), 2016 8th International Symposium on. IEEE, 2016, pp. 139-144.

BIOGRAPHIES

Pursing M.E. Degree in Computer Science & Engineering, From Sipna College of Engineering and Technology, Amravati, Sant Gadge Baba Amravati University.

Dr. Sheetal S. Dhande-Dandge Professor & Head, Department of Computer Science Engineering & Technology Amravati, Executive Member, CSI Amravati Chapter. MCSI, FIETE, MIE, MISTE.