IJCSE International Journal of Computer Sciences and Engineering **Open Access**

Research Paper **Vol.-7, Issue-5, May 2019** **E-ISSN: 2347-2693**

Detection Of Cyber Attack Using Artificial Intelligence Based Genetic Algorithm With Feedback Ingestion

Jay Parag Mehta[1], Digvijaysinh M. Rathod[2*]

[1, 2] Institute of Forensic Science, Gujarat Forensic Sciences University, Gandhinagar, India

[*] *Corresponding Author: digvijay.rathod@gfsu.edu.in*

DOI: https://doi.org/10.26438/ijcse/v7i5.672678 | Available online at: www.ijcseonline.org

Accepted: 24/May/2019, Published: 31/May/2019

***Abstract*—** Strong intrusion detection is considered as a basic requirement for detecting any cyber attack before the breach yield successful outcomes for intruders along with automated prevention or response to such attacks being the next level of requirement. Although various tools and techniques are available for detecting such activities, intruders are still able to intrude heterogeneous environments successfully across the globe. This research work essentially takes the case of various models suggested in this direction, how they get deployed and what appears insufficient in their functioning making it difficult to be implemented. This research work focuses on developing improved models or improving existing models for designing and deployment of network security frameworks and policies, in which functioning of each component and their interconnectivity is taken towards more sufficiency to yield better actions thereby ensuring best possible level of security for all the system present within environment. The fitness functions for the system and which parameters could be used to decide genes for various network events is discussed along with a method to calculate the overall fitness of various network events.

***Keywords*—** Attack vector, Artificial Intelligence, Crossover, Cyber attack, Cyber Security, Feedback ingestion, Fitness function threshold, Gene, Genetic Algorithm, Intrusion Detection System, Machine Learning, Model, Mutation, Network Event, Network Packet, Network Security, Network Security Policy Framework, Selection, Self-evolutionary.

I. INTRODUCTION

Detection of malicious connections in computer networks has been a growing problem motivating widespread research in computer science to develop better system for detecting intrusion.

In this project, a machine learning approach is presented known as Genetic Algorithm (GA), to identify such harmful / attack type of connections. The algorithm takes into consideration different features in network connections such as type of protocol, network service on the destination and status of the connection to generate a classification rule base. Each rule in rule set identifies a particular attack type. When a new network event comes, the analyzer judges whether the event is secure or not according to the rule base, and the policy system may give a policy decision too. Obviously, these two results may be different. So, the policies could be automatically adjusted by considering genetic calculated results also.

A value-added feature is also included in this system - SMS alert - which helps administrator of the system to keep an eye on any possible intrusion and take immediate necessary action. This system could greatly help system administrators in network security policy management and prevent any outside intrusion thereby, avoiding change of network security policies. This way, the security of system within the environment could be ensured and extended to greater extent.

This research work could be classified under the domain of "Network Security" and within that, the classification could be further taken down to the sub-domain of "Application of Artificial Intelligence". The reason for such a kind of classification is because intrusion detection comes under the domain of "Network Security" which forms the core idea for this research work but, since Genetic Algorithm used for this research work depends on the fundamentals of "Artificial Intelligence", hence the further classification could be deemed justified.

Rest of the paper is organized as follows, Section II contains the purpose behind this research work, Section III speaks about the motivation behind this research work, Section IV mentions the need of this research work, Section V contains literature survey performed to gain understanding of Genetic Algorithm and allied concepts, Section VI explains the relevant work done by various field researchers, Section VII provides more insight into the proposed work and problem statement, Section VIII states the research work objective, Section IX informs the scope for this research work, Section

X describes the assumptions in this research work, Section XI states the constraints for this research work, Section XII explains the methodology used for this research work, Section XIII describe the implementation details along with expected scenarios, Section XIV presents the results and finally Section XV concludes research work with future directions.

II. Purpose

The main aim of this research work is efficient threat detection along with time optimization in detection, performance increase in terms of accuracy and automation in designing network security policy framework along with deployment of various policies. Experimentation has been done using real data set from available local and remote networks. Our work is carried out on client-server architecture type.

