EEJOURNALS OPEN ACCESS
EURASIAN EXPERIMENT JOURNAL OF ENGINEERING(EEJE) ISSN: 2992-409X
©EEJE Publications Volume 4 Issue 1 2023

System Testing, Integration and Development; A case study of cloud log management server

Emeka Okorie, Iloka B.C. and Don-anyanwu C. P.

Department of Computer Science Tansian University Umunya, Nigeria

ABSTRACT

This research deals with the multi intrusion detection model developed for the case study cloud log management server. The security model was also validated and then compare with other state of the art threat detection algorithm to determine percentage improvement in threat detection accuracy. After the validation, the system was integrated into the testbed and then used to secure the organization against intrusion. The validation result of the multi-level intrusion detection system developed for the security of log management cloud based server. The validation result recorded MSE of 2.47e-05Mu and R= 0.99445. The implication of the results showed that the new algorithm developed was able to correctly monitor, detect and prevent threat penetration to cloud based server. In conclusion, the results showed that the performance of the new system was better due to its multi layered configuration of neurons to enhance data processing and computation in the hidden layers, then right choice of activation used, training algorithm adopted and also the quality of data used to train the neural network and achieve the threat detection algorithm. These features of the new algorithm make it to standout from the others with better performance.

Keywords: Multi intrusion, detection model, cloud and management server

System testing of the multi level intrusion system

This presented the performance evaluation of the intrusion detection system developed. To evaluate the performance, means square error, regression and validation models in [1] were adopted. The regression result was presented in figure 1;

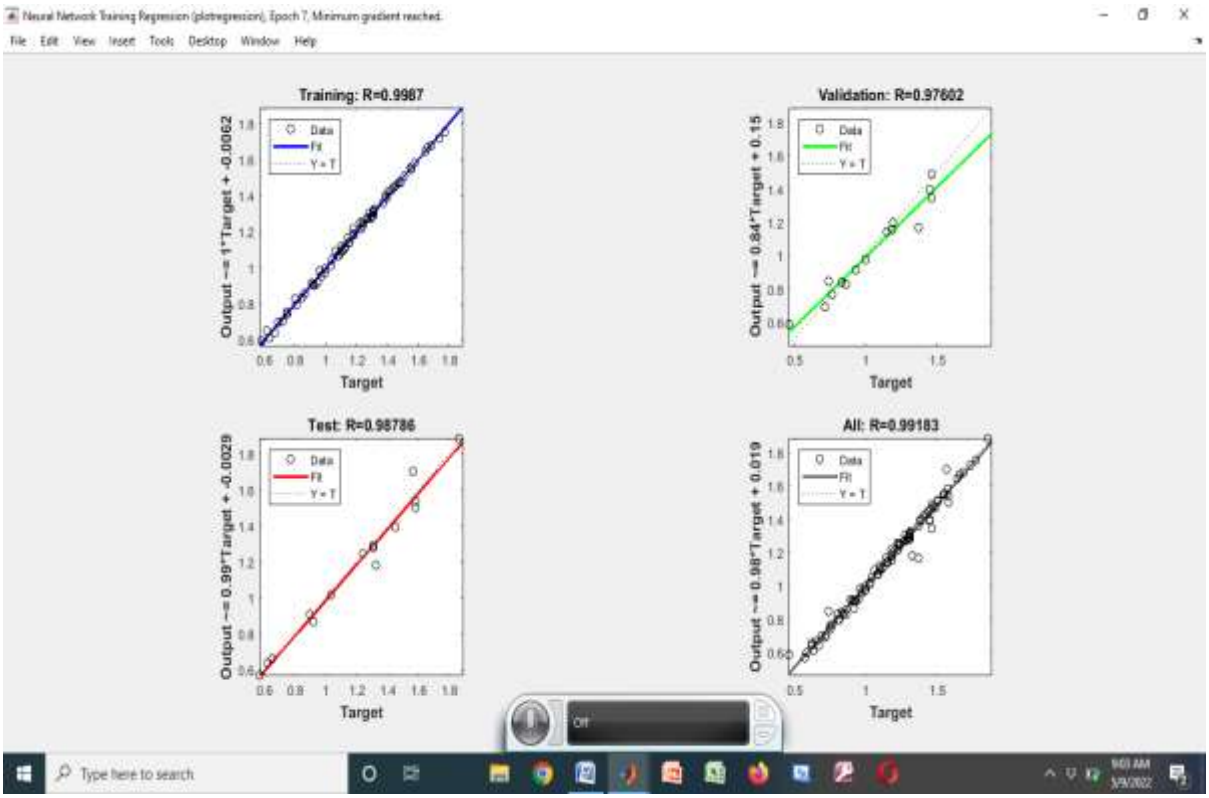

Figure 1: Regression performance of the neural network algorithm

Regression analyzer is an important tool developed for solving time series problem to check the ability of the security system to detect incoming threat on the cloud network correctly. The aim here is to achieve a regression value approximately or equal to 1, which indicated excellent threat detection result. From the figure 1, the regression result was measured using the average of the multi sets and the overall score is R= 0.99183. The implication of this result showed that algorithm was able to correctly detect threat from the hacker's nodes and prevent it from reaching the cloud. The next result presented the MSE performance as in figure 2;

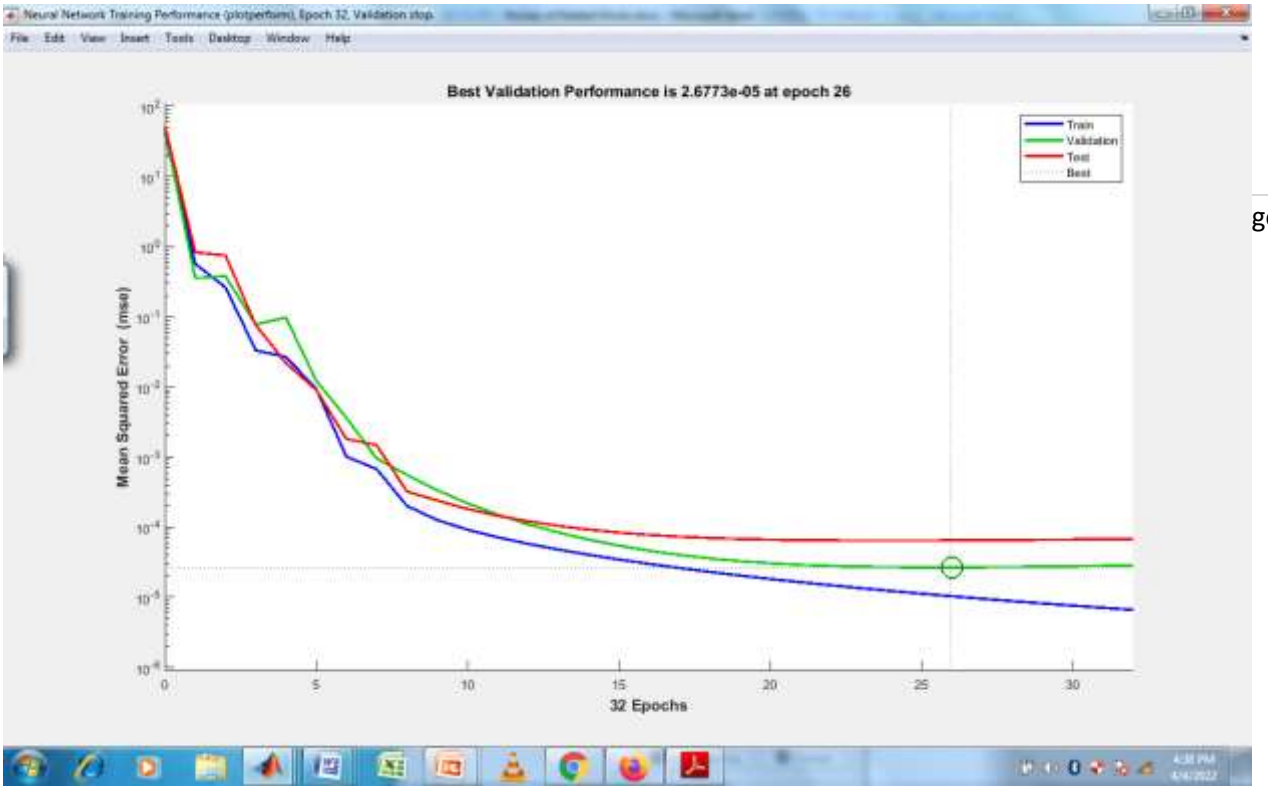

Figure 2: MSE performance

The MSE result in figure 2 presented the error achieved in the neural network training process toward the development of the security model. The aim of the researcher here is to achieve MSE of approximately zero which implied tolerable error during the training process. From the result achieved, the MSE is 2.6773e-05Mu. The implication of this result showed that the training process was very good as the error achieved is approximately zero. To further justify this results achieved, the tenfold cross validation was used which iteratively evaluated the MSE and R in ten-folds and the average reported as the overall system result as shown in the table 1.

Table 1: Validation of the Results

S/N	MSE	Regression
1	2.6773e-5	0.99183
2	2.0754e-5	0.99785
3	2.1475e-5	0.98867
4	2.5845e-5	0.99823
5	2.9733e-5	0.99787
6	2.4466e-5	1.00000
7	2.0552e-5	1.00000
8	2.7536e-5	0.97385
9	2.1866e-5	0.99844
10	2.8075e-5	0.99778
Average	2.47E-05	0.99445

The table 1 presented the validation result of the multi-level intrusion detection system developed for the security of log management cloud based server. The validation result recorded MSE of 2.47e-05Mu and R= 0.99445. The implication of the results showed that the new algorithm developed was able to correctly monitor, detect and prevent threat penetration to cloud based server [2-6].

Comparative Analysis

The comparative analysis drew insight from a recent work on qualitative analysis of machine learning based intrusion detection system by Binita (2021) and compared the new multi intrusion detection system developed with the selected algorithm in the study as shown in table 2;

Table 2: Comparative Analysis

Regression algorithms	**Regression**

Logistic regression	0.730
Decision tree	0.980
K-NN	0.950
Random forest	0.9800
GausianNB	0.9600
Multi-level intrusion system	0.9945

The table 2 presented a comparative analysis of the new system developed with the existing systems, and were analyzed in the figure 3;

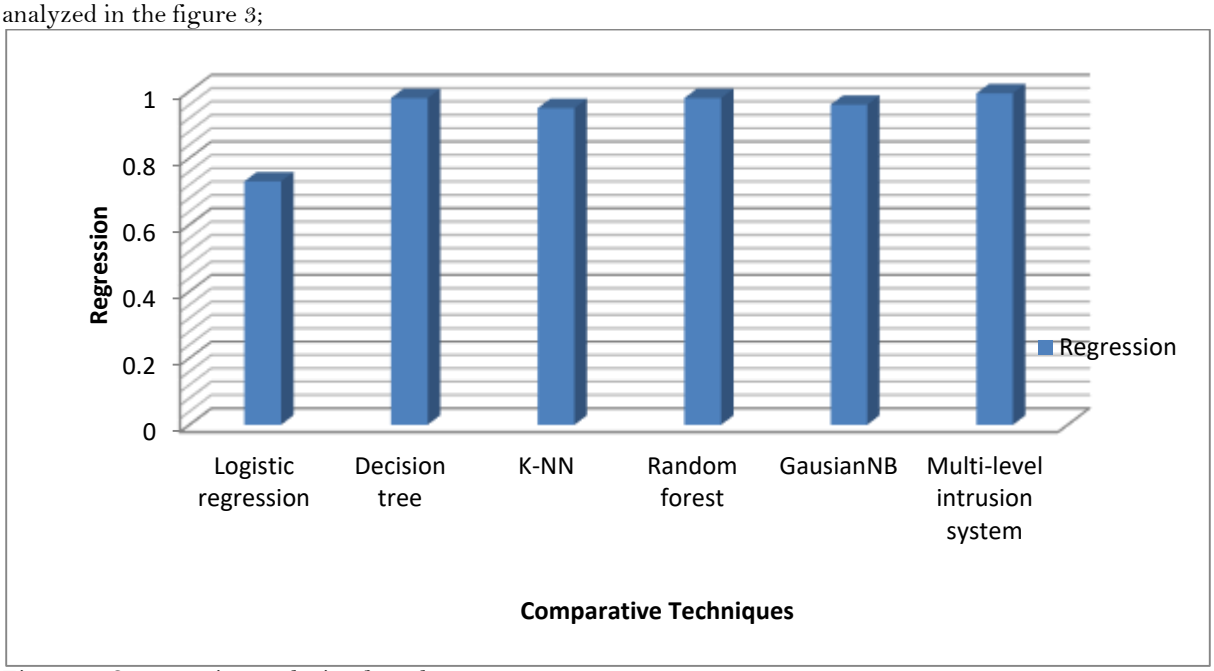

Figure 3: Comparative analysis of results

The figure 3 presented a comparative analysis of the various threat detection algorithms recently developed and the new multi intrusion detection system. From the result, it was observed that the performance of the new system was better due to its multi layered configuration of neurons to enhance data processing and computation in the hidden layers, then right choice of activation used, training algorithm adopted and also the quality of data used to train the neural network and achieve the threat detection algorithm. These features of the new algorithm make it to standout from the others with better performance [7-10].

System Integration

This process involves the implementation of the new system that interfaces with the existing system. The basic goal of this process is to solve the problems relating to the new system implementation. Software system integration begins with the definition of the existing systems or solutions. For instance, if the existing system uses outdated technology, a new system based on the currently available improvements over the existing system is proposed. In this case the multi intrusion detection algorithm was used, having tested and validated with results better than the conventional system, replace the existing encryption firewall as shown in figure 4.

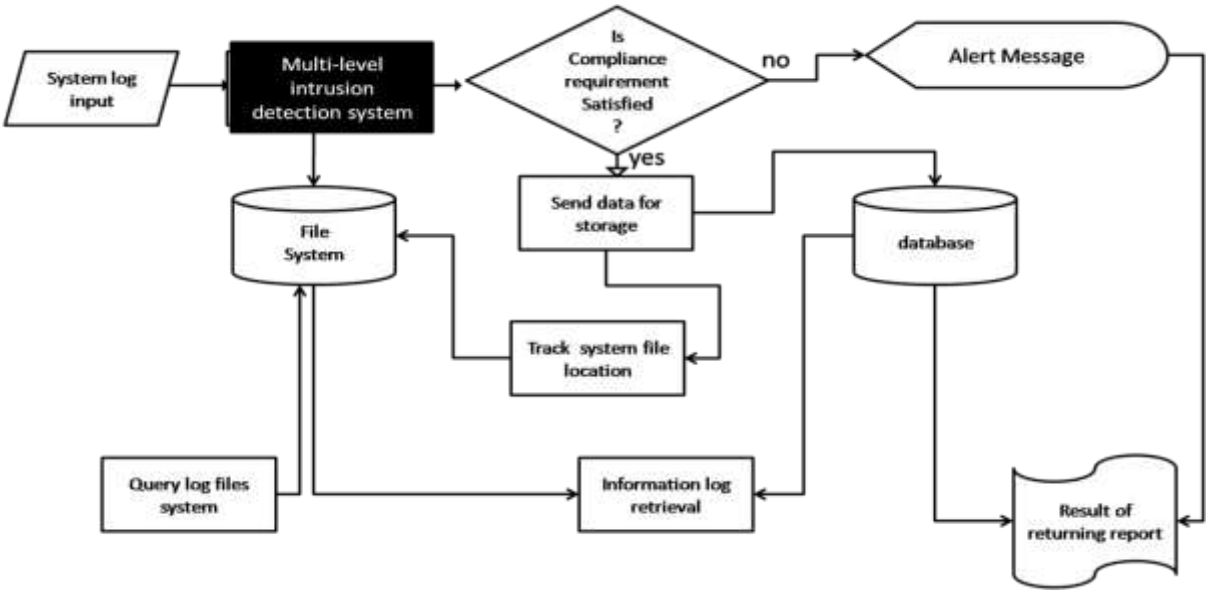

Figure 2: System Integration workflow

The figure 2 presented the system integration workflow which showed the performance of the multi level intrusion detection system embedded on the case study cloud based architecture. The security model was positioned at the gateway to the cloud server to train every user log input and allows throughput to non threat log requests, while the threat detected are flagged off and notified for instant control actions [11-13].

System Documentation

This is a very important part of the system development. The essence is to ensure future maintenance of the new system. The researcher properly documented the entire system for future use. The source code was organized and label with comments that elaborates every section of the system. This will help the software engineer, programmers and system analyst to have an understandable behaviour of the system and this will go a long way to help them deploy and maintain it after the system must have been configured and implemented. Also reference documentation (User guild) was created to help the user understand how to accomplish a given task with the new system [14-16].

Change Over to the New System

This explains how the newly developed system will be put to use. While trying to introduce a new system, the following has to be considered

i. Changeover style
ii. Conversion location
iii. Conversion modules

Changeover style

This refers to the speed at which we introduce the new system. This process could either be direct or parallel. The parallel method is applied when two system are allowed to operate simultaneously. In this case the direct change over approach was adopted as the new system is more reliable than the existing system [17-18].

Conversion location

This is the immediate organizational span of the new system introduction. This process could be pilot, simultaneous or phased. The pilot changeover process involves implementing the new system in some selected part of an organization. The phase changeover involves introducing the new system in other places of an organization in phases. While simultaneous changeover involves the implementation of the new system in all location in one move and completely eliminating issues of different parts of the organization utilizing various systems at the same time. In this work the simultaneous changeover style was used to deploy the security system, to all the gateways to the server for proper security and log management.

Conversion modules

This approach involves introducing the new system module by module or a whole system method that involves the entire developed system to be installed at a go. The approach selected among these three listed approaches will influence the system sustainability, cost, time and risk associated with the new system changeover. There are always a lot of risks associated in the deployment of every new system and this multi-level intrusion detection system is not an exception if not properly taken into consideration. Therefore the researcher adopted the simultaneous approach which involves implementation of the new system at all location in all time. This choice was made because from the empirical study, it was observed that the existing

system focused on the security of the packet and not the server, hence the choice of the simultaneous conversion approach [19-21].

User Training

This process is an important guild for both the new and existing users. It provides the required regulations and user guild for the system installation and effective system operability. The researcher implemented this guild in a simplified well comprehensive manner and user friendly with enough details pointing every module of the entire system.

CONCLUSION

The two security algorithms developed were married as multi level intrusion detection system and implemented with Simulink. The result after testing and validation recorded MSE of 2.47e-05Mu and R= 0.99445. The implication of the results showed that the new algorithm developed was able to correctly monitor, detect and prevent threat penetration to cloud based server. A comparative analysis was also conducted with other threat detection algorithms and from the result, it was observed that the performance of the new system was better due to its multi layered configuration of neurons to enhance data processing and computation in the hidden layers, then right choice of activation used, training algorithm adopted and also the quality of data used to train the neural network and achieve the threat detection algorithm. These features of the new algorithm make it to standout from the others with better performance. In conclusion, the results showed that the performance of the new system was better due to its multi layered configuration of neurons to enhance data processing and computation in the hidden layers, then right choice of activation used, training algorithm adopted and also the quality of data used to train the neural network and achieve the threat detection algorithm. These features of the new algorithm make it to standout from the others with better performance

REFERENCES

1. Debar H., M. Dacier, and A. Wespi (1999). Towards a Taxonomy of Intrusion Detection Systems, Int'l J. Computer and Telecommunications Networking, vol. 31, no. 9, pp. 805–822,1999.
2. deep learning," in Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, (ACM, Toronto, Canada), 2291–2293
3. Dhage S., Meshram B., Rawat R., Padawe S., Paingaokar M., Misra A., (2011) "Intrusion Detection System in Cloud Computing Environment", International Conference and Workshop on Emerging Trends in Technology (ICWET), pp. 235-239.
4. Doyen Sahoo, Chenghao Liu, and Steven CH Hoi. (2019) malicious url detection using machine learning: A survey. arXiv preprint arXiv:1701.07179.
5. ENISA. (2020). ENISA Threat Landscape 2020 – Web-based Attacks. DOI: 10.2824/552242 [Online] Available at: https://www.enisa.europa.eu/publications/webbased-attacks; Retrieved on 2/19/2022
6. Irfan Gul and M. Hussain (2011). Research on Distributed Cloud Intrusion Detection Model appear in International Journal of Advanced Science and Technology Vol. 34, September, 2011
7. JaeHyuk Jang (2010). Cisco, *Cloud computing: Drive Business Paradigm Shift*, 2010.
8. Jiang, Y., Hamer, J., Wang, C., Jiang, X., Kim, M., Song, Y., et al. (2018). Securelr: secure logistic regression model via a hybrid cryptographic protocol. *IEEE ACM Trans. Comput. Biol. Bioinf* 16, 113–123. doi:10.1109/TCBB.2018.2833463
9. Jolera. (2020). 3 Ways AI Prevents Phishing Attacks. [Online] Available at: https://www.jolera.com/3-ways-ai-prevents-phishing-attacks/; Retrieved on 3/2/2022
10. Jun Ho Lee, Min Woo Park and Jung Ho Ecom (2011).Multi-level Intrusion Detection and Log Management in Cloud computing IEEE computer society, pp 552-555, Feb.2011.
11. Kenny S. and B. Coghlan (2005). Towards a Grid-Wide Intrusion Detection System, Proc. European Grid Conf. (EGC 05),Springer, pp. 275–284,2005.
12. Kento S, Hitoshi. S, Satoshi. M, (2009). "A Model-based Algorithm for Optimizing I/O Intensive Applicationsin Clouds using VM-Based Migration", 9th IEEE/ACM International Symposium, Cluster Computing and Grid, 2009.
13. Lei, Y., Chen, S., Fan, L., Song, F., and Liu, Y. (2020). Advanced evasion attacks and mitigations on practical ml-based phishing website classifiers. *arXiv*
14. Liu, J., Juuti, M., Lu, Y., and Asokan, N.. (2017). "Oblivious neural network predictions via minionn transformations," in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, October 2017, 619–631
15. Mazzariello C., Bifulco R. and Canonico R. (2010) "Integrating a Network IDS into an Open Source Cloud Computing Environment", Sixth International Conference on Information Assurance and Security, pp. 265-270.
16. Shailendra Rathore, Pradip Kumar Sharma, and Jong Hyuk Park. Xssclassi_er: An effcient xss attack detection approach based on machine learning classi_er on snss. JIPS, 13(4):1014{1028, 2017.

17. Solomon Ogbomon Uwagbole, William J Buchanan, and Lu Fan. Applied machine learning predictive analytics to sql injection attack detection and prevention. In 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), pages 1087{ 1090. IEEE, 2017.
18. Uday Trivedi and Munal Patel. A fully automated deep packet inspection veri_cation system with machine learning. In 2016 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), pages 1{6. IEEE, 2016.
19. Vieira K., Schulter A., Carlos B. Westphall, and C. Westphall M. (2010), "Intrusion Detection for Grid and Cloud Computing", IEEE Computer Society, pp. 38-43.
20. Vieira, K. Schulter, A. Westphall, C.B. and Westphall, C.M. (2010). Intrusion Detection for Grid and Cloud computing IEEE computer society,vol 12, issue 4, pp. 38 – 43,2010.
21. Wang, J., Zhang, J., Bao, W., Zhu, X., Cao, B., and Yu, P. S. (2018). "Not just privacy: improving performance of private deep learning in mobile cloud," in Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining London, United Kingdom, January 2018, 2407–2416. testPerformance = perform(net,testTargets,y).

Emeka Okorie, Iloka B.C. and Don-anyanwu C. P. (2023). System Testing, Integration and Development; A case study of cloud log management server. *EURASIAN EXPERIMENT JOURNAL OF ENGINEERING (EEJE)* 4(1) 132-138