iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** VI **Month of publication:** June 2026

DOI: https://doi.org/10.22214/ijraset.2026.83733

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue VI June 2026- Available at www.ijraset.com

Implementation of a Hybrid Artificial Immune System for Autonomous Network Threat Detection

Vivek Rawat[1], Rakesh Kumar[2], Aumreesh Kumar Saxena[3], Sitesh Kumar Sinha[4]
[1]*Computer Science Engineering Rabindranath Tagor University Raisen, MP, India*
[2]*Computer Science Engineering Rabindranath Tagor University Raisen, MP, India*
[3]*Computer Science & Information Technology SIRT Bhopal*
[4]*Registrar SGSU Bhopal*

Abstract: ***This paper is focusing on Modern network security faces increasingly sophisticated cyber threats requiring intelligent, autonomous detection systems. This work introduces an intrusion detection framework inspired by biological immune mechanisms, specifically implementing danger theory and negative selection principles for enhanced threat identification. The system operates independently with minimal human intervention, featuring real-time detection, adaptive learning capabilities, and automated resource management. Our dual-phase methodology first employs danger theory to analyze network traffic and extract distinguishing behavioral features between legitimate and malicious activities, significantly reducing computational requirements while preserving detection accuracy. The second phase utilizes negative selection algorithms for pattern-based threat recognition, effectively identifying known attack signatures while classifying normal traffic and novel intrusions. Experimental evaluation across multiple metrics including detection rate, accuracy, true negative rate, and recall demonstrates superior performance in distinguishing normal behavior, known attacks, and previously unseen threats, with reduced false positives and robust operation in dynamic environments.***

Keywords: Intrusion Detection System, Artificial Immune System, Misuse Detection, Anomaly Detection, Network Security

I. INTRODUCTION

The gradual development of global network interconnections has taken place over time. Illegal accessing of any networks by attackers, can lead to control over the network [1, 2]. Denial of Service (DoS) [3, 4] is an example of such type of attack. Numerous methods are employed to protect network or communication through web portal; [1-3]. There are several inquiries regarding the necessity of IDS. Similar to how firewalls keep hackers and intruders, access control through password can be viewed as a function of the firewall, allowing only authorized users to access the Internet or send and receive emails without interference [2-4].

1) Intrusion detection system

An IDSs (Intrusion Detection System) [6] comprises a collection of techniques and methodologies employed to identify suspicious activities at both the network and host levels. Typically, an IDS gathers data from the network and applies its established rules to this data or identifies anomalies within it [7-9].

2) Immune Reactions System

It can have Two major branches of the immune system [12-13]. Artificail and adaptive and inborn or innate immune system further categorized into numerous different molecules and cells.

3) Artificial Immune System (AIS):

An Artificial Immune System (AIS) represents a broad field dedicated to research and study [14]. Its purpose to establish connection between immunology and its technical concepts. The field of immunology employs mathematical and computer simulation modeling techniques [14-15]. It was initially proposed in the mid-1980s and gained significant popularity.

II. PROPOSED WORK

Our proposed Artificial Immune System-based Intrusion Detection System implements a dual-phase architecture leveraging danger theory and negative selection algorithms. The system operates autonomously, requiring minimal human supervision while maintaining high detection accuracy and low false positive rates.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue VI June 2026- Available at www.ijraset.com

Fig. 1 and 2 are showing the presented IDS model with architecture. In this architecture, an agent is responsible for gathering the essential information required for analysis at the host, subsequently storing all pertinent data in the corresponding database. The database, "Signature_DB," comprises a collection of well-defined signatures, referred to as intrusions.

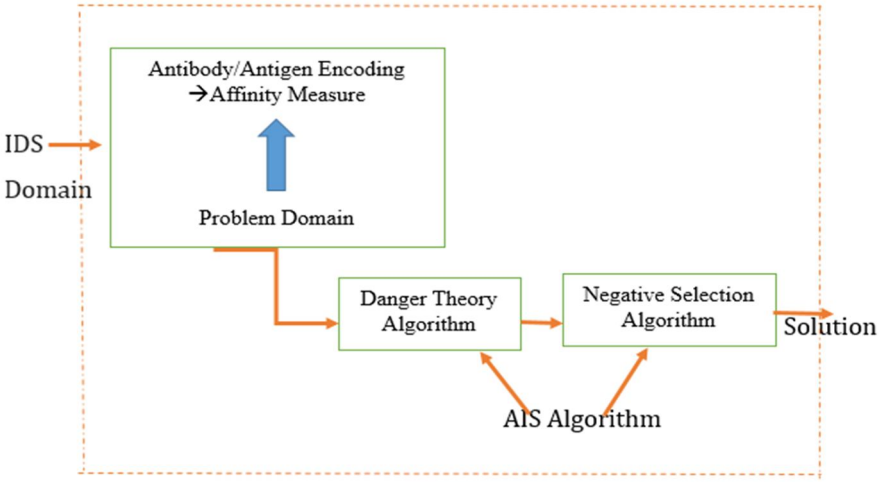


Fig. 1: Presented IDS Architecture

A. System Architecture Overview

Its architecture is formed by several specialized agents that work together within a distributed framework. These are data collection agents, danger signal processor agents, detection agents, and response coordinator agents. All these agents work semi-autonomously by using a common knowledge database and message passing system.