III. Motivation

To conduct any cyber attack, the intruder tries various techniques to breach any environment and gain entry into it. Then, the intruder would proceed towards gaining vital information that could be of help in compromising various security controls which would in place in that environment, to yield successful outcomes or gains from the attack. Thus, intrusion detection lies at the core, which also helps to rate the level of security for any environment. Hence, this strongly helps to further the core belief behind this research work that more faster and better the detection along with its timing, more is the window available to take the right steps in preventing further intrusion which could lead to a possible breach .

As Artificial Intelligence technologies are advancing and have much better role to play in intrusion detection, Genetic Algorithm being one such strong technique is made use of here, based on which various network security policy frameworks could be designed and implemented. However, existing models face challenges in terms of clarity about functioning of its components, which makes it difficult to be designed and implemented.

This has motivated the need for developing a strong network security policy framework. In this paper, a better model for security function is presented, which also helps in clarifying appropriate functioning of its components. The fitness function is examined for defining the genes of a network packet and a method to calculate fitness values is explained. Various types of attacks could be simulated and further, how these attacks get analyzed and prevented is discussed.

IV. Exigency Of This Work

In a complex network environment, new events are generated unpredictably on demand. Beside these new events, there are many events reporting system faults, status and performance information. Now, in such a vast network event environment, policies are usually created by administrator based on existing observations. But, there is also a possibility that security events might go unnoticed and administrator may fail to recognize, then how would the system handle such a situation? A traditional policy-based management and policy authoring system which rely on static authoring of “if [condition] then [action]” rules, becomes incapable. Also, for new and ambiguous situations these approaches fail to respond in systematic manner. Utility function, goal policies, and data mining and reinforcement learning, have emerged as new approaches.

Also in present scenario, to control / manage and update system security policies, manual intervention of administrator is required. This process becomes time consuming and many times it happens that administrator is unable to select the right policy at the right time.

These problems could be solved to a great extent using Genetic Algorithm for designing and deployment of network security frameworks and policies. Also, the system developed during the course of this research work could automatically detect intrusions and update policies as and when required. It works independently and does not require any outside support to counter new risks like other solutions, which require frequent updates of current threats to prevent them in the environment. SMS alert module integrated in this research work helps administrator in efficient management of security policies and to keep an eye on any possible intrusion.

This solution could be installed within any environment to monitor and manage the behaviour of network within that environment.

V. Literature Survey: Overview of Genetic Algorithm

To identify cyber attacks on any system within any environment has been a challenging problem in the domain of network security. Developing a solution for network security that has the power to predict and detect the type of incoming attacks other than identifying attack connections is being suggested. Amongst the different techniques available, “Genetic Algorithm” is selected.

Genetic Algorithm, a self-evolutionary algorithm, was invented to mimic some of the processes observed in evolution and natural selection. Many people, biologists included, are astonished that life at the level of complexity that is observed could have evolved in the relatively short time suggested by the fossil record. The idea for using Genetic Algorithm is to harness this power of evolution to solve such problems. These algorithms convert the problem in a specific domain into a model by using a chromosome-like data structure and evolve the chromosomes using following operators.

V.I Selection: During each successive generation, a portion of the existing population (individual genomes) is selected through a fitness evaluation process (called as fitness function) to breed a new generation.

V.II Crossover (also called recombination): This is a genetic operator used to combine the genetic information of two parents to generate new offspring.

V.III Mutation: This is a genetic operator used to maintain genetic diversity from one generation of a population of genetic algorithm chromosomes to the next wherein one or more gene values in a chromosome are altered from its initial state.

The father of the original Genetic Algorithm was John Holland who invented it in 1960 based on the concept of Darwin's theory of evolution; afterwards, his student David E. Goldberg extended Genetic Algorithm in 1989.

Initially, Intrusion Detection System were used to prevent intrusions, which was majorly the case of "if [condition] then [action]" rules. But, later on, when class and type of attacks and intrusions changed drastically, Genetic Algorithm was combined with network security policy frameworks to prevent system from attacks and intrusions in more efficient manner offering better security within the environment.

VI. RELATED WORK

Wei Li [5] had considered both temporal and spatial information of network connections in encoding the network connection information into rules in IDS. This is helpful for identification of various complex anomalous behaviour. This work was focused on the TCP/IP network protocols. This paper presented how network connection information was modelled as chromosomes and how the parameters in genetic algorithm were defined in this context as genes. It also described how to generate rule bases for improving the efficiency of the applied genetic algorithm by combining it with IDS.

