An Effective Intrusion Detection Scheme over Wireless Communication Environment based on Artificial Intelligence Enabled Modified Learning Strategy

Jeyanthi D.V[1] & Indrani B[2]

[1]*Assistant Professor, Department of Computer Science, Sourashtra College, Madurai, Tamil Nadu, India.*

[2]*Assistant Professor and Head (i/c), Directorate of Distance Education, Madurai Kamaraj University, Madurai, Tamil Nadu, India.*

***DOI**: https://doi.org/10.34293/acsjse.v3iS1.91*

***Received Date:** 08.05.2023* ***Accepted Date:** 10.11.2023* ***Publilshed Date:** 02.01.2024*

Abstract - *based on Artificial Intelligence Enabled Modified Learning Strategy In this present digital world, each and every document need to be in system format as well as preserved into the server end. So, that the transactions between client and server entities are handled by using wireless communication schemes. There are millions of individuals hooked up to the internet enabled network today, and each of them possesses some level of sensitive information. Nowadays, the most valuable asset is knowledge about the organization or its users. This attracts the attackers or hackers to acquire the personal or private information from the server end or else the path that is used for communication. Numerous types of hackers attempt to penetrate a private system in order to obtain access and extract all critical data that could harm the infrastructure, posing a significant threat to the firm. These kinds of attacks are called intrusions and the attackers are termed as intruders. This paper has a detailed study of the past detection scheme and proposed a novel intrusion detection scheme to support users to prevent the data from intruders. The major objective of this paper is to design a novel Intrusion Detection System with full of attack handling and identification capabilities as well as prevent the data safe in server end without give a lead to intruders to make an attempt. The motto of this work is to introduce a modified learning strategy with respect to the conventional learning scheme called Artificial Neural Network (ANN) and provides a robust support and resistance to identify the intruders over the wireless communication environment. To make the users more convenient to preserve the data over the remote server environment and make transactions in secured manner with the help of the proposed learning scheme. These objectives are clearly illustrated with graphical representations over the resulting section of this paper.This paper introduced a modified learning scheme called Artificial Intelligence Enabled Modified Learning Strategy (AIeMLS), in which it provides a support to genuine network users to carry on with their private data as well as preserve the data over the server end without any threats. The proposed logic called AIeMLS is derived from the conventional learning scheme called ANN, in which it is composed of a number of processing components that accept inputs and generate outputs according to their predetermined activation functions and it is being used to characterize complex situations and to anticipate the contents of specified model parameters based on their learning data. By modifying the last layer of the ANN and adapt the logic of Support Vector Machine (SVM) into it to customize the model into a novel design. This is helpful to identify the intrusions in an intellectual manner with maximum level of accuracy and performance ratio.The proposed modified learning approach AIeMLS attains the maximum accuracy ratio of 98.5% in an outcome, whereas the other conventional algorithms such as ANN and SVM attain 98% and 96% accuracy in results. These resulting performance and efficiency is portrayed in the resulting section using graphical outputs.This approach of identifying the intrusions over the wireless communication environment is helpful to users in real-time environment and significantly preserves the data in proper manner. In future the work can further be enhanced by means of adding some crypto security features to enhance the security level more in the proposed work.*

***Keywords**: Intrusion Detection, ANN, AIeMLS, Network Security.*

I INTRODUCTION

Nowadays, the most critical resource for any business is information. Organizations now store data in order to process it on a network-based system for certain reasons. Due to the widespread usage of ecommerce, it is important to secure the firm's infrastructure. Security, authenticity and reliability are critical factors in the development of any Information Technology or programming application for any company [1]. The intrusion-detection-scheme can recognize as well as counteract many types of intrusions. Additionally, this could respond to threats that may arise in a communication networking enabled systems. While intrusion detection systems are critical in data protection, this is impossible to implement a framework without flaws.