The main architectural components include Packet capture and preprocessing module, Danger theory-based feature extraction engine, Negative selection detection mechanism, Classification and alert generation system, Dynamic adaptation and learning module

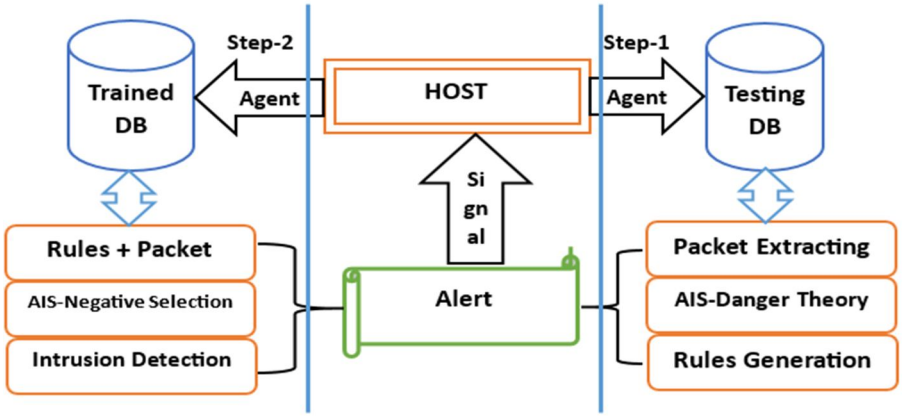


Fig. 2: Presented IDS Model

1) Phase 1: Danger Theory-Based Feature Selection

In the first phase, danger theory is used to extract essential behavioral parameters that make malicious traffic different from legitimate traffic. Unlike typical solutions that consider every possible feature, danger theory concentration is on non-threatening indicators.

Danger Signal Processing Algorithm capture network packets in real-time, extract the initial feature set from the network packets, compute the danger scores using the anomaly metrics, perform the threat filtering based on the defined thresholds, store the extracted feature set in the knowledge base, the danger signals are a compilation of several aspects, such as the violation of protocols, the packet pattern, the connection anomalies, and the statistical deviations.

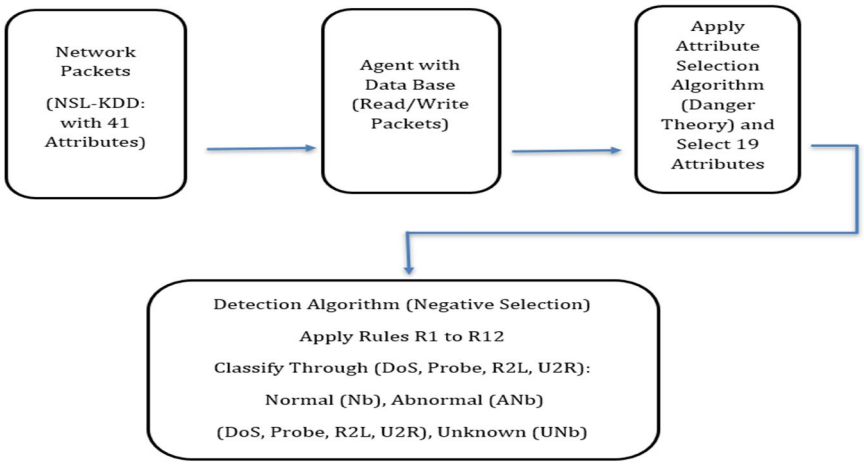


Fig. 3: Combined approach of Presented IDS Model

"Critical features include," according to danger theory, "Protocol type and service characteristics, Connection duration and data transfer volumes, Flag combinations and TCP transactions, Source and destination address patterns, and Packet rate and inter-arrival times. The selection of features helps reduce the dimensionality from the several hundred features that could be important to a refined set of 12-15 features, which are the critical ones." The reduction in features helps in reducing the complexity of computations. It further helps in easy execution in Real-time.

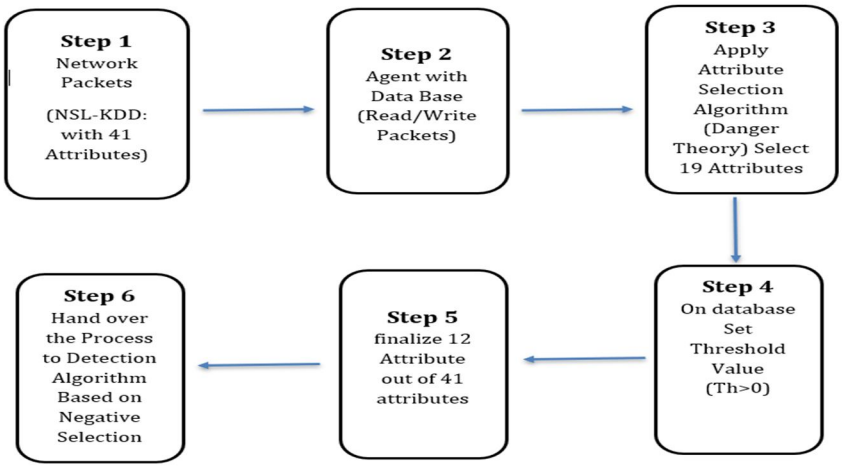


Fig. 4 : Phase 1- Danger Theory-Based Feature Selection and Classification Workflow

2) Phase 2: Negative Selection Algorithm

The second phase relies on negative selection algorithms for pattern recognition and classification. This process mimics the T-cell maturation phase. Detectors learn to identify self and non-self patterns.