Limitations: Wei Li [5] had provided theoretical overview about the idea presented which did not provide proper knowledge on the implementation aspects of any tool, technique or procedure. Also, architecture presented appeared insufficient in terms of providing a clear idea for implementation and the order of weights assigned to various network parameters appear challenging to adhere to due to lack of sufficient justification.

A.B.M. Alim Al Islam, Md. Ariful Azad, Md. Khurshid Alam, Md. Shamsul Alam [13] presented an approach of detecting the computer network security attacks (commonly termed as hacks). This work focused on improving fitness function (based on accuracy-existence-occurrence framework) to detect cyber attacks and developing security policy framework for taking necessary preventive actions. Also, they tested the algorithm using a simulation program in TC (Turbo C) to gauge its effectiveness and the side effects of its execution. The concepts of FPC (False Positive Count) and FNC (False Negative Count) were introduced to provide a new dimension for gauging the possibility of occurrence of any attack.

Limitations: A.B.M Alim Al Islam, Md. Ariful Azad, Md. Khurshid Alam, Md. Shamsul Alam [13] had mostly provided theoretical overview without sufficient details on implementation aspects of their idea. Also, ways to deduce major impact holder between FPC and FNC wasn't observed.

CHEN Xiao-su, WU Jin-hua, NI jun [14] presented usage of the Genetic Algorithm to the management of network security policy using a combined architecture with appropriate component functions / roles, discussed the evolution of Genetic Algorithm and the adjustment of security policy through feedback information and administrator interaction. This research work acted as a benchmark to take this idea further for development of some application around it.

Limitations: CHEN Xiao-su, WU Jin-hua, NI jun [14] did not put focus on assigning weights to various network parameters or introduce some technique to measure weights which could provide clues regarding the attack type and severity. Also, rule base management required improvements for avoiding duplicate rules and policy management required improvements for better integration with Genetic Algorithm and feedback modules.

Atish Mishra, Arun Kumar Jhapate, Prakash Kumar [17] presented an improved architecture for network security policy framework in which functioning of each component and there interconnectivity is explained in more depth. Focus point of this paper is to deal with the incoming malicious network packets and few important network parameters to be considered are brought to highlight.

Limitations: Atish Mishra, Arun Kumar Jhapate, Prakash Kumar [17] did not put focus on weight assignment or measurement of various network parameters which could help to determine the attack type and severity. Although this is a theoretical paper, directions to evaluate rule base and fitness function are not provided.

VII. Proposed Work

Intrusions are increasing and advancing from the technology angle for which timely detection and remedial action is a challenge. This is actually the point of motivation to find and develop techniques such that detection accuracy enhances to a great extent and likelihood of false positives and false negatives coming up becomes almost negligible.

There are many techniques and algorithms available out of which Genetic Algorithm is selected as it has a high potential of being successful in attack detection, once all the necessary data sets are in place, easily scalable with automation and also because it is based on the most naturally occurring phenomena known since ages.

The problem statement could hence, be further simplified and stated as an attempt to understand good and bad network packets with the help of Genetic Algorithm, decide on remedial actions and use this as a benchmark for developing network security policy framework as per requirement of individual environment.

VIII. Objective

Objective of this research work is: Incoming packets need to be sniffed and Genetic Algorithm operators need to analyze the policy changes performed by malicious packets. Policy change happening for the first time is detected, registered into rule base, administrator permission is taken and necessary auto-response is configured and saved, indicating that rule base is populated with sample attack data thereby strengthening detection capability along with the corresponding remedial action to be taken. Later on, policy changes happening any number of times are prevented based on this sample data set and SMS alerts are delivered to the administrator.

IX. Scope

Scope for this research work is: The test environment is limited to 2 laptop system running on Windows platform which are used to represent client-server type architecture. The application to detect packets runs on one of the system which behaves as a server while the other system is used to represent an intruder and behaves as a client. Windows Registry is used as a test bed to showcase policy changes performed by the intruder. Also, data set is limited and only few important network parameters are considered for this experimental purpose.