A. System Analysis

Presently, almost everything in the world of communication and innovation is attempting to be computerized for the purpose of consistency and improved outcomes. Therefore, data is a crucial component of any business and t here are trillions of people using the internet worldwide as well as everyone of them possesses some level of confidential material. Nowadays, the most valuable asset is knowledge about the company or its consumers. Numerous cyber attackers attempt to penetrate a company's system in order to obtain permission and recover all critical data that might undermine the infrastructure, posing a significant danger to the firm. To ensure the security of a system, the Intrusion Detection Scheme (IDS) is an important factor but also it notifies the organization whenever somebody attempts to hack the system or network as well as also enables a means to deal with the attack. Numerous intrusion-detection techniques are employed, but they are also inadequate in several situations. Artificial Intelligence (AI) may play a critical role in securing the information management system and by combining Artificial-Neural-Network (ANN) and Fuzzy-Enabled architecture with learning analysis principle, AI will improve intrusion detection outcomes. This research analysis will attempt to distinguish between Intrusion Detection Schemes that do not use Artificial Intelligence and those that do, as well as the merits of utilizing Artificial Intelligence in the discipline of Intrusion-Detection-Scheme.

B. Intrusion-Detection-System

Intrusion-Detection-Schemes are vital aspects of contemporary software technology because they assist in monitoring and identifying harmful network connections (such as unauthorized access to the system or low maintained system configurations infrastructure). The preponderance of corporate Intrusion-detection-systems are signature-based, relying on characteristics in network activity to identify what represents unwanted internet traffic. While signature enabled Artificial Intelligence based detection techniques are extremely successful against imminent vulnerabilities, often fail while access routes are unfamiliar or when existing threats are changed to circumvent such restrictions [2]. Along with the difficulty of identifying unexpected or changed hazards, this AI based detection in intrusion detection scheme is commonly afflicted with wrongful convictions in authentic situations. This is especially dangerous and lead to detecting suspicious command shell - an identified critical

vector that allows intruders to gain unauthorized command prompt significant exposure to both conventional computing processes and cyber physical structures like SmartGrid environment - because executables styles can be complicated to discern from relatively harmless communications [3]. For instance, whereas planning to work as an internet backbone security professional for the Retail Precise Team and utilizing the intrusion-detection system techniques from the Ubuntu Linux - based operating protection, it was discovered that detection methods order to accommodate reverse shell commonly replicated on binaries as well.

Due to the high rate of these wrongful convictions, the characteristics actually would have to be deactivated, proving them ineffective. This situation with wrongful convictions in shell code and Artificial Intelligence enabled systems is rather frequent; Microsoft discusses it extensively in their intellectual property on techniques for detecting harmful shell-code with fewer wrongful convictions in storage [3]. Resulting in improved accessibility and influence that executable script provides an intruder, this is commonly utilized as a weapon in experiences related techniques [4]. The following Figure, Figure -1 illustrates the perception of proposed architectural design in clear manner with proper specification.

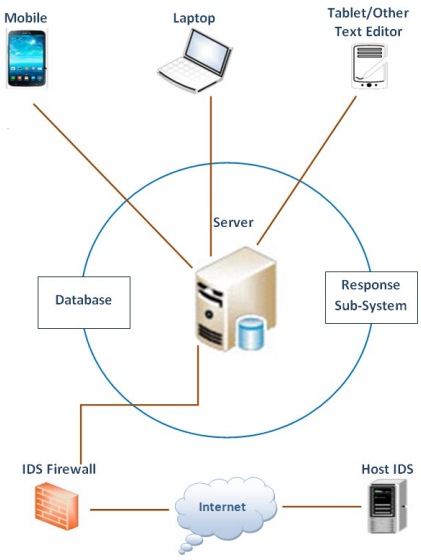


Figure 1: Proposed IDS Architectural View

This paper details a technique for detecting harmful command shell that is not signature enabled and is dependent on Artificial-Neural-Network (ANN). The offered outcomes demonstrate that this unique classification method is smart enough to recognize executables with a fair degree of precision as well as a low rate of misclassification. The proposed strategy of Artificial intelligence enabled scheme called Artificial Intelligence Enabled Modified Learning Strategy is validated through recurrent k-fold cross validation as well as then evaluated for positive result identifying issues by using a large - scale database of typical internet traffic information stored into the server. The basic objective of an Intrusion-Detection-Scheme is to determine when a direct attacker is aiming to disrupt a

functional requirement of the system. That really is, induce the technology to behave in a way that it would not be intended to. This might manifest as a breach of the software's security, accessibility and consistency, as well as the information it stores and controls. Servers, processors, connectivity devices, routers and other intermediate systems are all examples of structures [5].