Detector Generation Process are Define self-set by normal traffic patterns in the training data, Generate random detectors as candidates, eliminate detectors with self-patterns (negative selection), Verify detectors with known attack patterns, Distribute verified detectors for online detection tasks, r-contiguous bit detectors employ bit-matching techniques and have detection threshold values that are adjustable. In r-contiguous bit detectors, detectors match bits using r-contiguous bit-matching techniques to produce detection triggers that surpass predefined threshold values.

Detection Classification Categories are Normal Traffic Patterns matching self-set, no detector activation, known attack Patterns matching trained attack signatures, and Novel Threats: Patterns activating detectors without known signatures in the Proposed

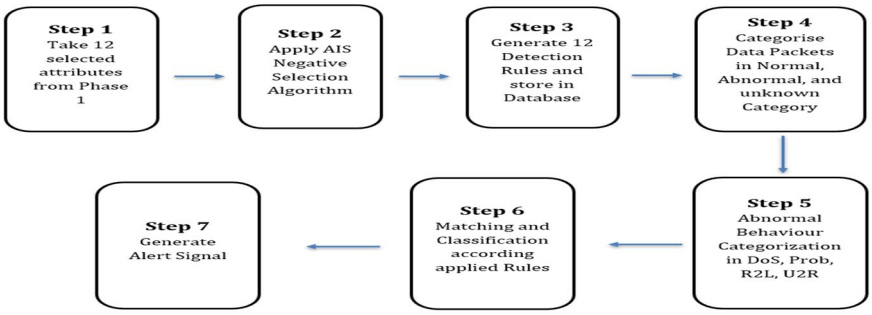


Fig. 5: Phase 2 - Negative Selection–Based Detection and Classification Workflow

B. Dynamic Adaptation Mechanism

The system incorporates continuous learning capabilities, updating detector populations and danger signal thresholds based on operational feedback. When novel attack patterns emerge, validated detectors incorporate new signatures into the knowledge base, enhancing future detection accuracy.

Adaptation mechanisms are Periodic detector regeneration incorporating new attack signatures, Self-set updates reflecting legitimate traffic evolution, Automatic threshold adjustment based on false positive rates, Agent failure detection and automatic recovery, Load balancing across distributed detection agents, This self-organizing capability minimizes administrative overhead, allowing the system to maintain effectiveness as network conditions and threat landscapes evolve. Failed agents trigger automatic redistribution of monitoring responsibilities, ensuring continuous protection without manual intervention.

In Presented IDS Model Working of agent is as follow showing as

Extract Packet: The agent will pick up the packet individually from the database to fetch the attribute details from the packet. All the attributes are maintained in a separate database for easy processing. It is already known that by capturing the packet in real-time, only 8 to 10 attributes are derived from the packet, but in the NSL KDD dataset [34], there are 41 attributes for the packet. There are several issues regarding deriving 41 attributes for the packet from only 8 to 10 attributes. To overcome this problem, the proposed Intrusion Detection System (IDS) system will apply the concept of the Kyoto dataset theory [34], which explains the concepts for designing 10-13 additional attributes. A close observation of the NSL KDD CUP dataset [34] identifies that not all 41 attributes are efficient for intrusion detection due to their zero numeric values. It has been identified that most of the attributes have zero numeric values, which are ineffective for the identification of intrusions. Further observations from the dataset imply that only 12-13 attributes are present in a packet that are efficient for the identification of intrusion. To prepare the 12-13 attributes presented, the Intrusion Detection System (IDS) will utilize another concept from Artificial Immune Systems (AIS) known as "Danger Theory" [35]. Currently, there is a misinterpretation between self and non-self, where, for instance, a normal packet may be misidentified as an intrusion, and an intrusion may be misidentified as a normal packet within a host. Therefore, the AIS "Danger Theory" mechanism will be employed. To defend against harmful antigens, the human body's immune system possesses an effective mechanism that can accurately identify harmful antigens. Similarly, the presented IDS will accurately identify or evaluate attributes by employing the "Danger Theory" mechanism. The proposed IDS will capture packets and assess each packet individually; during the packet evolution process, it will discard attributes that do not indicate an intrusion and retain only those attributes that do. All attributes and packets will be stored in a database.

Attribute Selection Algorithm (ASA) based on Danger Theory: The preference of attribute is done by the agent where values for attribute preference are as follows.