X. Assumptions

Assumptions for this research work are: Code developed for the application works without encountering any errors during real-time execution. Packets getting sniffed and captured by the application are stored in the database at the rate at which they are received without any packet getting dropped during transmission. Database connectivity for storing details about captured packets and mobile phone connectivity for delivering SMS alerts to the administrator do not get disconnected or go down. Packets sent from client to server simulate the real-world scenario of any intruder trying to break into any environment.

XI. Constraints

Constraints for this research work are: Evaluation version of Microsoft Visual Studio and Microsoft Office Suite are used. Application code is developed in C# and Microsoft Access is used as back-end database. Nokia PC Suite is used for pairing Nokia mobile phone with server system via Bluetooth. SMS alert is delivered from developed application to Nokia mobile phone via Bluetooth as licenses of proprietary tools, separate SMS Gateway hardware and official services (API code) for sending SMS messages are too costly. Initial data set is prepared for testing which is time consuming. SMS alerts just notify the administrator about unauthorized policy changes that happen.

XII. Methodology

XII.I Steps carried out to acquire and process, interpret inputs for this research work are: 1. Code was developed to extract information from the incoming packets and the necessary content was stored in the database. 2. These entries in the database, would provide future references for the Genetic Algorithm to generate population. 3. Since TCP, IP and UDP packet formats are widely used and known publicly, hence they are used here. 4. Sample IP packet contents from the data set are: (a) IP, (b) Ver, (c) Header Length, (d) Differentiated Services, (e) Total Length, (f) Identification, (g) Flags, (h) Fragmentation Offset, (i) Time to live, (j) Protocol, (k) Checksum, (l) Source, (m) Destination, (n) Date Value. 5. From the GUI-based front-end, inputs are taken from administrator interaction and incoming packets. 6. Fitness calculator used to study the different possibilities of incoming packet types by analyzing every detail of packets and evaluating their fitness. 7. Based on the fitness values, packets were allowed or disallowed in the system. 8. Later on, Genetic Algorithm works on those packets only, which were allowed to enter and harmed the system by changing policies of the system. 9. Whenever policy changes occur in the system, the administrator receives a SMS alert with the details of the policy changes that happened. 10. The policy changes would be rolled back and those packet entries get stored in the data set, to avoid further harm to the system in future. 11. After some time duration, the data set would have many entries of such malicious packets, indicating application is trained and data set is populated with sufficient scenarios which would help to take preventive action against such packets before they harm the system next time.

XII.II Steps carried out for research work are: 1. The required software on the server system was set up so that all the prerequisites are met to ensure compatibility across different hardware configuration. 2. Available software products in the market were used to install all required software and do the necessary compilations in a conflict-free manner. 3. For Genetic Algorithm, various operators applied are: (a) Selection, (b) Crossover (Single-point Crossover), (c) Mutation to generate some desired population. 4. Next that followed was the setting up and testing of the required data set, including its entries in the database. 5. Fitness calculator and policy management were worked upon and few policies were decided to be taken for this research work. 6. After all the above steps, the GUI-based front-end was developed which provided easy access to all of the required functionalities mentioned in above steps. 7. For testing purposes, LAN access was set up on the following devices: (a) DELL Inspiron 1545 Laptop, (b) DELL Inspiron 1564 Laptop. 8. For alerting the administrator, Bluetooth-enabled Nokia mobile phone was paired to the server machine. 9. Documentation stating various parameters and information related to the research work was prepared in a standard format.

XIII. Implementation

XIII.I Experimental Setup:

XIII.I.I Following software were used: 1. Operating System: Microsoft Windows XP Service Pack 2. 2. Front-end: Microsoft Visual Studio 2008 (.Net Framework 3.5 or above). 3. Programming Language: C#. 4. Database or Back-end: Microsoft Access. 5. Other Tools: (a) SMS Gateway, (b) Nokia PC Suite.

XIII.I.II Following hardware were used: 1. 2 laptops: (a) DELL Inspiron 1545 Laptop, (b) DELL Inspiron 1564 Laptop. 2. In-built High-Speed Ethernet or LAN Port or NIC Card. 3. Co-axial cable of CAT-5 with RJ45 connector each on both ends. 4. Bluetooth-enabled Nokia mobile phone.