Historically, security mechanisms have been separated into two main classifications, such as: host-based IDS and network-based IDS. The earlier is an isolated device identifying vulnerability, whereas the subsequent is a network of devices recognizing vulnerability in transmission [6]. Intrusion detection systems may be subsequently classified into methods that rely on neural networks and the associated systems that are based on signatures. Industrial network firewalls rely heavily on Artificial Intelligence enabled signature assisted patterns with outlier based solutions being primarily studies that were conducted [7] with just a limited provider instances. Alerts as well as other occurrence data given by IDS are rapidly being used as a fed into identity and access monitoring schemes, where they are combined with some other archives and streams to provide a more comprehensive portrait of a possible issue.

II RELATED STUDY

Chung-Ming Ou et al., proposed a paper related to the risk theory of the artificial immune system informs the design of an adaptive agent-based IDS (AAIDS). Because dendritic cells in immune systems identify and categorize danger signals, the AAIDS learning mechanism mimics this process. Instead of analyzing network packets, the AG, DC, and TC agents work together in concert to react immediately to system requests. The results of the simulations indicate that AAIDS is capable of identifying a number of important system behavior situations when packet analysis is not feasible [9].

Georgi Tsochev et al., proposed a paper suggesting that using intelligent techniques to increase computer network security, this article presents some of the findings made at the Faculty for Computer Systems as well as Technology at the Technical University of Sofia. Also, a study is being conducted on current hybrid cyber security techniques that use a variety of artificial intelligence technologies. Using basic real-time models developed in a laboratory setting, the article presents a model of intrusion detection systems based on multi-agent systems [10].

Kanimozhi et al., proposed a paper related to artificial intelligence (AI) that is a new developing technology that allows machines to imitate human behavior. The IDS is the most critical tool for detecting cyber assaults and other harmful activity (IDS). When it comes to intrusion detection systems (IDS), artificial intelligence (AI) is a game changer. Artificial-intelligence algorithms are becoming increasingly popular as a new computer approach that may be used to solve real-time problems. Artificial intelligence techniques like neural network algorithms are becoming more popular in contemporary times. Using the suggested approach, financial sectors as well as banking services would be protected against botnet attacks that represent a significant danger. An artificial intelligence-based cyber defense system is developed by applying AI to the most recent Canadian-Institute for Cyber security

(CIC) Intrusion Detection Dataset produced in 2018 on AWS (CSE-CIC-IDS2018) (Amazon Web Services). In the suggested Artificial Neural Networks system, the Accuracy score is 99.97 percent, the average area under the ROC curve is 0.999, and the average False-Positive rate is only 0.001 percent. The proposed system for Artificial Neural Networks offers an excellent performance. Artificial intelligence (AI) is being suggested for botnet attack detection since it is more powerful, more precise, and more accurate. For traditional network-traffic-analysis, cyber-physical system traffic data, and real-time network traffic analysis, the innovatively-proposed system may be implemented in n machines [11].

Kalaivani et al., proposed a paper related to the majority of swarm optimization methods are based on flock of bird traits and behavior, while Artificial Bee Colony mainly based on bee foraging characteristics. However, ABC's solutions to certain issues don't provide the intended outcomes when it comes to performance. ABC is a newly developed swarm intelligence method mostly used for numerical problem optimization. When comparing to other swarm-optimization methods, ABC has features like fathom-ability and flexibility, and there are several potential applications for it. The applicability and usefulness of cloud computing are both constrained by the technology's inherent limitations. Several security problems, such as Dos attacks, replay attacks, and flooding attacks, occur often in the cloud computing environment. This article proposes a useful classifier for cloud computing based on an Artificial Bee Colony. The assessment results clearly show that the suggested classifier has a better accuracy rate than the current classifier [12].