Input: D_i (D->Data Set and j->1 to n) and A_j (A->Attributes with non-zero values and i-> 1 to n).

Idyllic: Threshold Value > 0.

Output: $A_j \in A_j \rightarrow D_i$

1. Attribute $A_j \varepsilon D_i$. (Set the Values)
2. Choose $A_j \leftarrow D_i$ (value selection form database).
3. $D_i/2 \rightarrow D_1$ & D_2 (Where $D_1 \rightarrow$ for Zero Values (A_i) and $D_2 \rightarrow$ for Non Zero Values (A_i))
4. Compare the attributes value(V) with threshold value (Th)

   V > (Th)
5. Collect the chosen attributes values in D_i dataset referred as a final dataset.

After applying above algorithm on a packet, presented IDS select 12 strong attribute out of 41 attribute as per NSL KDD CUP dataset [34] for further process.

Agent with Database: database working with agent is play an important role because agent can read or write information in a database. All type of packets record is stored in the database where agent fetch the related information and forward for further process.

Agent with Retrieve Information: The work of agent is that it will reclaim information from database with coordination of data base (DB) and passes this information to rules.

Agent with Rule: Rule in presented IDS used as second AIS concept which is "negative Selection" [18] to improve correctness of intrusion detection [19]. Presented IDS can be classified to packets into normal or abnormal by using negative selection algorithm just like self-cell or non-self-cell in immune system. Negative selection [28] work with Rules which is helped to classified the packets into particular category that is normal/abnormal.

Detection Algorithm (DA) based on Negative Selection Technique

Input: R_i (i= 1 to 12) (Rules) → D_b (Database), Nb (Normal Behavior) and ANb (Abnormal Behavior), UNb(Unknown Behavior),

Output: Nb and ANb { ANb_1 → DOS, ANb_2 →Probe, ANb_3→R2l and ANb_4→U2R}, UNb_i (i 1 ton)

1. Rules R_i (R_1, R_2, R_3……..R_{12}) generation and store in data base D_b.
2. Generate Three classes Nb_1 for normal and ANb abnormal behavior and UNb for unknown behavior.
3. ANb (abnormal) behavior ANb_1 → DOS, ANb_2 →Probe, ANb_3→R2l and ANb_4→U2R.
4. Give Rules R_i to Nb, ANb & UNb.
5. Extract a Packet P_i (i = 1 to n).
6. Rule Match to P_i (packet ->1 to n) and R_i (Rules 1 to 12)
   If (P_i = R_i→ Nb) then P_i is assigned as normal behavior.
   Else If (P_i = R_i→ ANb) then P_i is assigned as abnormal behavior and
   Rules can be classified abnormality into its type.
   If (P_i = ANb_1) that means P_i referred to DoS intrusion.
   Else If (P_i = ANb_2) that means P_i referred to Probe intrusion.
   Else If (P_i = ANb_3) that means P_i referred to R2L intrusion.
   Else If (P_i =ANb_4) that means P_i referred to U2R intrusion.
   Otherwise
   P_i is assigned as "Unknown behavior".
7. Agent will preserve in database to UP_i for future reference.

If a packet matches the normal behavior condition during intrusion identification, it can be considered normal; if not, it will be treated as abnormal. By matching the rules that are already stored in the database, rules use a negative selection mechanism to identify both normal and abnormal packet behavior. With the help of NSL KDD [34] data set, presented IDS created rules for normal and abnormal (Probe, DoS, R2L and U2R) [34-35] behavior of packets. All rules are defined properly and accurately.

C. Self-Design general rule

Rule –

```
If  (Pack_Prot_Flag= "SF" || "REJ" || "RSTO" || "RSTR" || "S0" || "S1")
{    Rule → "Normal_Behavior"
}
Else If  (Pack_Prot_Flag= "S2" || "S3" || "RSTOS0" || "RSTRH" || "SH" || "SHR" || "OTH")
{    Rule → "Abnormal_Behavior"
}
Else
{    Rule → "Unknown_Behavior"
}
```

Algorithm of general rule as called "Rule-Algorithm" After designing general rule "Rule-Algorithm", presented IDS show "Normarl_Behaviour_Packet" and "Abnormal_Behaviour_Pacekt" where "Unknown_Behaviour_Packet" is the future work of the presented IDS.

Agent with Alert Signal: Once intrusion is detected than an alarm produces by the agent of presented IDS to Host regarding alertness. This alarm can be a message or it can be an email etc. which is supported by Host.

D. Working of the Proposed framework

In the presented IDS incorporated two approaches of AIS like negative selection and danger theory. Presented IDS is the misuse detection IDS. Figure 3.1 is showing the presented IDS architecture. In this architecture, an agent is responsible for gathering the essential information required for analysis at the host, subsequently storing all pertinent data in the corresponding database. The database, "Signature_DB," comprises a collection of well-defined signatures, referred to as intrusions. Presented IDS is retrieve the information through agent from the “Signature_DB” data base and passes to match the rules. If signatures matched and detect intrusion, then agent generated an alarm to host. In the presented IDS working of agent is important factor because agent is collecting information, extracting information, passing the information, conveying message or alert to host system. For alert message or communication agents can use diverse strategies like pipes, message lines, and shared memory. Presented IDS have an agent which can move in hosts as per necessity of the host system. If an agent inactivates during processing over Host then an alarm signal will generate which automatically fixed by presented IDS in the form of new agent.

