Hybrid Policy-Based Architecture for Intrusion Detection System

I.O. Mustapha[1*]; J.B. Awotunde[2]; S.O. Ganiyu[3]; and A.M. Oyelakin[1]

[1]Department of Computer Science. Alhikmah University, PMB 1601, Ilorin. Nigeria
[2]Department of Computer Science. University of Ilorin. Nigeria.
[3]Federal University of Technology, Minna, Nigeria.

E-mail: salnet2002@alhikmah.edu.ng*
awotunde.jb@unilorin.edu.ng
gshefiu@gmail.com
amoyelakin@alhikmah.edu.ng

ABSTRACT

Day-in and day-out, malicious network users have continuously engaged in the analysis of specific network security vulnerabilities of organizations for possible intrusive activities through diversified and dynamic technology. Although experts in the domain have presented different architectural designs to curb malicious network intruders via the use of intrusion detection systems, most of the designs have not incorporated organizational security policy into the designs. Consequently, some available intrusion detection systems which are generally designed for various organizations are unable to meet their specific security needs because the security policy of said organization that emanated from their unique vulnerability was not taken into consideration. To this end, this paper presents a hybridized Intrusion Detection System architecture that takes into consideration the specific security policies of an organization. Signature-based approach, anomaly-based approach, and policy-based approach were hybridized in the framework using mobile agents. If the proposed architecture is implemented, it is expected to perform better in the detection of intruders within a network system.

(Keywords: network intrusion detection system, IT system intrusion, vulnerability, mobile agent, security policy)

INTRODUCTION

Intrusion is a term used for the description of all forms of internal or external illegal penetration into information or resources on a computer network. It includes all illegal breakage, malicious attacks, misuse of computer network resources, and all kinds of suspicious activities that exist across a computer network. Intruders tend to search for every means of acquiring the right of use for a network system illegally to be able to modify or render the system unusable and capture the available private information in such a system.

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents or attacks, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices (Jain and Saxena, 2016; Balogun and Jimoh, 2015). Intrusion Detection System refers to an automated set of computer programs used for detecting network misuse, illegal penetration, and some other forms of malicious activities across a computer network. It tends to detect and signal the system or security administrator concerning network misuse. It is a preemptive approach in computer security that senses threats and misuse to prevent them from an occurrence.

System security vulnerability refers to flaws on the part of computer or network system design that enhance intrusion. It can also exist because of lapses on the part of computer or network system users while the security policy of an organization is an access control mechanism for the description of access rights of the system user. It tends to specify the operational behavioral pattern of the system user. System vulnerabilities have been part of the source of various intrusive activities and intrusion has become the gateway for all forms of cybercrimes, hacking, internet fraud, and all other forms of computer network attacks.

Organizational security policy has an impact on the vulnerabilities of an organization's network because security policy is part of those steps to be taken to secure the network and avoid vulnerabilities. The relationship between organizational security policy and specific system vulnerability can easily be noticed especially when the policies from which software is developed are too numerous or complicated. At the same time, frequent policy changes may also pave way for system vulnerability. It has been ascertained that most attacks are carried out through the exploitation of company system vulnerabilities and those vulnerabilities vary from firm to firm.

Vulnerabilities of organization networks are difficult to totally predict and identify, hence the dynamism of organization security policy is inevitable. Such a dynamic security policy that is set down to protect the network needs to be embedded in IDS architecture. This is necessary because intrusive behavior of intruders is sometimes subjected to the unique vulnerability of the organization hence organizations sometimes need an intrusion detection system that is based on their specific policy which emanates from past experiences of intruders' pattern of behavior and past specific vulnerability of their organization. Hence to include organizational security policy in IDS, this paper proposed hybridized IDS architecture that includes policy-based approach, signature-based approach, and anomaly-based approach using a mobile agent.