Mohammed Ishaque et al., proposed a paper suggesting that it is possible to utilize computer intelligence to intelligently handle huge amounts of data utilizing Deep Learning, a Machine Learning study field. A completely trainable system, a deep-learning-system starts with raw input and ends with identified objects as its final output. In order to reduce the dimensionality or reduce the number of attributes, feature selection may be used. This helps make the information more clear and accessible. Deep learning is capable of constructing a variety of learning models that could also abstract hidden information by focusing on a small selection of relevant characteristics. When dealing with invasive data or data moving inside a web network or system, deep learning's characteristic of detecting anomalies makes it helpful in the analysis of extremely complicated information. In order to create a clever Intrusion detection system, we combined the intelligent capacity of Deep Learning with our methodology [13].

III METHODOLOGIES

This paper introduced a novel learning-based Intrusion identification methodology called Artificial Intelligence Enabled Modified Learning Strategy (AIeMLS), in which it identify the intrusion by using the conventional algorithm such as Artificial Neural Network support. The reason for implementing artificial intelligence is to build and construct an Innovative intrusion detection mechanism that properly determines "false-alarms" or very few "false-alarms," that cannot be readily tricked by minor pattern variations, and operates in real time. Intelligent Intrusion Detection System is not only capable of detecting intrusions; it is also capable of acknowledging potential attacks and predicting new threats based on earlier

common threats. The overall purpose of incorporating Machine learning and artificial intelligence into the system proposed to detect intrusion is to design a method able to distinguish between various assortments of assaults in a distributed system. Out of many machine learning techniques the Artificial Neural Network has subset that is motivated by the activity of biological neural networks inside the central nervous systems. Generally, signals to the ANN are delivered everything into several hidden layers, in which they are evaluated and handled to determine the outcome towards the subsequent phase. ANNs employ a "transfer learning" (typically stochastic conquest back propagation of faults) that enables dynamic tuning of the collection of network weights for the convolution layer and output vector cells. Considered to be self structure analysis, ANNs are useful for quickly detecting very complicated and complex connections between interdependent and random parameters. ANNs have been applied to a broad range of classification techniques across such a large number of application fields. In connection to the classification models like multiple regression and regression models that should have a depth knowledge in data generated by system in probabily, Here the fundamental framework of system is required because it adopts technique of “black box” for ANN.This plays a vital role in disciplines including planning strategically for finding hidden weapons,predicting Internet traffic,verifying signature because they have ability to adapt huge datasets,also it helps to ease the difficulties in model building for different classifiers like k-nearest neighbouring and decision tree methodologies. ANNs are most often used in a wide range of computer networks, such as the assessment of web application structural flaws and malware scanning. ANN-based strategies to accurately detecting kinds of network attack vectors have indeed been demonstrated to be efficacious, but while their implementation to shell code identification wasn't really presumed.This Figure, Figure - 2 explains the proposed approach of the logical block diagram.

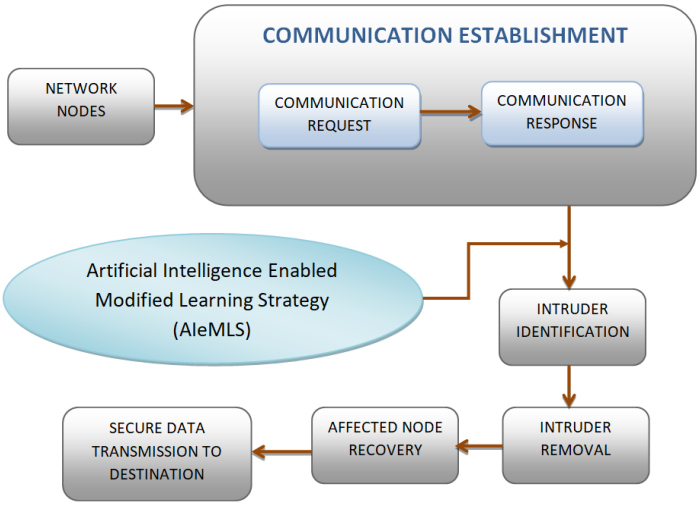


Figure 2: Proposed Approach Block Diagram

In two distinct ways, fuzzy set theory may assist intrusion detection mechanism. Initially, many characteristics utilized in attack detection, like Central Processing Unit (CPU) and memory time, knowledge and communication and so on, are regarded fuzzy factors.

Secondly, the cyber security notion is already imprecise. The purpose of using fuzzy approach in Intrusion detection systems is to enable it simpler to distinguish among typical and aberrant usage patterns. Dickerson [8] used fuzzy rule - based information retrieval techniques to determine networking infiltration. They invented Fuzzy-Intrusion-Recognition-Engine (FIRE), in which it use inductive reasoning to identify whether an infrastructure entity is undergoing hostile actions [8]. Similarly, in this proposed approach the logic of fuzzy is utilized to improve the efficiency of data integrity on communication. This will enhance the efficiency of the proposed approach intrusion detection ability by means of stabilize the recognition probabilities in dense manner using learning model.

IV RESULTS AND DISCUSSION

In this paper, a novel learning based intrusion detection strategy called AIeMLS is introduced by using the conventional ANN algorithm. The prototypical model of the proposed approach is cross-validated by using the network simulator tool and attains the best outcome in results. The Figure mentioned, Figure-3 explains the input parameter requirements of the proposed approach. As well as the following Figure, Figure-4 (a) illustrates the perception of communication environment with number of nodes presented into the network region and the Figure, Figure-4 (b) illustrates the perception of successful identification of intruder nodes presented into the network region. In this Figure, Figure-4 (b) multiple source mobile nodes (12, 16, 18, 27, 36, 40, 48 etc.) are available to make a perfect communication to the respective destination mobile nodes such as 28, 31, 38 and so on. The proposed approach identifies some intruder nodes over the communication area and marked it as red in color (2, 9 and 13). So, that the proposed approach efficiency is good enough to identify the intrusions in clear manner and the identified intruder nodes are marked into the training model. The trained model is considered as a trace over here to cross-validate the testing scenario of communication.

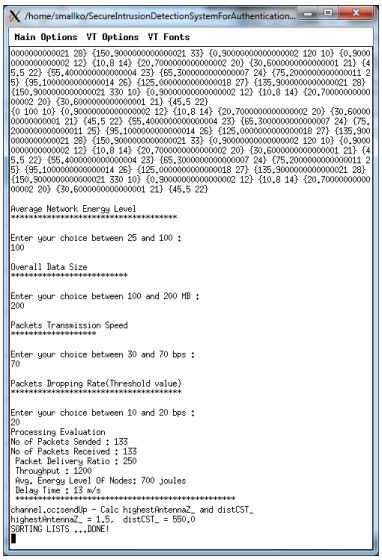
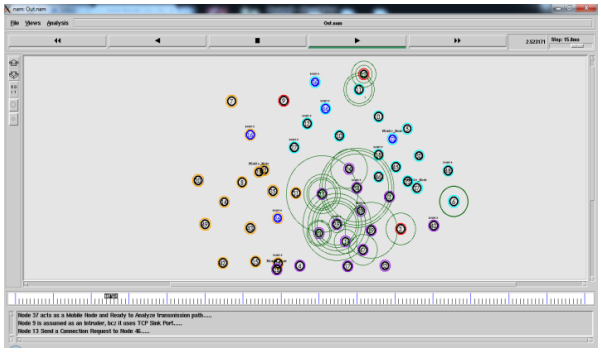
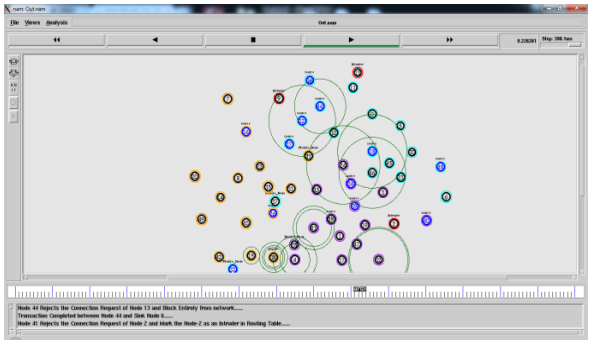


Figure 3: Input Parameters



(a)



(b)

Figure 4: (a) Nodes Presence over Communication Environment and (b) Intrusion Detection Model

The Receiver-Operating-Characteristics (ROC) curve is a graphical representation of the effectiveness of multi-dimensional categorization information and t is widely regarded as among the most important assessment measures for determining the correctness of any trained model. The curve shown in the following Figure, Figure -5 represents the ratio of True-Positives to False-Negatives at distinct threshold levels. The curve indicates how effectively the binary classification distinguished among two distinct types, safe or harmful. The proposed learning based classification model called AIeMLS is trained on a dynamic samples generated while executing the prototype with different input parameter values and then optimized using 10 fold cross-validation to get the Receiver-Operating-Characteristics curve shown in the following Figure, Figure - 5.

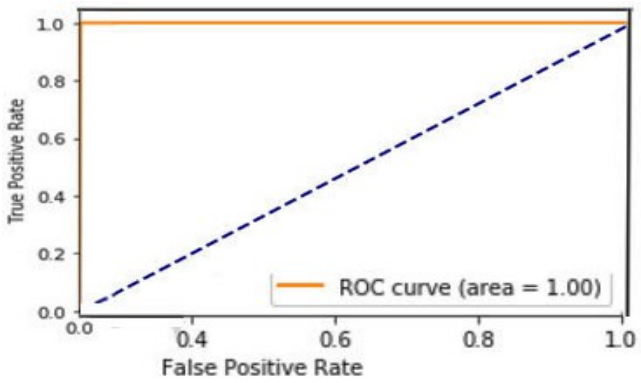


Figure 5: ROC Curve

The confusion matrix of the AIeMLS summarizes the set of possible and false predictions as well as the number of legitimate and harmful cyberattacks in this approach. The following Figure, Figure -6 illustrates the mentioned confusion matrix with samples how well it detects normal and harmful intrusion attacks in perfect way. Thus, the entire confusion matrix passes the efficiency assessment of the proposed approach metrics.

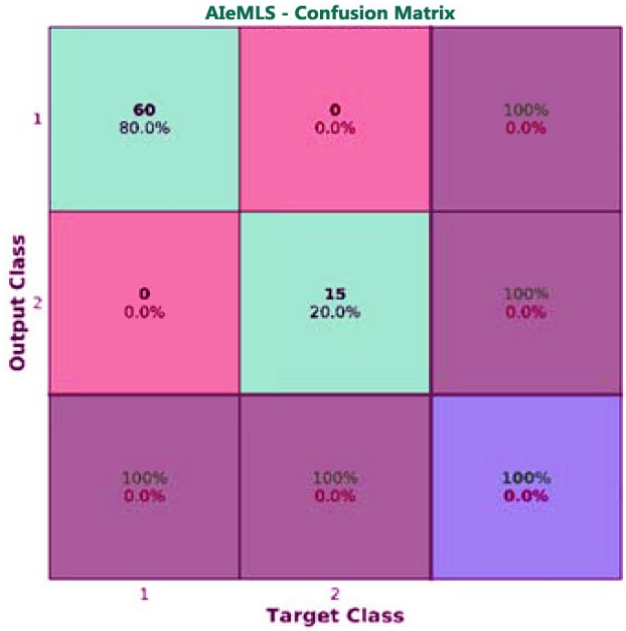


Figure 6: Confusion Matrix

The following Figure illustrates the perception of proposed approach intrusion detection accuracy in clear manner with the attainment of 98.5%, whereas the proposed approach is cross-validated with the conventional classification schemes such as ANN and SVM to prove the efficiency of the proposed approach. In which the ANN and SVM attains 98% and 96% accuracy levels of the intrusion prediction.

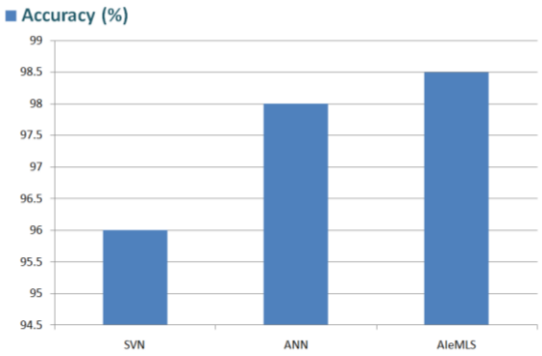


Figure 7: Efficiency Analysis

V CONCLUSION AND FUTURE WORK

By employing logic of Artificial Intelligence Enabled Modified Learning Strategy (AIeMLS) to identify intrusions over network environment and the associated data, the IDS described in this research considerably outperforms AI enabled signature based detection

techniques. And also the proposed approach of AIeMLS demonstrates excellent responsiveness on the test data, but it also exhibits outstanding accuracy. The proposed approach's performance was then evaluated in terms of false positive rate using extremely large data samples, as the sample generation is entirely based on the dynamic execution process and the associated network traffic file content and the proposed approach achieved a false positive rate of less than 2%. Minimizing false positives is critical for the real-world deployment of network intrusion systems, since large rates of false - positive results in an incredibly low signal to noise ratio, frequently rendering the system ineffective.

This paper provides an asynchronous method for identifying intrusion detection scheme patterns inside information and the method reported in this research is now being integrated into online based IDSs and being tested on actual network information, with additional significant changes for continuous network activity a focus of exploration. Another topic for future research is the implementation of the adaptive method to intrusion detection scheme described above to other aspects of networking cyber security, like the identification of cross-site programming and SQL code injection on web - based applications.

VI References

[1] Idris, N. B., & Shanmugam, B. (2005). Artificial intelligence techniques applied to intrusion detection. *Annual IEEE India Conference - Indicon*. https://doi.org/10.1109/indcon.2005.1590122

[2] Stiawan, D., Abdullah, A. H., & Yazid Idris, M. (2010). The trends of intrusion prevention system network. *2nd International Conference on Education Technology and Computer*. https://doi.org/10.1109/icetc.2010.5529697

[3] Blackstone, M. S. (2005). *United States Patent*. https://patentimages.storage.googleapis.com/69/f7/ab/a428ace2810ebe/US8413246.pdf.

[4] Polychronakis, M., Anagnostakis, K. G., & Markatos, E. P. (2008). Real-world polymorphic attack detection using network-level emulation. *Proceedings of the 4th Annual Workshop on Cyber Security and Information Intelligence Research: Developing Strategies to Meet the Cyber Security and Information Intelligence Challenges Ahead*. https://doi.org/10.1145/1413140.1413164.

[5] Singh, R., Kumar, H., Singla, R. K., & Ketti, R. R. (2017). Internet attacks and intrusion detection system. *Online Information Review*, 41(2), 171–184. https://doi.org/10.1108/oir-12-2015-0394.

[6] Liao, H. J., Richard Lin, C. H., Lin, Y. C., & Tung, K. Y. (2013). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, 36(1), 16–24. https://doi.org/10.1016/j.jnca.2012.09.004.

[7] Maestre Vidal, J., Sandoval Orozco, A. L., & Garcia Villalba, L. J. (2015). Quantitative criteria for alert correlation of anomalies-based NIDS. *IEEE Latin America Transactions*, 13(10), 3461–3466. https://doi.org/10.1109/tla.2015.7387255.

[8] Dickerson, J. E., & Dickerson, J. A. (2000). Fuzzy network profiling for intrusion detection. *19th International Conference of the North American Fuzzy Information Processing Society - NAFIPS*. https://doi.org/10.1109/nafips. 2000.877441.

[9] Ou, C. M. (2019). Host-based intrusion detection systems inspired by machine learning of agent-based artificial immune systems. *IEEE International Symposium on INnovations in Intelligent SysTems and Applications*. https://doi.org/10. 1109/inista.2019.8778269.

[10] Tsochev, G., Trifonov, R., Yoshinov, R., Manolov, S., & Pavlova, G. (2019). Improving the efficiency of IDPS by using hybrid methods from artificial intelligence. *International Conference on Information Technologies*. https://doi.org/10.1109/ infotech.2019.8860895

[11] Kanimozhi, V., & Jacob, T. P. (2019). Artificial intelligence based network intrusion detection with hyper-Parameter optimization tuning on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing. *International Conference on Communication and Signal Processing*. https://doi.org/10.1109/iccsp. 2019.8698029

[12] Kalaivani, S., Vikram, A., & Gopinath, G. (2019). An effective swarm optimization based intrusion detection classifier system for cloud computing. *5th International Conference on Advanced Computing & Communication Systems*. https://doi.org/ 10.1109/icaccs.2019.8728450.

[13] Ishaque, M., & Hudec, L. (2019). Feature extraction using deep learning for intrusion detection system. *2nd International Conference on Computer Applications & Information Security*. https://doi.org/10.1109/cais.2019.8769473.