In figure 3.2: Combined Artificial Immune System Based Intrusion Detection Framework shows The combined framework illustrates the complete workflow of the proposed AIS-based IDS. Network and host traffic are processed sequentially through three biologically inspired phases problem encoding, danger evaluation, and negative selection resulting in accurate intrusion detection and alert generation.

Attribute Selection

In diagram represents the operational workflow of the proposed agent-based Intrusion Detection System (IDS) inspired by Artificial Immune System (AIS) principles. The process starts with network packets obtained from the NSL-KDD dataset, which consists of 41 distinct attributes describing various network traffic behaviors. These packets serve as the raw input for the IDS. An intelligent agent integrated with a database act as the core processing unit. This agent continuously reads and writes packet information to the database, ensuring efficient data management and enabling coordination between different detection stages. The stored packet data is then forwarded to the Attribute Selection Algorithm (ASA), which is designed using the Danger Theory concept. This algorithm evaluates attribute values against a predefined threshold to identify features that exhibit potentially suspicious behavior. By filtering out insignificant or redundant attributes, the system reduces dimensionality and retains only the most relevant features (illustrated as a reduced set of selected attributes). This optimization improves processing speed while maintaining high detection capability. The selected attributes are subsequently passed to the Detection Algorithm (DA) based on the Negative Selection Technique. This stage applies a predefined set of rules (R1 to R12) to analyze packet behavior. Using immune-inspired self and non-self-discrimination, packets are classified into Normal (Nb), Abnormal (ANb), or Unknown (UNb) categories. Abnormal traffic is further categorized into specific attack types, namely Denial of Service (DoS), Probe, Remote-to-Local (R2L), and User-to-Root (U2R) attacks. Packets that do not match existing rules are labeled as unknown and stored in the database for future learning and rule enhancement. Overall, the diagram highlights a structured, adaptive, and efficient IDS framework that combines intelligent agents, feature reduction, and immune-based detection to enhance intrusion detection accuracy.

III. RESULT ANALYSIS

Experimental results demonstrate consistent high performance across all evaluation metrics. True Negative Rate ranges from 0.997 to 0.975 across five iterations, indicating excellent normal traffic classification with minimal false alarms. Corresponding False Positive Rates range from 0.0054 to 0.0091, representing substantial improvement over traditional intrusion detection approaches. Overall accuracy maintains values between 0.991 and 0.963, while precision ranges from 0.992 to 0.971. Detection rates span 0.993 to 0.961, demonstrating robust attack identification capabilities. These metrics consistently approximate 0.99, indicating stable performance regardless of data partition variations. Experimental results demonstrate consistent high performance across all evaluation metrics. True Negative Rate ranges from 0.997 to 0.975 across five iterations, indicating excellent normal traffic classification with minimal false alarms. Corresponding False Positive Rates range from 0.0054 to 0.0091, representing substantial improvement over traditional intrusion detection approaches. Overall accuracy maintains values between 0.991 and 0.963, while precision ranges from 0.992 to 0.971. Detection rates span 0.993 to 0.961, demonstrating robust attack identification capabilities. These metrics consistently approximate 0.99, indicating stable performance regardless of data partition variations. The system's feature selection mechanism, utilizing 12 critical attributes identified through danger theory, significantly contributes to computational efficiency.

Reducing dimensionality from 41 original features to 12 selected attributes decreases processing overhead while preserving detection accuracy, enabling real-time operation on standard hardware. In the initial phase, the proposed IDS will be evaluated offline. The effectiveness of the proposed IDS will be meticulously assessed through experiments utilizing the NSL-KDD dataset, which is an enhanced version of the KDD'99 datasets [35]. The redundancy present in the training and testing records of the KDD dataset necessitates the use of the NSL-KDD dataset [71-73]. For dual classification, the NSL-KDD categorizes network traffic into two distinct classes: abnormal and normal. Each connection record in this dataset is characterized by 41 attributes. The attribute list, which includes both discrete (symbolic) and continuous variables, is detailed in Table 2, presenting a significant challenge in identifying intrusions. Normal packets and infected packets records of NSL-KDD data set is showing in Table 3. Presented IDS will have used during results analysis.

Table 1: Normal and Attacks Records in NSL-KDD Dataset [35]

	"Records"	"Normal"	"DoS"	"Probe"	"U2R"	"R2L"
"Train_20%"	25192	13449	9234	2289	11	209
		53.39%	36.65%	9.09%	0.04%	0.83%
"Train_All%"	125973	67343	46972	11565	52	995
		53.46%	36.45%	9.25%	0.04%	0.79%

The proposed IDS will execute on normal training and testing data record as well as intrusion training and testing data record which is shown in table 4.