LITERATURE REVIEW

The negative impact of intrusive activities has motivated researchers in the domain of IDS to vigorously put in place different models and techniques for intrusion detection. Some of the adopted techniques for the development of IDS include the use of embedded sensors in web server, File Transfer Protocol (FTP) servers, and database server applications to give signals in case of intrusive activities (Wu and Chen, 2008).

Evolutionary computation was also adopted (Kumar and Kumar, 2013). The design of network-based architecture that makes use of map reduce framework to face the challenges of a signature-based intrusion detection system (Holtz, David, and Timoteo, 2011). Data mining approach (Saad, Manickam, and Ramadass, 2013); Association rule (Tian and Pan, 2005); the use of mobile agents (Nandeshwar and Bijwe, 2015); Khobragade and Padiya, 2015); and Machine learning approach have also been used as techniques for reduction of less important attributes of network log (audit record) using heuristic functions (Kumar and Kamlesh, 2016). Most of these approaches have shown some effectiveness in the detection of intruders, but up till now, total eradication of intrusion from computer networks has yet to be achieved and researches continue in the domain.

It has been asserted that there is still an avenue for improvement on IDS via the use of mobile agent technology if the characteristics of Mobile Agent (MA) are judiciously and objectively utilized since agents can be reconfigured and rescheduled within a distributed network environment to perceive the changes within the environment and respond according to instruction promptly (Trushna, Patil, and Banchhor, 2013; Ganapathy, Yogesh, and Kannan, 2012; Jain and Saxena, 2016).

Different architectural approaches that use mobile agents have been developed across the globe and some were analyzed and categorized into eight groups (Saurabh and Saugata, 2011). Real-time IDS that involve a multi-agent system and data miming technique were designed for reduction of network traffic data processing time. (Al-Yaseen, Othman, and Nazri, 2016).

Biswas, Sharma, Poddder, and Kar, 2015) also hybridized host and network-based IDS in which multilayer technology was used with the help of coordinated monitoring multi-agent. The system was noted to prompt detection of intrusion. Abdulrrazaq, Bambang, and Rahardjo (2015) used ant colony clustering technology together with a highly coordinated cooperating agent for the detection of a coordinated intrusive attack. Banik, Bernsen, and Javed (2013) also came up with network-based IDS for the detection of distributed attacks. The research work uses agent technology with three different scanning algorithms for intrusion detection.

Even though the benefits derived from the above research cannot be over emphasis, there is a need for improvement in the area of incorporating organizational policy for the detection of intrusion. This becomes necessary because some of the intrusive activities exist as a result of mutational lapses relating to operational process policy, lapses during system development together with policy pattern of the organization. Gibson and

Clouse (2017), claimed that the detection of the beach of security policies of a network depends on information extracted from packet traffic and their flow pattern. He asserted that the expected pattern of traffic flow can be more informative for the detection of intrusion if the functional roles of hosts and the operational policy of a network system are taken into consideration. That is the pattern of packets flow is a function of the operational policy of hosts within a network system.

Additionally, Mamun, Kabir, Hossen, and Khan (2009) designed a policy-based intrusion response system that is focused on fault tolerance. Mobile agents are reconfigured to take over functionality within the network to avoid performance degradation in terms of power supply in a wireless network. Efficient resource management and scalability was an outstanding achievement in the study, except that policy which may cause system insecurity was not considered for possible intrusion detection.

Mark (2015) claimed that security monitoring policy and IDS have correlation, he explained that their purpose is geared towards the same goal, hence incorporating the policy of organization in the Intrusion detection system is necessary. Differently, this paper analyzed the normal operational processes and authority pattern of an organization and formalized it as a policy, then hybridized it with two other intrusion detection approaches for better detection of a known and unknown attack. No study has been published to the best of our knowledge and in line with this research literature review, where hybrid of organization policy and the two commonly used approaches for intrusion detection was found.

MODEL CONCEPTUAL DESCRIPTION

The Hybrid framework combines three approaches that include Policy-based approach, Signature-based approach, and Misuse approach using mobile agents to resolve some of the shortcomings in each of the approaches. The three approaches were modeled together for the detection of activities that are against the security policy of a particular system and a necessary response was put in place.