XIII.II Implementation Procedure: 1. This research work was executed on the client-server environment. 2. Both laptops were connected through high-speed LAN ports. 3. No extra software was required to be installed on the client system. 4. The connection between both system was started and various types of packets (clean and malicious) were sent from the client system to the server system. 5. The policy changes due to malicious packets were viewed on the front-end console. 6. SMS alert was received by the administrator for policy changes that happened.

The console administration may give rise to various scenarios, some of which are mentioned within the sub-sub-sections of the next sub-section of this research paper.

XIII.III Expected Scenarios:

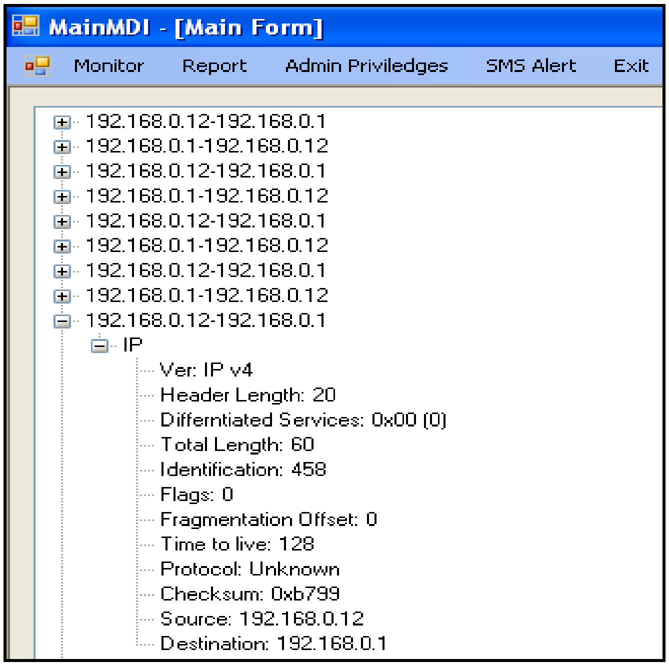
XIII.III.I View Packet Details Scenario: An administrator wants to sniff incoming packets and view their detailed information.

XIII.III.II Configure Policies Scenario: An administrator wants to define security policies for his system which need to be monitored.

XIII.III.III Enable System Protection Scenario: An administrator wants to prevent malicious packets coming from intruders and protect system from unnecessary harm.

XIV. Results and Discussion

After following the procedure mentioned in the sub-section "Implementation Procedure" from the section "Implementation" of this research paper, it was observed that packets were initially sniffed. Also, upon expanding the properties for any random packet, several properties were getting captured and recorded in back-end data set, that is, database (refer Figure 1 below).



```
⊞ 192.168.0.12-192.168.0.1
⊞ 192.168.0.1-192.168.0.12
⊞ 192.168.0.12-192.168.0.1
⊞ 192.168.0.1-192.168.0.12
⊞ 192.168.0.12-192.168.0.1
⊞ 192.168.0.1-192.168.0.12
⊞ 192.168.0.12-192.168.0.1
⊞ 192.168.0.1-192.168.0.12
⊟ 192.168.0.12-192.168.0.1
    ⊟ IP
        Ver: IP v4
        Header Length: 20
        Differntiated Services: 0x00 (0)
        Total Length: 60
        Identification: 458
        Flags: 0
        Fragmentation Offset: 0
        Time to live: 128
        Protocol: Unknown
        Checksum: 0xb799
        Source: 192.168.0.12
        Destination: 192.168.0.1
```

Figure 1: Packets getting sniffed in developed application. One random packet expanded to view various properties getting captured and recorded in data set.

Security Policy Frameworks were developed by leveraging few important configuration within Windows Registry (refer Figure 2 below) which could also be configured by the administrator as required, and changes performed by intruder in these policies were prevented using developed application. This implies that Genetic Algorithm studied network behaviour and using its operators, learned and matured the back-end data set to prevent same and new forms of attacks along with providing real-time reports and SMS alerts.