Table 2: Trained Data Sets [35]

	"Records"		"Normal"	"DoS"	"Probe"	"U2R"
Train_20%	25192		13449	9234	2289	11
			53.39%	36.65%	9.09%	0.04%

The analysis was conducted based on several parameter showing from equation (1) to equation (6) [35]. True Negative (TN) indicates instances that are correctly identified as an attack. False Positive (FP) denotes instances that are predicted as an attack when they are not. False Negative (FN) signifies instances that are predicted as normal when they are actually an attack [36]. Table 5 illustrates that an event action, like if intrusion occur or detect than alarm is produces in the form of massages which is alert to host.

- False Negative Rate: FNR = 1 – TPR…….(1)
- True Negative Rate: TNR = 1 – FPR……..(2)
- False Positive Rate: FPR = 1 – TNR or FPR = FP/ (FP+TN)…….(3)
- Precision: Precision = TP / (TP+FP)……...(4)
- Recall: Recall = TP / (TP + FN)……..(5)
- Accuracy (ACC): ACC = (TP+TN)/(TP+TN+FP+FN)……..(6)

Presented IDS calculated various parameters like accuracy, Precision, FPR, DR and TNR on 12 attributes with number of iteration on 20% dataset of actual dataset which is shown in table 6.

Table 3: ACC-Precision-FPR-DR-TNR results with the Presented IDS on 12 attributes

S. No.	Number of Iteration	ACC	Precision	FPR	DR	TNR
1	I	.99	.99	.0051	.99	.99
2	II	.98	.98	.0062	.98	.99
3	III	.97	.98	.0061	.97	.99
4	IV	.97	.98	.0081	.96	.98
5	V	.96	.97	.0091	.96	.97

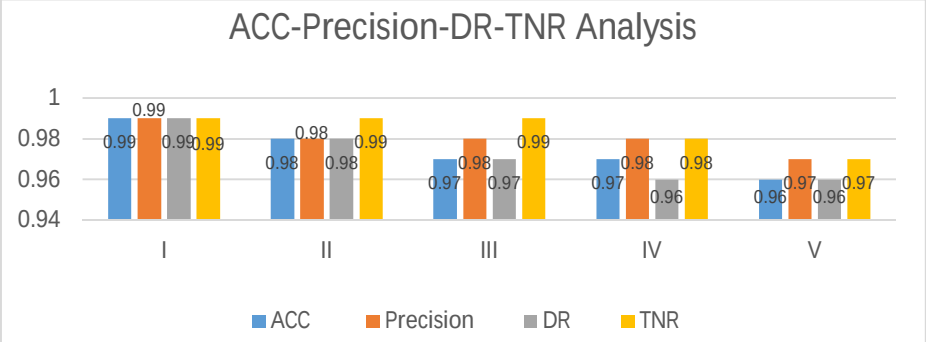


Fig. 6: Pictorial Representation of ACC, Precision, DR and TNR over 12 attributes