The proposed system has four modules as shown in Figure 1, which includes Intrusion Detection Module, Decision Module, Administrator Interface, and Intrusion Prevention Module.

Intrusion Detection Module consists of Policy based model, Anomaly based model, and Signature based model. Current user activities and those in the repository are the input to Intrusion Detection Module.

Framework for IDS

Intrusion Detection Module (IDM): The tasks performed, and methodology used by each model in IDM are explained as follows:

Policy-Based Model (PBM): This has to do with modeling the unique expected operation processes of each host in line with organizational policy, therefore it makes use of some predefined operational patterns which are allowed by the organization to suspect intrusion. That is, any user activities and program operation which is not in line with the predefined organization specification are to be suspected as intrusive (Jaisankar, Saravanan, and Swamy, 2009; Lee, Yoo, Kim, and Lee, 2011). Its parameters were generated based on organization security specifications and vulnerability tests. This makes a difference to the misuse approach because the misuse approach is based on previous experience of intrusive activities alone.

Jaisankar, Saravanan. and Swamy (2009) have earlier designed a similar framework except that vulnerability analysis was not inclusive and the design is to detect anomalous user activities alone. PBA is a control model that uses dynamic rules extracted from the organizational policy concerning what task can be performed by the user and which resources can a user have access to based on firm policy. Some of its features include the number of web pages allowed for each host; access to outdated applications for each host; access to applications by each host; processor time allocated for each host; average time for each host; size of disk for each host; types and size of data to be transferred and received by each host; amount and type of system file for each host; amount and type of Log file for each host; number and type of request for each host; and maximum memory usage for each host. Each host record relating to those features were used via rule-based machine algorithm to generate the rules that are embedded in PBM.

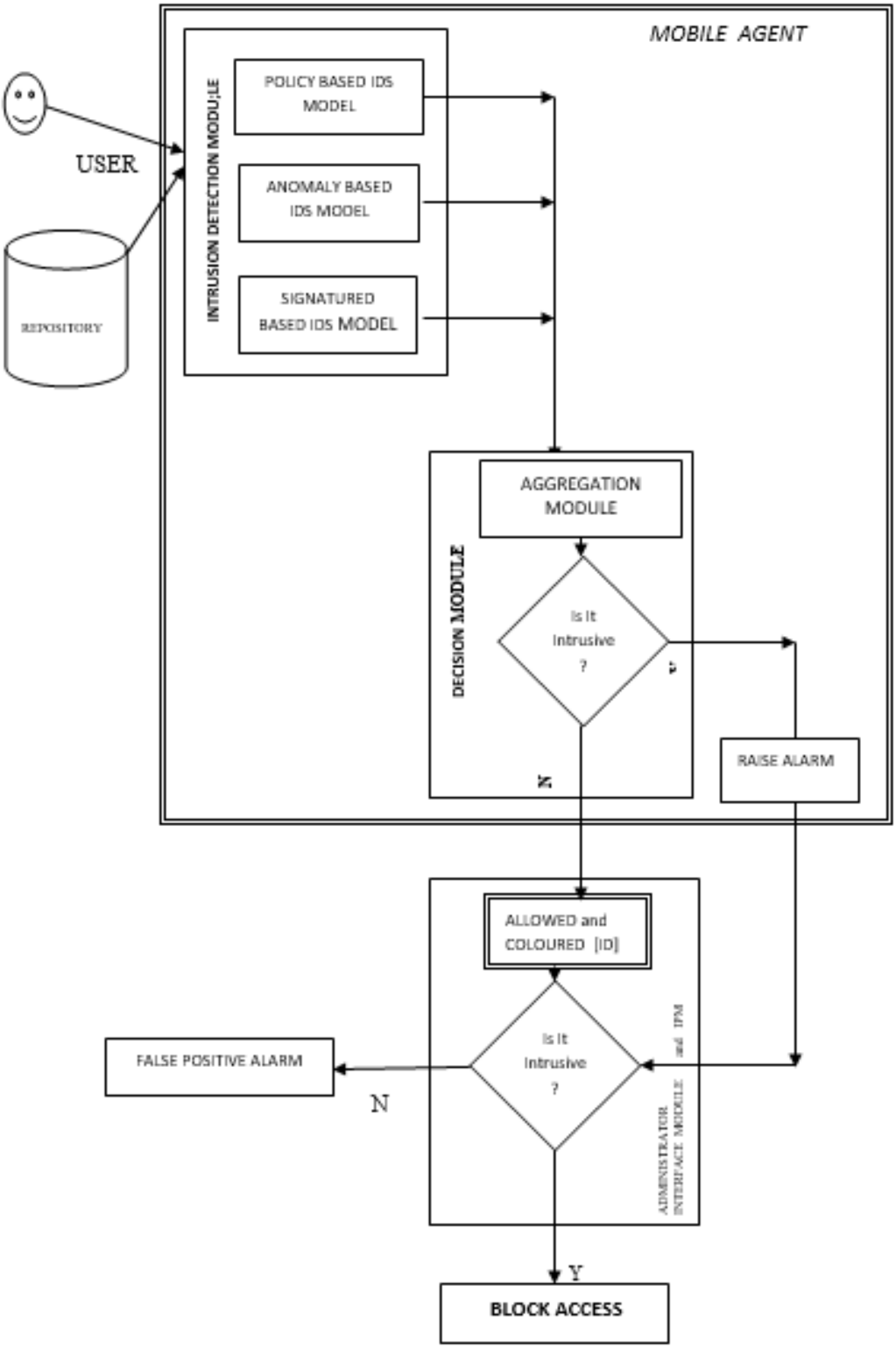

Figure 1: Intrusion Detection System.

Consequently, user activities are monitored and output from PBM to be either intrusive or non-intrusive, then digitally represented by one or zero and forwarded to DM.

Anomaly Based Model (ABM): this uses an approach whereby normal system behaviors are modeled, and an alarm is raised when a contrary behavior is suspected. For this model, relevant intrusion-related features of the UNB-CIC Network Traffic Dataset were extracted using the hybrid technology that includes the use of Greedy Stepwise and Best First search method via Correlation-based Feature Selection (CFS) Subset Evaluator together with ranker search method via information gain evaluator in WEKA application package. Hybridized feature selection machine learning algorithms were used to help the IDS process only the relevant features of the gathered data to avoid significant overhead (Hodo, Bellekens, Iorkyase, Hamilton, Tachtatzis, and Atkinson, 2017).

The selected features of the dataset were used to generate rules for ABM through ZeroR, OneR, and PART machine algorithm using 10-fold cross validation. The simulation results depict that the Projective Adaptive Resonance Theory (PART) algorithm is the best classifier of intrusive and non-intrusive activities out of the three experimented machine learning algorithms therefore it was used for this model. Some parts of the generated rules are shown below:

```
=== Classifier model (full training set) ===

PART decision list
------------------

 Source Port <= 49157: NORMAL (109184.0/3.0)

 Avg Fwd Segment Size > 10: NORMAL (33764.0)

Fwd IAT Total > 82700000 AND
 Fwd IAT Std > 19500000: ATTACK (9403.0/1.0)

 Timestamp = 7/7/2017 4:03: NORMAL (4320.0)

 Timestamp = 7/7/2017 3:57 AND
 Avg Fwd Segment Size > 6.4: NORMAL (4265.0)

 Timestamp = 7/7/2017 3:59: NORMAL (4257.0)

 Timestamp = 7/7/2017 4:01: NORMAL (4208.0)

 Timestamp = 7/7/2017 4:02: NORMAL (4166.0)

Total Length of Fwd Packets <= 14 AND
```

Therefore, when the network stream flows through ABM, series of zero and one are generated as an output from the model to be passed to the Aggregation module which is a sub-module in the DM for aggregation with the outcomes from other models within the IDS module.

Signature Based Model (SBM): this uses an approach in which possible known intruders' behaviors are modeled and an alarm is raised when a match is detected. Therefore, already known characteristics of intruders were used for this model so that if the characteristics of the current user match already known characteristics of intruders, then intrusion is suspected and one "1" is assigned to such host otherwise zero "0" is assigned.

This model also used the traffic dataset of the Canadian Institute of Cyber Security (CIC) from the University of New Brunswick to extract known patterns of attackers via the use of machine learning algorithm. In line with the dataset, all characteristics that matched known attacks are represented with one "1" and any other is represented with zero "0" in the decision field of this model. Then the series of zeros "0" and ones "1" that are outputted from this model are also sent to the aggregate's module in DM for aggregation with other outcomes from the other two models.

Decision Module (DM): this consists of an aggregation section that uses the principle of "AND gate" based on the signal of zero and ones received from ABM, PBM, and SBM to filter out intrusive activities that will then be forwarded to administrator interface for a necessary response. The "AND gate" is as shown in Table 1.

Hosts suspected by the system to be intruders are red colored while others will be blue colored. In case the network administrator realizes a, red-colored host is not an intruder and he responded "NO" then such will be sent to a false positive alarm counter. The false positive alarm counter helps in the calculation of the false positive alarm rate from the system.

Table 1: True Table for Final Decision (FD) in Aggregation Module.

User id	A (PBM)	B (ABM)	C (SBM)	FD
SAL	0	0	0	0
Mgr	0	0	1	1
Mgr	0	1	0	1
Mgr	0	1	1	1
Mgr	1	0	0	1
SAL 1	1	0	1	1
SAL 2	1	1	0	1
SAL 3	1	1	1	1

Intrusion Prevention Module (IPM): This is an IPM section where the administrator interface is displayed, and it majorly consists of a series of user identities whose activities are colored red if intrusive and are green colored if not intrusive. The section allows the system administrator to block a user and take note of false positive alarms from the system.

Table 2: Host Identity on Administrator Interface.

tblSystem		
ID	System Name	IP Address
1	IDS-SYSTEM-1	192.168.203.24
2	IDS-SYSTEM-2	98.136.189.41
3	IDS-SYSTEM-3	192.168.255.02
4	IDS-SYSTEM-4	172.27.14.93
5	IDS-SYSTEM-5	172.27.12.109
6	IDS-SYSTEM-6	192.168.431.50
7	IDS-SYSTEM-7	172.27.15.69
8	IDS-SYSTEM-8	172.27.14.94
9	IDS-SYSTEM-9	172.27.12.63
10	IDS-SYSTEM-10	98.136.189.40

RESULTS

Metric Involved

The metrics that were used to evaluate each of the three hybridized models include overall accuracy, sensitivity, specificity, precision, Matthews Correlation Coefficient (MCC), and Balanced Classification Rate (BCR) as shown in Equations 1-6.

$$Accuracy(ACC) = \frac{TP + TN}{TP + FP + TN + FN} \quad \textbf{(1)}$$

$$Sensitivity(SEN) = \frac{TP}{TP + FN} \quad \textbf{(2)}$$

$$Specificity(SPE) = \frac{TN}{FP + TN} \quad \textbf{(3)}$$

$$\Pr ecision(PRE) = \frac{TP}{TP + FP} \quad \textbf{(4)}$$

$$MCC = \frac{(TP * TN) - (FP * FN)}{\sqrt{(TP + FP)(TP + FN)(TN + FP)(TN + FN)}} \quad \textbf{(5)}$$

$$BCR = \frac{1}{2} * \left(\frac{TP}{P} + \frac{TN}{N} \right) \quad \textbf{(6)}$$

Where,

True Negative (TN) is a measure of the number of non-intrusive events rightly classified as non-intrusive.

True Positive (TP) is a measure of intrusive events classified rightly as intrusive.

False Positive (FP): a measure of non-intrusive events misclassified as intrusive.

False Negative (FN) is a measure of intrusive events misclassified as non-intrusive.

Total intrusive events (P) are a measure of all the possible intrusive events in the sampled traffic.

Total non-intrusive events (N) are a measure of all the possible non-intrusive events in the sampled traffic.

Simulation Results

The simulation results of each of the three models using UNB-CIC data set in term of True Positive Rate, True Negative rate, False Positive rate, and False Negative rate. Accuracy, Sensitivity, Specificity, Precision, Matthews Correlation Coefficient (MCC), and Balanced Classification Rate (BCR) were carried out also presented in Tables 3 and 4 for comparative evaluation. Such metrics were used as a result of their merits in the evaluation of binary classification task.

Table 3: Comparative Analysis of Basic Metric Rates for PBM, ABM and SBM.

Model	True Positive rate	True Negative rate	False Positive rate	False Negative rate
PBM ($ZERO_r$)	0.857	0.167	0.143	0.833
ABM (PART)	1.000	1.000	0.000	0.000
SBM (Cubic)	1.000	0.946	0.004	0.054

Table 4: Comparative Analysis for PBM, ABM and SBM on UNB-CIC data in term of Accuracy, Sensitivity, Specificity, Precision, MCC and BCR.

MODEL	ACC	SEN	SPE	PRE	MCC	BCR
PBM	0.85	0.857	0.833	0.706	0.031	0.8185
ABM	0.81	1.0	1.0	1.0	1.0	0.558
SBM	0.994	0.948	0.995	0.996	0.943	0.973

In line with the parameters used for the above analysis, it can be seen that each of the models has its own detection capability, hence when such detection capability is combined in the hybridized model better detection of intruders can be achieved. Moreso, the features that were used by each model for detection differ from each other hence making the system to be robust.

CONCLUSION

This paper presented hybrid IDS architecture that provides an enhancement on IDS via the use of human defined security policy. The proposed architecture has the ability for dynamic adaptability to the mutational and diverse attitudes of hackers. Its practicality can be assured, since most of the embedded approaches in it are well known and have been implemented before. After implementation, it is expected to perform better in the detection of intruders.

REFERENCES

1. Abdurrazaq, M., R. Bambang, and B. Rahardjo. 2015. “DIDS Using Cooperative Agents Based on Ant Colony Clustering”. *Journal of ICT Research and Application*. 8(3). http://journals.itb.ac.id/index.php/jictra/article/view/937

2. Al-Yaseen, W.L., Z.A. Othman, and M.Z.A. Nazri. 2016 . “Real-Time Intrusion Detection System Using Multi-agent System”. *International Journal of Computer Science*. 43:1. IJCS_43_1_10

3. Balogun, A.O. and R.G. Jimoh. 2015. “Anomaly Intrusion Detection using an Hybrid of Detection Tree and K-Nearest Neighbor”. *Journal of Advances in Scientific Research and Applications (JASRA)*. 2(1): 67-74. http://uilspace.unilorin.edu.ng:8080/jspui/bitstream/123456789/257/1/JASRA-V2N1P7.pdf

4. Banik, S.M., D.S. Bernsen, and M. Javed. 2013. “Intelligent Mobile Agent-based Intrusion Detection System”. ACMSE’13, April 4–6, 2013, Savannah, GA. ACM 978-1-4503-1901-0/13/04.{17}

5. Biswas, A., M. Sharma, T. Podder, and N. Kar. 2015. “An Approach towards Multilevel and Multiagent based Intrusion Detection System”. *International Conference on Advanced Communications, Control and Computing Technologies*. doi.org/10.1109/ICACCCT.2014.7019417

6. Ganapathy, S., P. Yogesh, and A. Kannan. 2012. “Intelligent Agent-Based Intrusion Detection System using Enhanced Multiclass SVM”. *Computational Intelligence and Neuroscience*. 2012: 10-18. do:10.1155/2012/850259.

7. Gibson and Clouse. 2017. “Intrusion Detection and Ubiquitous Host to Host Encryption”. https://arxiv.org/abs/1711.08075

8. Holtz, M.D., B.M. David, and R. Timoteo. 2011. “Building Scalable Distributed Intrusion Detection System Based on the MapReduced Framework”. *Revista Telecomunicacoes*. (13)2: 22-31

9. Hodo, E., X. Bellekens, E. Iorkyase, A. Hamilton, C. Tachtatzis, and R. Atkinson. 2017. “Machine Learning Approach for Detection of Non TOR Traffic. *ARES' 17*. 17(2): 1-6.

10. Jaisankar, N., R. Saravanan, and K.D. Swamy. 2009. “Intelligent Intrusion Detection System Framework Using Mobile”. *International Journal of Network Security & Its Applications (IJNSA)*. 1(2): 72-88.

11. Jain, C. and A.K. Saxena. 2016. “General Study of Mobile Agent Based Intrusion Detection System (IDS)”. *Journal of Computer and Communication*. 2(4): 93-98.

12. Kajal, K.N and B.B. Komal. 2015. “Distributed Intrusion Detection System Using Mobile Agent Technology". *International Journal of Engineering Research and General Science*. 3(2): Part 2: 319-323.

13. Khobragade, S. and P. Padiya. 2015. “Distributed Intrusion Detection System Using Mobile Agent”. “International Journal of Engineering and Innovative Technology (IJEIT)”. 5(4).

14. Kumar, G. and K. Kumar. 2013. “Design of an Evolutionary Approach for Intrusion Detection”. *The Scientific World Journal*. Article ID 962185. https://doi.org/10.1155/2013/962185

15. Kumar, D. and T. Kamlesh. 2016. “A New Intrusion Detection Benchmarking System”. In: FLAIRS Conference. 4(1): 252–256.

16. Lee, Y., Y. Sang-Guun, J. Kim and S. Lee. 2011. “Specification-Based Intrusion Detection System for WiBro”. 5th International Conference on Convergence and Hybrid Information. Pages 445-455. DOI: 10.1007/978-3-642-24082-9_55

17. Mamun. M.S.I., A.F.M. Kabir, M. Hossen, and M.R.H. Khan. 2009. “Policy Based Intrusion Detection and Response System in Hierarchical WSN Architecture”. https://www.researchgate.net/publication/258727145

18. Saad, R., S. Manickam, and S. Ramadass. 2013 . "Utilizing Data Mining Approaches in the Detection of Intrusion in IPv6 Network: Review & Analysis". *International Journal of Network Security*. 4: 2152-5064.

19. Srivastava, S.S., N. Gupta, S. Chaturvedi and S. Ghosh. 2011. “A Survey on Mobile Agent based Intrusion Detection System”. International Symposium on Devices MEMS, Intelligent Systems & Communication (ISDMISC) 2011 Proceedings published by International Journal of Computer Applications® (IJCA) 19.

20. Tian-rui. L., and Pan, W.M. 2005. “Intrusion Detection System based on New Association Rule Mining Model”. 2005 IEEE International Conference on Granular Computing. 2(1): 512-515. doi: 10.1109/GRC.2005.1547344

21. Trushna, T., K. Patil, and C. Banchhor. 2013. “Distributed Intrusion Detection System”. *International Journal of Advanced Research in Computer and Communication Engineering*. 1901-1903.

22. Wu, S. and Y. Chen. 2008. “An Embedded Intrusion Detection System Model for Application Program”. 2008 IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application. doi : 10.1109/PACIIA.2008.394.

SUGGESTED CITATION

Mustapha, I.O., J.B. Awotunde. S.O. Ganiyu. and A.M. Oyelakin. 2024. “Hybrid Policy-Based Architecture for Intrusion Detection System”. *Pacific Journal of Science and Technology*. 25(1): 42-49.