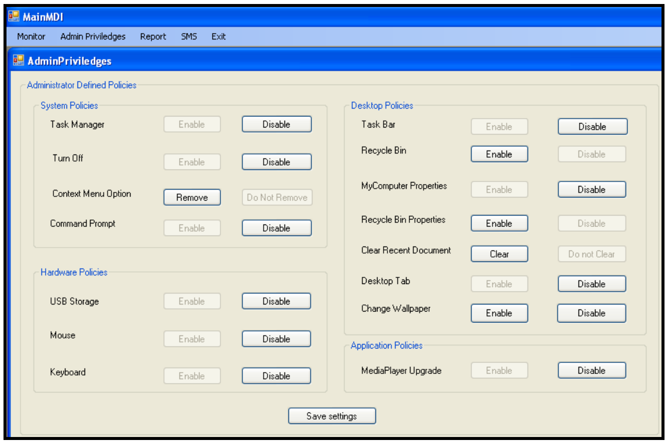
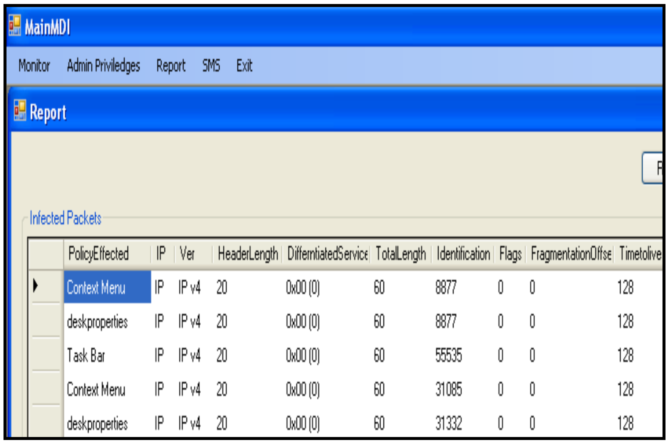


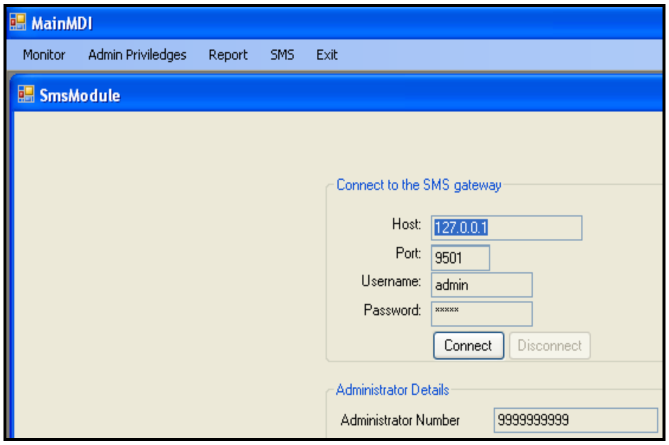
*Figure 2: Security Policy Frameworks developed by leveraging few important configuration within Windows Registry***.**

Security policies which were getting affected were visible to the administrator under reporting section on console such that the administrator could monitor for suspicious network events on real-time basis (refer Figure 3 below).



PolicyEffected	IP	Ver	HeaderLength	DiffernitatedService	TotalLength	Identification	Flags	FragmentationOffse	Timetolive
Context Menu	IP	IP v4	20	0x00 (0)	60	8877	0	0	128
deskproperties	IP	IP v4	20	0x00 (0)	60	8877	0	0	128
Task Bar	IP	IP v4	20	0x00 (0)	60	55535	0	0	128
Context Menu	IP	IP v4	20	0x00 (0)	60	31085	0	0	128
deskproperties	IP	IP v4	20	0x00 (0)	60	31332	0	0	128

*Figure 3: Security policies getting affected are visible to the administrator under reporting and this could be monitored live***.**



Host: 127.0.0.1
Port: 9501
Username: admin
Password: *****

Administrator Number 9999999999

Figure 4: Administrator could configure SMS alert settings.

SMS alert settings could be configured by the administrator as required, to receive SMS alerts for suspicious activities that could happen (refer Figure 4 above).

XV. CONCLUSION AND FUTURE SCOPE

Through this research work, an attempt at improving efficiency of attack detection has resulted in a fair amount of success. The purpose of this is to enable Intrusion Detection System to leverage the capabilities of Genetic Algorithm for designing and deployment of network security frameworks and policies across varied environments, which could be customized too.

The initial findings obtained from experimental setup have proved to be beneficial at this stage of the research work. The case of attack detection is taken into consideration for this research work where as, it could be expanded to include automatic remediation also for attacks which are detected successfully.

SMS alert mechanism could be improved to use licensed products for catering to huge environments. Also, specific commands could be worked and decided upon, which, being sent as a reply to threat alerts received via SMS, action should get validated, saved and executed by the application during situations when the administrator may not be physically present to act. Moreover, email-based alert mechanism could also be added.

Techniques should be developed for the following: 1. Assignment of appropriate weights to various network parameters for better outcomes from fitness function. 2. Bringing reduction in false positive count and false negative count 3. Integration between Genetic Algorithm and policy frameworks to be tightened further, such that, the system moves towards better stability in taking decisions on its own. 4. Provisioning support, integration and compatibility for upcoming protocols. 5. Populating data sets at a faster rate. 6. Efficient usage of selection, crossover and mutation operators. 7. Integrating other enterprise-wide security solutions and authentication mechanisms.

Also, attack remediation should be taken as the next step of improvement providing holistic approach. Tools and techniques should be developed to automate initial response to attacks thereby, improving the overall efficiency of the application to deal with various cyber attacks and ensuring security of the environment at best.

REFERENCES

[1] Leslie Pack Kaelbling, Michael L. Littman, Andrew W. Moore, *"Reinforcement Learning: A Survey"*, Journal of Artificial Intelligence Research, pp.**237-285**, **1996**.

[2] SU Pu-Rui, LI De-Quan, FENG Deng-Guo, *"A Host-Based Anomaly Intrusion Detection Model Based on Genetic Programming"*, Journal of Software, pp.**1120-1126**, June **2003**.

[3] Pohlheim, Hartmut, *"Genetic and Evolutionary Algorithms: Principles, Methods and Algorithms"*, Genetic and Evolutionary Algorithm Toolbox, 30 October **2003**.

[4] Mukkamala R., Chekuri L., Moharrum M., Palley S., *"Policy-Based Security Management for Enterprise Systems"*, International Federation for Information Processing: Research Directions in Data and Applications Security XVIII, Springer, Boston, MA, Vol.**144**, pp.**219-233**, **2004**.

[5] Wei Li, *"Using Genetic Algorithm for Network Intrusion Detection"*, Proceedings of the United States Department of Energy Cyber Security Group 2004 Training Conference, Kansas City, Kansas, **USA**, pp.**1-8**, 24-27 May **2004**.

[6] Jeffrey O. Kephart, William E. Walsh, *"An Artificial Intelligence Perspective on Autonomic Computing Policies"*, Proceedings of the Fifth IEEE International Workshop on Policies for Distributed Systems and Networks, Yorktown Heights, NY, **USA**, pp.**3-12**, 9 June **2004**.

[7] Arosha K. Bandara, Emil Constantin Lupu, J. Moffett, Alessandra Russo, *"A Goal-based Approach to Policy Refinement"*, Proceedings of the Fifth IEEE International Workshop on Policies for Distributed Systems and Networks, Yorktown Heights, NY, **USA**, pp.**229-239**, 9 June **2004**.

[8] Yao Jian, Sun Changping, Sun Hu, Mao Bing, Huang Hao, Xie Li, *"Research on Policy-Based Security Management"*, Computer Applications and Software, March **2005** (in Chinese).

[9] Chuanhuan Yin, Shengfeng Tian, Houkuan Huang, Jun He, "*Applying Genetic Programming to Evolve Learned Rules for Network Anomaly Detection*", International Conference on Natural Computation: Advances in Natural Computation, Springer, Berlin, Heidelberg, Vol.**3612**, pp.**323-331**, 27-29 August **2005**.

[10] Ryen W. White, Joemon M. Jose, Ian Ruthven, *"An implicit feedback approach for interactive information retrieval"*, Information Processing & Management, Vol.**42**, Issue.**1**, pp.**166-190**, January **2006**.

[11] Hoi Chan, Thomas Kwok, *"A Policy Based management System with Automatic Policy Selection and Creation Capabilities by using Singular Value Decomposition Technique"*, Seventh IEEE International Workshop on Policies for Distributed Systems and Networks, London, Ont., **Canada**, pp.**4-99**, 5-7 June **2006**.

[12] Anup Goyal, Chetan Kumar, "*GA-NIDS: A Genetic Algorithm based Network Intrusion Detection System*", **2007**.

[13] A.B.M Alim Al Islam, Md. Ariful Azad, Md. Khurshid Alam, Md. Shamsul Alam, *"Security Attack Detection using Genetic Algorithm (GA) in Policy Based Network"*, International Conference on Information and Communication Technology, Dhaka, **Bangladesh**, pp.**341-347**, 7-9 March **2007**.

[14] CHEN Xiao-su, WU Jin-hua, NI jun, *"Genetic-Feedback Algorithm Based Network Security Policy Framework"*, International Conference on Wireless Communications, Networking and Mobile Computing, Shanghai, **China**, pp.**2278-2281**, 21-25 September **2007**.

[15] Atish Mishra, Prakash Kumar, *"Storing Scheme for State Machine based Rule Base of Genetic Feedback Algorithm Based Network Security Policy Framework Depending on Memory Consumption"*, International Conference on Machine Learning and Computing, pp.**349-353**, **2009**.

[16] Atish Mishra, Arun Kumar Jhapate, Prakash Kumar, *"Designing Rule Base for Genetic Feedback Algorithm Based Network Security Policy Framework using State Machine"*, International Conference on Signal Processing Systems, **Singapore**, pp.**415-417**, 15-17 May **2009**.

[17] Atish Mishra, Arun Kumar Jhapate, Prakash. Kumar, *"Improved Genetic Feedback Algorithm Based Network Security Policy Frame Work"*, Second International Conference on Future Networks, Sanya, Hainan, **China**, pp.**8-10**, 22-24 January **2010**.

[18] Suhas B. Chavan, L.M.R.J. Lobo, "*Network Security policy framework and Analysis*", IJCA Special Issue on Network Security and Cryptography, pp.**55-58**, **2011**.

[19] Srinivasa K.G., "*Application of Genetic Algorithms for Detecting Anomaly in Network Intrusion Detection Systems*", International Conference on Computer Science and Information Technology: Advances in Computer Science and Information Technology. Networks and Communications, Springer, Berlin, Heidelberg, Vol.**84**, pp.**582-591**, **2012**.

[20] B. Uppalaiah, K. Anand, B. Narsimha, S. Swaraj, T. Bharat, "*Genetic Algorithm Approach to Intrusion Detection System*", IJCST, Vol.**3**, Issue.**1**, pp.**156-160**, March **2012**.

[21] Louis Mervin Rainey Joseph Lobo, Suhas B. Chavan, "*Use of Genetic Algorithm in Network Security*", International Journal of Computer Applications, Vol.**53**, Issue.**8**, pp.**1-7**, September **2012**.

[22] Khalid Jebari, Mohammed Madiafi, *"Selection Methods for Genetic Algorithms"*, International Journal of Emerging Sciences, Vol.**3**, Issue.**4**, pp.**333-344**, December **2013**.

Authors Profile

Mr. Jay Parag Mehta completed Bachelor of Engineering from University of Pune, Maharashtra (India) in the year 2012 and Master of Science from Gujarat Forensic Sciences University, Gujarat (India) in the year 2016. He is currently working as a professional in the Digital Forensics and Cyber Security industry. He is a member of the CyberAttack Community since 2014. He has published research paper in reputed international journal. His main research areas are Digital Forensics and Cyber Security (majorly Critical IT Infrastructure Security). He has 5 years of overall Industry Experience and 2 years of Research Experience.

Dr. Digvijaysinh M. Rathod completed Ph.D. in composition of RESTful web service from Ganpat University, Gujarat (India) and currently working as Assistant Professor (Cyber Security and Digital Forensics) in Institute of Forensic Science, Gujarat Forensic Sciences University since 2014. He has published more than 25 research papers in reputed international journals and conferences including IEEE. His main research work focuses on Web Application Security, Cloud Security, IoT Security, Darkweb Forensics and Block Chain. He has 15 years of Teaching and Research Experience.