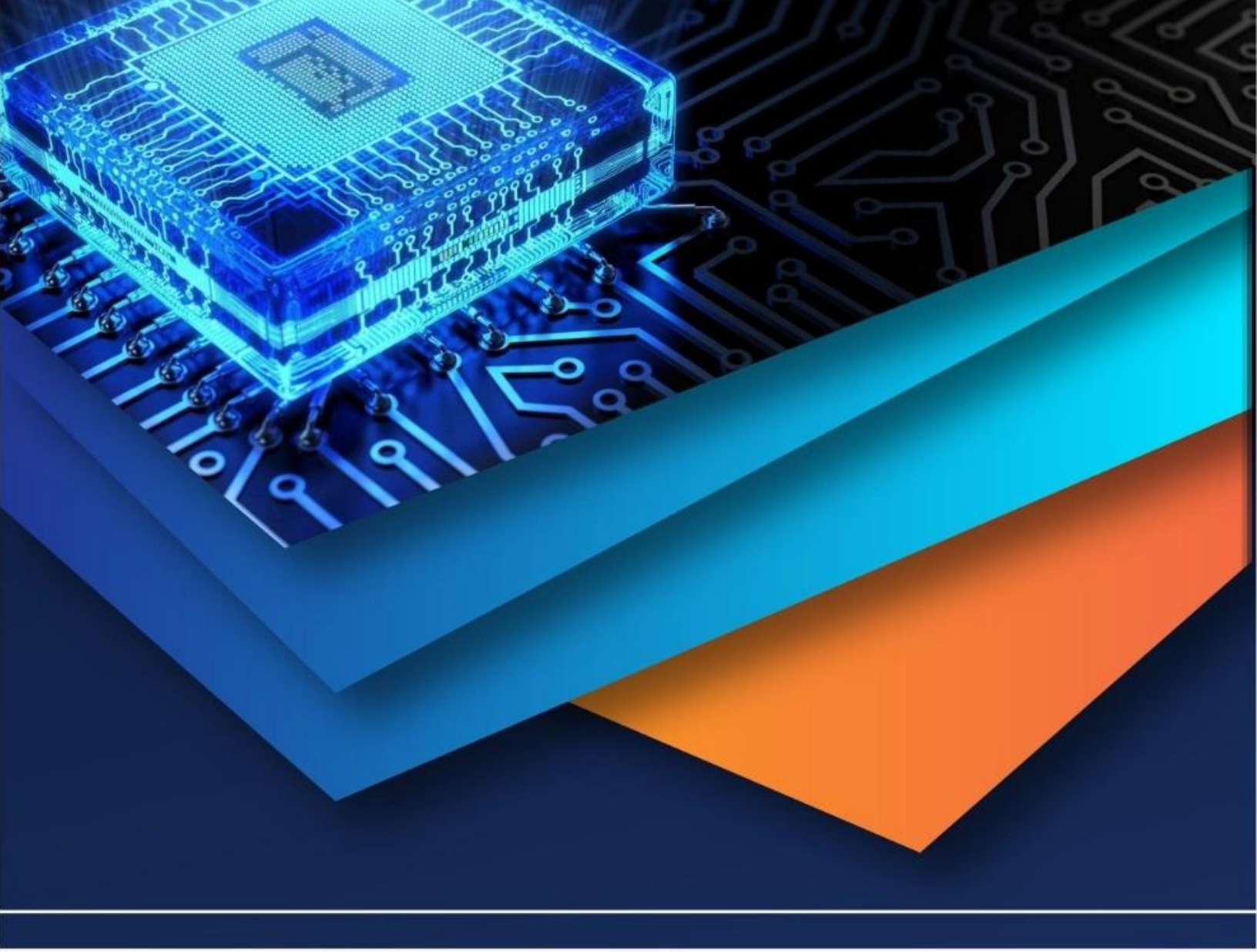
IV. CONCLUSION

Presented IDS is misuse IDS which is focusing on accuracy, efficiency, reliability, maintainability, dynamic adaptation. The presented IDS is the light weight agent working IDS that work to extract information from data packet, stored strong attribute in database, retrieve the information, match the rule and finally generate alert. Results showed that presented IDS decrease False Positive Rate (FPR) and improved detection accuracy. After analysis of results presented IDS produce TNR which is 0.997 to .975 and FPR from 0.0054 to 0.0091 for iteration one to iteration five. Similarly accuracy 0.991 to 0.963, precision 0.992 to 0.971 and detection rate with 0.993 to 0.961 are varying on each iteration but maximum time it consist or near by 0.99 which is good. Presented results showing the performance of presented IDS over 12 attributes. Another working of presented IDS is that, if working of agent inactivated due to any reason then it identifies issue related with agent and according situation it is adjust automatically which is lead to dynamic adaptation. In Future with the advancement in the network system and agent working is to be redesign. Furthermore, it can upgrade from "AIS based IDS" to "AIS based IDS-and intrusion prevention system (IPS)".

REFERENCES

[1] Julie Greensmith and Uwe Aickelin "Firewalls, Intrusion Detection Systems and Anti-Virus Scanners" Computer Science Technical Report No. nottcs-
[2] Camilo Gutiérrez Amaya "IDS, Firewall and Antivirus: what you need to have installed" article at https://www.welivesecurity.com/2015/04/30/ids-firewall- antivirus-need-installed/ 2015
[3] Monali S. Gaigoleand Prof. M. A. Kalyankar "The Study of Network Security with Its Penetrating Attacks and Possible Security Mechanisms" International Journal of Computer Science and Mobile Computing IJCSMC2015
[4] Umesh Kumar Singh; Chanchala Joshi "Network security risk level estimation tool for information security measure" IEEE 7th Power India International Conference (PIICON) Pp: 1 – 6 India 2016
[5] Monali S. Gaigoleand Prof. M. A. Kalyankar "The Study of Network Security with Its Penetrating Attacks and Possible Security Mechanisms" International Journal of Computer Science and Mobile Computing IJCSMC, Vol. 4, Issue. 5, pg.728 – 735 May 2015,
[6] Aumreesh Kumar, Saxena ,Sitesh Sinha, Piyush Shukla, "A Review on Intrusions Detection System in Mobile Ad-Hoc Network" Proceeding of International conference on Recent Innovations is Signal Processing and Embedded Systems (RISE - 2017), 27th – 29th October, IEEE, 2017.
[7] Aumreesh Kumar Saxena, Sitesh Sinha, Piyush Shukla, "Performance Analysis of Classification Techniques by using Multi Agent Based Intrusion Detection System", International Journal of Computer Network and Information Security(IJCNIS), Vol.10, No.3, pp.17-24, 2018. DOI:10.5815/ijcnis.2018.03.03
[8] Aumreesh Kumar Saxena, Sitesh Kumar Sinha, Piyush K Shukla, Prashant k Shukla, M. Maheswari, M. Pandey, Ssdhana K "Multi Agent Based Intrusion Detection System using Artificial Immune System for Distributed Network" May 2020 ACM Transactions on Multimedia Computing, Communications and Applications DOI:10.1145/3378544
[9] B. J. Bejoy and S. Janakiraman, "Artificial immune system based intrusion detection systems—a comprehensive review," *Int J Comput Eng Technol*, vol. 8, no. 1 Bejoy, B. J. and Janakiraman, S. (2017) 'Artificial immune system based intrusion detection systems—a comprehensive review', Int J Comput Eng Technol, 8(1), pp. 85–95., pp. 85–95, 2017.
[10] Mr. Suryawanshi G.R, Prof. Vanjale S.B "Mobile Agent for Distributed Intrusion detection System in Distributed System" Publication in" International Journal of Artificial Intelligence and Computational Research (IJAICR.) ", Pp 1-8, 2010
[11] DuXianFeng and QiangZanXia "A Model of Intrusion Detection System Based on Aglet with Multi-Agent" IEEE International Conference on Computer Application and System Modeling(ICCASM 2010) Volume: 6 Pp: V6-232 - V6-234 china 2010,
[12] Rafael Paez, Miguel Tirrer" laocoonte : An agent based intrusion detection system" 2009 International Symposium on Collaborative Technologies and systems, Pp: 217 - 224, 2009
[13] Aumreesh Kumar Saxena, M. Arshad, Sitesh Sinha Evaluation of Agent Based Host Intrusion Detection System (AHIDS) through Various Classification Techniques Rabindranath Tagore University Journal Vol. IX/Issue XVII September 2019 ISSN: 2278- 4187
[14] Aumreesh Kumar Saxena, S. Sinha and P. Shukla, "General study of intrusion detection system and survey of agent based intrusion detection system," 2017 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India, 2017, pp. 471-421, doi: 10.1109/CCAA.2017.8229866.
[15] Chandrakant Jain, Aumreesh Kumar Saxena "General Study of Mobile Agent Based Intrusion Detection System (IDS)" Journal of Computer and Communications Vol.4 No.4, April 13, 2016
[16] A. Trivedi, A. Shrivastava, A. Saxena and M. Manoria, "Survey Analysis on Immunological Approach to Intrusion Detection," 2018 International Conference on Advanced Computation and Telecommunication (ICACAT), Bhopal, India, 2018, pp. 1-11, doi: 10.1109/ICACAT.2018.8933710.

[17] AnkitaTrivedi , Dr. Aumreesh Kumar Saxena, M. Arshad , Mr. Shivendra Dubey and Dr. Sitesh Kumar Sinha "INTRUSION DETECTION USING BIOLOGICAL INSPIRED IMMUNE SYSTEM" International Journal Of Scientific & Technology Research Volume 8, Issue 10, October 2019 Issn 2277-8616 Pp:1337-1344
[18] S. Alhasan, G. Abdul-Salaam, L. Bayor and K. Oliver, "Intrusion Detection System Based on Artificial Immune System: A Review," *2021 International Conference on Cyber Security and Internet of Things (ICSIoT)*, France, 2021, pp. 7-14,
[19] Hanyuan Huang, Tao Li, Yong Ding, Beibei Li, Ao Liu, "An artificial immunity based intrusion detection system for unknown cyberattacks, Applied Soft Computing, Volume 148, 2023, 110875, ISSN 1568-4946,
[20] Ehsan Farzadnia, Hossein Shirazi, Alireza Nowroozi, "A novel sophisticated hybrid method for intrusion detection using the artificial immune system" Journal of Information Security and Applications, Volume 58, 2021, 102721, ISSN 2214-2126.
[21] J Greensmith,and A Whitbrook, U Aickelin "Artificial immune systems" Handbook of Metaheuristics, 421-448 2010
[22] Kim J, Bentley P J, Aickelin U, et al. Immune System Approaches to Intrusion Detection - A Review [J]. Natural Computing, 6(4): Pp:413-466 2007.
[23] L. de Castro and J. Timmis. An artificial immune network for multimodal function optimization. In Proc. of the Congress on Evolutionary Computation (CEC), volume 1, pages 699-704, Los Alamitos, CA, USA, 2002. IEEE Computer Society.
[24] J Kim, PJ Bentley, U Aickelin, J Greensmith, G Tedesco, J Twycross "Immune system approaches to intrusion detection–a review" Natural computing 6 (4), 413-466 2007
[25] U Aickelin, J Greensmith, J Twycross "Immune system approaches to intrusion detection–a review" International Conference on Artificial Immune Systems, 316-329 2004
[26] Nazeema, R. A. ., Kouser, S. ., Hassen, S. M. ., Babikar, N. ., & Adam Boush, M. S. . (2024). An Improved Explainable Artificial Intelligence for Intrusion Detection System in Cloud Environment. International Journal of Intelligent Systems and Applications in Engineering, 12(3), 352–360.
[27] Tanksale, V. Intrusion detection system for controller area network. Cybersecurity 7, 4 (2024). https://doi.org/10.1186/s42400-023-00195-4
[28] J. -L. Chen et al., "AI-Based Intrusion Detection System for Secure AI BOX Applications," 2023 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), Bali, Indonesia, 2023, pp. 360-364, doi: 10.1109/ICAIIC57133.2023.10066986.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY