Pilot Study on Web Server HoneyPot Integration Using Injection Approach for Malware Intrusion Detection. Computing, Information Systems

Article · March 2024

DOI: 10.22624/AIMS/CISDI/V15N1P2

3 authors:

Bridget Malasowe
University of Delta Agbor

Fidelis Aghware
University of Delta, Agbor, Delta State, Nigeria

Edim Bassey Edim
University of Calabar

Pilot Study on Web Server HoneyPot Integration Using Injection Approach for Malware Intrusion Detection

[1]Malasowe Bridget, [2]Aghware Fidelis & [3]Edim, Bassey Edim
[1,2]Department of Computer Science, Faculty of Computing
University of Delta, Agbor, Delta State, Nigeria,
[3]Department of Computer Science, Faculty of Physical Science
University of Calabar, Calabar, Nigeria
E-mails: [1]bridget.malasowe@unidel.edu.ng, [2]fidelis.aghware@unidel.edu.ng
[3]edime@unical.edu.ng

Abstract

The digital world is rapidly coming together as well as transforming a lot of our valued data onto digital forms. Its consequent dissemination eased via the advent of the Internet has also encountered many attacks due to predictable responses from many users – leading up to social engineering and exploits on trust-level of users. The use of deception is now playing a very prominent role in enhancing data security. Several approaches abound to discourage and redirect challenges (via the use of honeypot), and to detect such intrusive activities (via an intrusion detection systems). These have been successfully used to minimize security breaches. We explore a deep learning deception-based honeypot to minimize breaches by adversaries. Used on web servers, it is equipped with identification capabilities as the system learns and defends a user system against intrusive actions. Our confusion matrix shows model has sensitivity of 0.81, specificity 0.08, and prediction accuracy of 0.991 with an improvement rate of 0.39 for data that were not originally used to train.

Keywords: Web Server, HoneyPot, Integratio, Injection Approach, Malware Intrusion Detection

CISDI Journal Reference Format
Malasowe B., Aghware, F. & Edim, B.E. (2024): Pilot Study on Web Server HoneyPot Integration Using Injection Approach for Malware Intrusion Detection. Computing, Information Systems, Development Informatics & Allied Research Journal. Vol 15 No 1, Pp 13-.28. dx.doi.org/10.22624/AIMS/CISDI/V15N1P2. Available online at www.isteams.net/cisdijournal

1. INTRODUCTION

The continued quest for technological advances in our society today – has continued to birth new threat to digital data processing (Said et al., 2023). The capability to safeguard data is now very critical, and has become am art. Network administrators must now be prepared to protect both the network system and data with extreme and diverse measures (Ojugo & Yoro, 2020a, 2021b, 2021a). An example is adoption of deception tools called honeypots (Broadhurst et al., 2018). Honeypots simply tricks an adversary into believing they have accessed the network – since, the only way a network administrator can block access is to is to check the history of users logs to ascertain who accessed the network and how the resources were accessed (Cooper, 2015; Linh, 2018). Thus, honeypots use subterfuge means to lure an adversary or intruder – and keep them around the network long enough for their identity and other of their credentials to be extracted and revealed without them knowing. However, it is a resources that functions over a network with a with a false input data to mimic the illusion of real life data (Mahajan & Sharma, 2015).

This is designed in a way that it behaves as the real host to attract and adversary. It is expected to practically keep engaging the adversary long enough to be able to achieve the exploit the required information needed. It is expected to obtain and monitor all activities on the network and its operations – ensuring that any adversary using a backdoor or Trojan horse malware is kept at bay (Harris, 2020). Thus, it stores the interaction between an adversary and the honeypot scheme – via analytic tools that seeks to investigate the reason or reasons for the breach or attack (Catrantzos, 2010; Chen et al., 2022; Ojugo & Eboka, 2018b, 2020b).

A honeypot is designed to fit within a firewall. It functions is to reverse-engineer the normal workings of a regular firewall so that as against controlling activities that enters into the network. This conrols the data traffic into the network, and goes further to restrict the feedback sent back from the network system (Allenotor et al., 2015; Allenotor & Ojugo, 2017). It lures an intruder, and serves a variety of purposes: (a) it allows an administrator to monitor an adversary as s(he) exploits the vulnerabilities of a network, (b) lets an administrator learn the network vulnerabilities and marks such for redesign, (c) reveals to an administrator full identity of any intruder via an extracted data from the activities on the network and (d) helps an administrator dissuade intruders from access to root directory (Ojugo et al., 2014; Ojugo & Otakore, 2018b).

Its study of an adversary's activities helps the system developer to generate a more secured and possibly invulnerable network system in time. With data traffic anomaly detected, honeypot listens to all incoming traffic, monitors and study data traffic logs to observe anomalies and detect its source (Obruche et al., 2024). Honeypot simulates various resource (e.g. web/mail/app servers, database-server, and firewalls).

By design, it mimics a system an intruder will like to access. A good honeypot keeps an adversary engaged and unaware he/she is being tricked and/or monitored. Thus, honeypots are best installed inside firewalls so that they can be better controlled. There is lesser control when they are installed outside of firewall (Akazue, Asuai, et al., 2023; Ibor et al., 2023; Oladele et al., 2024; Yoro, Aghware, Akazue, et al., 2023).

Deception, will always play a relatively implicit, prominent role as it is fundamentally different from conventional security modes (Ojugo & Oyemade, 2021) – because, it has been used to manipulate an adversary to act in ways that have proven more beneficial to a network administrator. It is inherent in measuring firewalls, gateways and intuition detection systems. Thus, used in conjunction with IDS and machine learning – yielded great results (Akazue, Debekeme, et al., 2023; Akazue & Omede, 2023). Honeypots have a great potentials as the they can detect new attackers before network database is compromised.

Thus, study aims to: (a) deploy a deep learning framework to handle such a chaotic, dynamic and complex filtering, to ultimately enhance adequate classification, (b) design the new system to resolve conflicts in data en/de(coding) of data for hybrid technique adopted, and (c) resolve conflict in heuristics adopted by the various schemes at play in the proposed honeypot system as well as compensate for such hybridization

2. MATERIALS / METHODS

2.1. On Honeypot Architectures
Odiakaose et al. (2023) investigated the gaps in honeypots implemented on a virtual machine (VM). Since VM are complex, they are vulnerable to exploits if misconfigured, and yield high risk of honeypots running on them. They explored internal-sensors running within a honeypot to record invoked system calls, their responses and data about which processes the calls. They, also used external-sensors to minimize errors of internal sensors – noting external-sensors can intercept data traffic of a honeypot to monitor internal sensors (Odiakaose et al., 2023) and agrees with (Kowalski et al., 2008; Matthew D. Waters, 2016). Akazue et al., (2023) focused on trade-off issues between system accuracy to reduce false positive and false positive error rates within the high level of interaction with the honeypots in anomaly intrusion detection scheme.

Shadow honeypot was used so that incoming users request to the server will execute the shadow honeypots. This embedded honeypot monitors the behaviors of each request. If such request is confirmed to be malicious, all executed activities relation to such request will be returned back immediately. Al incoming requests are processed via an anomaly detection scheme. The confidential malicious requests are sent to the honeyport shadow, then the ones classified as genuine are directed to the production sever (Akazue, Yoro et al., 2023).

Omede and Okpeki (2023) research work was on low/high hybrid fused interaction honeypot to achieve low resources requirements to implement for the implantation of low interaction Honeyports and to imitate all responses in high interactions. A proxy approach is used by the Honeyport to generate the virtual hosts and redirecting data traffic. Each virtual host emulates the full system in high-interaction honeypot via on-demand invoke calls of such virtual host minimize resource consumptions. High-interaction are invoked automatically only when traffic that requires such high-interaction honeypots arrive at a host (Omede & Okpeki, 2023).

2.2. Honeypots in Malware Detection
In Eboka et al., (2020) research work, he proposed a honeypot that can effectively extract signatures for detecting polymorphic worms to achieve zero day detections. This mode of analysis is called the position aware distribution signature (PADS). It utilizes worms to monitor outgoing connections from an inbound to an outbound honeypot to easily identify worms. (Eboka & Ojugo, 2020). This agrees with (Muslikh et al., 2023; Okonta et al., 2013, 2014; Oyemade et al., 2016). Bako et al (2020) proposed a new mode to detect worms by monitoring the rate of their outgoing connections. This approach slows down the worm by regulating the rate of creation of a new outgoing connections that is based on a closed feedback loop control. The algorithm slowed down the spread of the malware approximately five times with sandbox to blacklist hosts and kill infected processes via multiple-feedbacks loops that intelligently queues connections, spreads of the worms which could be stopped with a significantly fewer number of hosts infected (Kabir Bako et al., 2019)..

2.3. Motivations / Statement of Problem
The challenge in design, layout, modelling and implementing of honeypots within a firewall using the injection approach to allow for ease of integration into a malware detection system so as to ensure security, confidentiality, non-repudiation, availability, integrity and privacy, even in the knowledge that adversaries will frequently attempt to breach the network as well as evade detection which has made this study design possible.

Thus, the study is motivated (Chibuzo & Isiaka, 2020; Durojaye et al., 2015; Malasowe et al., 2023; Ojugo & Eboka, 2018a, 2021) as:

1. Previous deployment and enhancement of security measures to ensure intruders or adversaries are identified cum kept at bay are error prone. Thus, the use of deception strengthen by the machine learning IDS scheme.
2. The use and adoption of firewalls with its faulty packet filtering method can make evasion for adversary and more possible. Thus, honeypots was use to engage these adversaries long enough to trace-back to their source machine.
3. The use of IDS schemes with its fusion with machine learning schemes – often finds machine learning schemes trapped at local minima. Also, it has been found to increase cost, while, also slowing down network speed due to its performance inefficiency and ineffectiveness. Thus, we adopt a machine learning scheme that will not get trapped at local minima; But, rather yield optimal solution with high false positives and true-negatives rates.
4. The chaotic nature of signature-based and anomaly-based detection data makes the adaptation of adversaries quite flexible and robust. Thus, we use the deep machine learning approach cum framework design to help effectively identify and classify malware.

Thus, study aims to: (a) deploy a deep learning framework to handle such a chaotic, dynamic and complex filtering, to ultimately enhance adequate classification, (b) design the new system to resolve conflicts in data en/de(coding) of data for hybrid technique adopted, and (c) resolve conflict in heuristics adopted by the various schemes at play in the proposed honeypot system as well as compensate for such hybridization

2.4. Experimental Testbed Setup

We adopt Adishi et al. (2023) for setting up a honeypot specifically for detecting and studying SQL injection. It employs the non-production systems for web-servers to make the honeypot appears as real as possible. This mode allows adversaries access the network to the level of data manipulation. The system is monitored cum restricted via use of certain procedures such as addition of a proxy between the database and web-servers. This will help to stop any SQL commands from reaching the network database. This design called a honey-net will simulate to a real network. Consequently help forward all SQL injection attacks to the honeypot with any server. Specifically, if the honeypot is designed to protect the database, the database is then populated with real-like data called honey-tokens (i.e. data that looks real enough and can be traced when it is accessed or used). The honey-net with firewalls, gateways and IDS configuration will ensure the uneasy access to the designated server (Adishi et al., 2022).

The system properly set-up will achieve: (a) the honeypot can easily identify the system vulnerabilities as an adversary tries to access the honey-net and used them, (b) the honey-net will gathered data that seeks to identify which methods was employed by the adversary to capture data, (c) the honey-net will seek alternatives to such attack with various purposes aimed to capture, delete or alter data in the server, (d) knowing that some adversaries access a network via malicious script on a user browser and/or via malware – the honey-net will monitor, redirect any user to other sites via designated URLs and/or detect user source IP, (e) for connection logs recorded, the honey-net will show which attack was done more frequently on the web application, (f) honey-net will seeks to unveil the source IP address of the adversaries as it employs trace-back to track the source and origin of the attacks, (g) with the connection logs studied, it tells the net-administrator the pattern of attacks that were successful and those that failed, (h) the recorded data on the honeypot will also further show tools and techniques are employed by hackers (Ejeh et al., 2022; Ejim, 2017; Iskandarov, 2020; Ojugo & Ekurume, 2021b, 2021a).

2.5. Proposed Experimental Phishing Detection Ensemble

It is known fact that hybrid have proven to be better than single models. However, we must be able to resolve conflicts arising from data encoding as transcribed from one heuristic to another, and the conflict of structural dependencies imposed on the hybrid. Thus, we use a hybrid memetic model with 3-blocks (Behboud, 2020; Ojugo & Nwankwo, 2021) as: (a) modular neural network, and (b) cultural genetic algorithm – as in figure 1 (Ojugo et al., 2013; Ojugo, Aghware, et al., 2015; Ojugo et al., 2021; Ojugo & Eboka, 2014, 2018c; Ojugo & Otakore, 2018a), and is further explained as thus:

a. Cultural Genetic Algorithm (GA): Fundamentally, a GA block uses 4 operators (initialize, fitness function and select, mutation and crossover) to uncover probable solution(s). A gene is fit if its value is close to optimal. This is a variant of GA, the Cultural GA (CGA), this variant uses4 belief spaces to define its solution these are: (1) the normative belief, this defines the specific value ranges to which a gene is bound, (2) domain belief, this contains knowledge about the task being undertaken, (3) Temporal belief, this contains knowledge about the availability problmes space and (d) spatial belief, this contains knowledge about the topography for the task . It also uses influence function to bridge the belief spaces and the gene pool to ensure any further modification of genes and still conform with the belief space(s). The CGA is expected to yield a result pool that does not violate its belief space and still assist in reducing the number of the potential gene generated by the GA until optimum is reached (Aghware et al., 2023b; Al-Qudah et al., 2020; Al-Turjman et al., 2019; Tomar & Manjhvar, 2015).
b. Kohen Modular Network (MNN) is a feedback network. The number one layer accepts input and re sends unbound to its second layer, this uses the transfer function to offer competitive computation. The competitive layer the maps similarity patterns into relations. The competitive layer then maps similarity patterns into relations. Pattern relations noticed are used to determine the result after training. We modified the parameters and carefully created our deep learning Kohonen MNN through a deep architecture. Our deep learning is achieved by training the network component via 2-stages namely the pre-trained, and fine-tuned processes as described in (Abakarim et al., 2018; Urbanowicz et al., 2018).

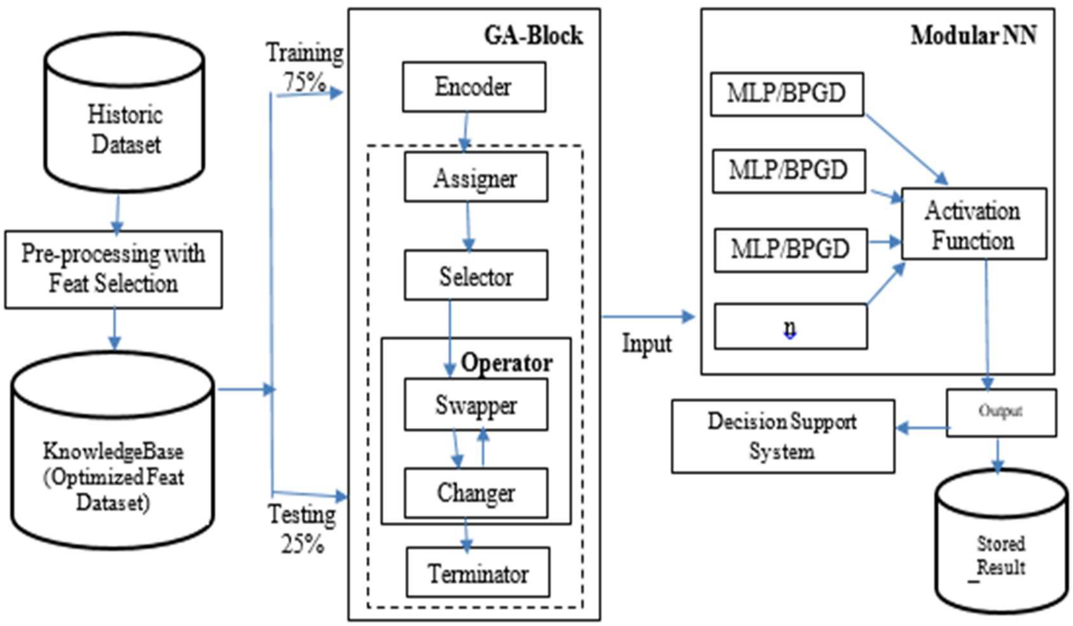

Figure 1. Genetic Algorithm Trained Modular Neural Network

2.6. Parameters/Features Tuning and Estimation

The rule-based optimized dataset's data labels are used to identify a model's prediction ability. At the input layer of our deep learning Kohonen map, we use 10 neurons (a neuron for each feature). The output layer is made up of two neurons (a neuron for each possible class of normal and benign rules). The learning rate(s), epoch size, transfer function, and hidden layer structure, are among the parameters to be tuned.

Thus, we used a 500-epoch Rectified Linear Unit Transfer Function (Ampatzidis et al., 2020). Mindful of our model's mean convergence time and precision, optimal values were found with epoch configuration (of 100, 300, and 500 respectively) (Goldstein et al., 2018; Pantazi et al., 2016) to yield the least amount of error, and best-fit results. The trial-and-error method was used to determine the number of hidden layers (Liu & Campbell, 2017; Nahavandi et al., 2022).

3. FINDINGS AND DISCUSSION.

3.1 Performance Evaluation for the Honeypot

Leveraging on (Aghware et al., 2023a; Wemembu et al., 2014) – in other to successfully deploy honeypot, the frame and setup architecture must be correct. While, there are no single rule on how to deploy, for efficiency – our 3-core elements of the honeypot to defines its architectural structure as thus:

3.1.1. Data Capture

Here, the proposed system tries to monitor all log activities within the honeypot. To ensure that effective data capture is done, the honeypot system uses several methods as no single layer can capture all the data required.

3.1.2. Data Control

The purpose of this segment is to control and contain the activity of an adversary. It gives access and entry to an adversary unto the network. But it entraps them by redirecting their entry and access to other networks to wreak havoc. This is achievable by isolating the target systems in the honey net with a layer two bridge device. The key here is to control the data and the amount of it the adversary has access to. Thus, this component grants an adversary access unto the network; But, controls the adversary's out-bound activities to wreak havoc on other networks by limiting these capability and permission.

In this study, we achieve this via the embedded honey net (this grants entry but blocks all outbound connections at the bridge). A well designed and implemented honey net blocks all outbound connections, stops the adversaries from harming other systems, and its real value is in its ability to learn and track what an adversary does once access is granted or have been obtained.

3.1.3. Performance of Memetic Algorithm

To compute accuracy of the ensemble, the performance was evaluated using Equation 1– yielding figure 2a as the confusion matrix that is supported by figure 2b as thus:

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \qquad (1)$$

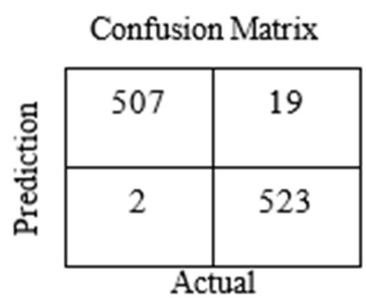

Figure 2a. Confusion Matrix

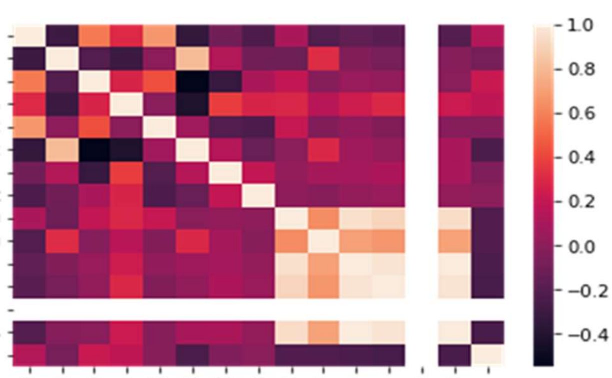

Figure 2b. Model Accuracy prediction

Figure 2b yields a performance of 99.1% classification accuracy with an improvement rate of 39% for the hybrid memetic modular neural network deep learning framework as in Table 1. And this agrees with (Barlaud et al., 2019; Ojugo, Eboka, et al., 2015b).

4. RESULTS AND FINDINGS

Simulation was carried out on testbeds using a single layered network of 1 to1 0 neurons, this yielded the highest f-score and least training loss time to results in the best number of layers. Adding a second and third hidden layer also yielded a good results with the highest number of neurons yielding the best scores. Table 4 shows the first layer configuration with 10 neurons and extra 2 neurons for optimal extra processing (Ojugo et al., 2013, 2021, 2023; Ojugo, Eboka, et al., 2015a).

The hidden layers of 9,11 neurons resulted in 1 99.1% f-score and 0.39 training loss value. The hybrid favours the use of a second hidden layer with greater value for f-score, which agrees with the findings. (Gao et al., 2021; Yuan & Wu, 2021; Zareapoor & Shamsolmoali, 2015)
.

Table 1. Training accuracy with 2-hidden layer configuration analysis

Hidden Layer	Precision	Recall	F1 Score	Iteration	Train Loss	Epoch
9, 1	0.91	0.92	0.83	29	0.393	500
9, 2	0.93	0.92	0.85	24	0.392	500
9, 3	0.91	0.92	0.90	25	0.483	500
9, 4	0.90	0.87	0.89	25	1.185	500
9, 5	0.58	0.92	0.91	18	1.482	500
9, 6	0.92	0.92	0.86	19	1.699	500
9, 7	0.59	0.92	0.89	22	0.318	500
9, 8	0.85	0.93	0.90	14	1.484	500
9, 9	0.94	0.92	0.91	19	1.659	500
9, 10	0.91	0.92	0.92	18	1.371	500
9, 11	0.92	0.94	**0.99**	14	0.390	500
9, 12	0.93	0.93	0.94	16	1.280	500

Table 2 result shows that from 57,345 instances of the record retrieved from the dataset with 23 field(all of which has been preprocessed), 22 out of the 30 recorded data were correctly classified as test data, where 52,560 cases are genuine and over 5,411 benign cases where in the first class labelled 0. Ensemble correctly identified 5,210 cases are benign true positive instance However, 8 out of 30 cases were incorrectly classified as genuine transactions, and marked as false positive instance in the class labelled 1 (Ojugo et al., 2015, 2015; Ojugo & Eboka, 2020a; Ojugo & Otakore, 2020a; Ojugo & Yoro, 2020b). Also, 276 cases were incorrectly identified as fraud transactions and as false negative and 233 cases were correctly identified as malicious instances, these were marked as true-negative.

Table 2. Predicted values of selected data traffic transactions with hybrid

Transaction	Duration	Attack	Confusion Matrix
0.24069543	0.12 sec	Yes	TP
0.92057455	0.13 secs	Yes	TP
1.19477387	0.13 secs	Yes	TP
0.54475628	0.21 secs	Yes	TP
0.54754147	0.19 secs	Yes	TP
1.49257306	0.20 secs	Yes	TP
1.68077918	0.25 secs	Yes	TP
1.46754675	0.30 secs	No	FN
0.98409124	1.13 secs	No	FN
1.58973958	1.09 secs	No	FN
1.19001043	0.26 secs	Yes	TP
0.73513175	1.16 secs	No	FN
1.47307977	2.01 secs	Yes	TP
1.91412663	0.93 secs	Yes	TP
0.68066651	0.82 secs	Yes	TP
0.78385333	0.45 secs	Yes	TP
0.95404663	1.34 secs	No	FN
0.76097431	0.98 secs	Yes	TP
1.25818485	0.23 secs	Yes	TP
1.34559804	0.43 secs	Yes	TP
0.9708285	0.23 secs	Yes	TP
1.42120613	1.49 secs	No	FN
1.41576289	1.60 secs	No	FN
1.25585408	0.21 secs	Yes	TP
1.44015847	1.20 secs	Yes	TP
1.20401244	2.01 secs	No	FN
1.67491842	0.12 secs	Yes	TP
1.61675307	0.31 secs	Yes	TP
2.08888464	0.24 secs	Yes	TP
1.95249323	2.76 secs	No	FN

5. CONCLUSION

Fifty six (56) rules were generated for the proposed model. Fitness were found within the ranges of [0.8,0865] and are estimated to be 80% good in classification in market clustering dataset. This goes further to imply that achieving a set of good rules is far better than single optimum rule. This is turn is better for such clustering dataset. Also, the fight against network intrusion will always require a concerted effort. Also, many detected filters, schemes and heuristics often profile network transaction request by adopting their parameter of interest to analyze the created profiles as well as carry out proactive decision. The performance is often time hindered by the misclassification of unidentified data point.

The much required ensemble should correctly and effectively group all packet profile request packets into various classes with zero-tolerance for errors. Our resulting confusion matrix shows that model was found to have a sensitivity value of 0.81, specificity 0.08, and prediction accuracy of 0.991 with an improvement rate of 0.39 for data that were not originally used to train the model.

REFERENCES

Abakarim, Y., Lahby, M., & Attioui, A. (2018). An Efficient Real Time Model For Credit Card Fraud Detection Based On Deep Learning. Proceedings of the 12th International Conference on Intelligent Systems: Theories and Applications, 1–7. https://doi.org/10.1145/3289402.3289530

Adishi, E., Ejeh, P. O., Okoro, E., & Jisu, A. (2022). Reinforcement deep learning memetic algorithm for detection of short messaging services spam using filters to curb insider threats in organizations. FUPRE Journal of Scientific and Industrial Research, 6(3), 80–94.

Aghware, F. O., Yoro, R. E., Ejeh, P. O., Odiakaose, C. C., Emordi, F. U., & Ojugo, A. A. (2023a). DeLClustE: Protecting Users from Credit-Card Fraud Transaction via the Deep-Learning Cluster Ensemble. International Journal of Advanced Computer Science and Applications, 14(6), 94–100. https://doi.org/10.14569/IJACSA.2023.0140610

Aghware, F. O., Yoro, R. E., Ejeh, P. O., Odiakaose, C. C., Emordi, F. U., & Ojugo, A. A. (2023b). Sentiment analysis in detecting sophistication and degradation cues in malicious web contents. Kongzhi Yu Juece/Control and Decision, 38(01), 653.

Akazue, M. I., Asuai, C., Edje, A. E., & Omede, E. (2023). Cybershield: harnessing ensemble feature selection technique for robust distributed denial of service. Kongzhi Yu Juece/Control and Decision, 38(August), 1211–1224.

Akazue, M. I., Debekeme, I. A., Edje, A. E., Asuai, C., & Osame, U. J. (2023). UNMASKING FRAUDSTERS : Ensemble Features Selection to Enhance Random Forest Fraud Detection. Journal of Computing Theories and Applications, 1(2), 201–212. https://doi.org/10.33633/jcta.v1i2.9462

Akazue, M. I., Ojugo, A. A., Yoro, R. E., Malasowe, B. O., & Nwankwo, O. (2022). Empirical evidence of phishing menace among undergraduate smartphone users in selected universities in Nigeria. Indonesian Journal of Electrical Engineering and Computer Science, 28(3), 1756–1765. https://doi.org/10.11591/ijeecs.v28.i3.pp1756-1765

Akazue, M. I., & Omede, E. (2023). Development of a Semantic Web Framework for the Blind. International Journal of Innovative Science and Research Technology, 8(1), 1781–1789.

Akazue, M. I., Yoro, R. E., Malasowe, B. O., Nwankwo, O., & Ojugo, A. A. (2023). Improved services traceability and management of a food value chain using block-chain network : a case of Nigeria. Indonesian Journal of Electrical Engineering and Computer Science, 29(3), 1623–1633. https://doi.org/10.11591/ijeecs.v29.i3.pp1623-1633

Al-Qudah, D. A., Al-Zoubi, A. M., Castillo-Valdivieso, P. A., & Faris, H. (2020). Sentiment analysis for e-payment service providers using evolutionary extreme gradient boosting. IEEE Access, 8, 189930–189944. https://doi.org/10.1109/ACCESS.2020.3032216

Al-Turjman, F., Zahmatkesh, H., & Mostarda, L. (2019). Quantifying uncertainty in internet of medical things and big-data services using intelligence and deep learning. IEEE Access, 7, 115749–115759. https://doi.org/10.1109/ACCESS.2019.2931637

Allenotor, D., & Ojugo, A. A. (2017). A Financial Option Based Price and Risk Management Model for Pricing Electrical Energy in Nigeria. Advances in Multidisciplinary & Scientific Research Journal, 3(2), 79–90.

Allenotor, D., Oyemade, D. A., & Ojugo, A. A. (2015). A Financial Option Model for Pricing Cloud Computational Resources Based on Cloud Trace Characterization. African Journal of Computing & ICT, 8(2), 83–92. www.ajocict.net

Ampatzidis, Y., Partel, V., & Costa, L. (2020). Agroview: Cloud-based application to process, analyze and visualize UAV-collected data for precision agriculture applications utilizing artificial intelligence. Computers and Electronics in Agriculture, 174, 105457. https://doi.org/10.1016/j.compag.2020.105457

Barlaud, M., Chambolle, A., & Caillau, J.-B. (2019). Robust supervised classification and feature selection using a primal-dual method.

Behboud, G. (2020). Reasoning using Modular Neural Network. Towards Data Science, 34(2), 12–34.

Broadhurst, R., Skinner, K., Sifniotis, N., & Matamoros-Macias, B. (2018). Cybercrime Risks in a University Student Community. SSRN Electronic Journal, May. https://doi.org/10.2139/ssrn.3176319

Catrantzos, N. (2010). Tackling the insider threat. CRISP Report. https://popcenter.asu.edu/sites/default/files/library/crisp/insider-threat.pdf

Chen, D., Ertac, S., Evgeniou, T., Miao, X., Nadaf, A., & Yilmaz, E. (2022). Grit and Academic Resilience During the Covid-19 Pandemic. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4001431

Chibuzo, O. B., & Isiaka, D. O. (2020). Design and Implementation of Secure Browser for Computer-Based Tests. International Journal of Innovative Science and Research Technology, 5(8), 1347–1356. https://doi.org/10.38124/ijisrt20aug526

Cooper, P. W. (2015). Managing Insider Threat. Managing Insider Threats, Special Is, 1–14.

Durojaye, S. D., Okon, E. O., & Samson, D. D. (2015). Software Quality and Usability for Computer-Based Test in Tertiary Institution in Nigeria: A Case Study of Kogi State University. American Journal of Educational Research, 3(10), 1224–1229. https://doi.org/10.12691/education-3-10-3

Eboka, A. O., & Ojugo, A. A. (2020). Mitigating technical challenges via redesigning campus network for greater efficiency, scalability and robustness: A logical view. International Journal of Modern Education and Computer Science, 12(6), 29–45. https://doi.org/10.5815/ijmecs.2020.06.03

Ejeh, P. O., Adishi, E., Okoro, E., & Jisu, A. (2022). Hybrid integration of organizational honeypot to aid data integration, protection and organizational resources and dissuade insider threat. FUPRE Journal of Scientific and Industrial Research, 6(3), 80–94.

Ejim, S. (2017). Computer based examination system with multi-factor authentication and message notification features (Issue February) [Abubakar Tafawa Balewa University, Bauchi]. https://doi.org/10.13140/RG.2.2.14713.88167

Gao, Y., Zhang, S., Lu, J., Gao, Y., Zhang, S., & Lu, J. (2021). Machine Learning for Credit Card Fraud Detection. Proceedings of the 2021 International Conference on Control and Intelligent Robotics, 213–219. https://doi.org/10.1145/3473714.3473749

Goldstein, A., Fink, L., Meitin, A., Bohadana, S., Lutenberg, O., & Ravid, G. (2018). Applying machine learning on sensor data for irrigation recommendations: revealing the agronomist's tacit knowledge. Precision Agriculture, 19(3), 421–444. https://doi.org/10.1007/s11119-017-9527-4

Harris, S. (2020). Insider Threat Mitigation Guide. Cybersecurity & Infrastructure Security Agency, November, 1–133. https://www.cisa.gov/insider-threat-mitigation

Ibor, A. E., Edim, E. B., & Ojugo, A. A. (2023). Secure Health Information System with Blockchain Technology. Journal of the Nigerian Society of Physical Sciences, 5(992), 1–8. https://doi.org/10.46481/jnsps.2022.992

Iskandarov, S. (2020). Develop a centralized and secure online testing system for a large number of users. Journal of Information & Knowledge Management, 23(October), 1–6.

Kabir Bako, H., Abba Dandago, M., & Shamsudeen Nassarawa, S. (2019). Food Traceability System: Current State and Future Needs of the Nigerian Poultry and Poultry Product Supply Chain. Chemical and Biomolecular Engineering, 4(3), 40. https://doi.org/10.11648/j.cbe.20190403.11

Kowalski, E., Keverline, S., Ph, D., Williams, M., & Moore, A. (2008). Insider Threat Study: Illicit Cyber Activity in the Government Sector. Carnegie Melon Software Engineering Institute, 12(1).

Linh, D. (2018). Insider threat detection: Where and how data science applies. Cyber Security: A Peer-Reviewed Journal, 2, 1–8. https://www.ingentaconnect.com/content/hsp/jcs/2018/00000002/00000003/art00003

Liu, D., & Campbell, W. K. (2017). The Big Five personality traits, Big Two metatraits and social media: A meta-analysis. Journal of Research in Personality, 70, 229–240. https://doi.org/10.1016/j.jrp.2017.08.004

Mahajan, A., & Sharma, S. (2015). The Malicious Insiders Threat in the Cloud. International Journal of Engineering Research and General Science, 3(2), 246–256. www.ijergs.org

Malasowe, B. O., Akazue, M. I., Okpako, E. A., Aghware, F. O., Ojie, D. V., & Ojugo, A. A. (2023). Adaptive Learner-CBT with Secured Fault-Tolerant and Resumption Capability for Nigerian Universities. International Journal of Advanced Computer Science and Applications, 14(8), 135–142. https://doi.org/10.14569/IJACSA.2023.0140816

Matthew D. Waters. (2016). Identifying and Preventing Insider Threats. 1–9.

Muslikh, A. R., Setiadi, I. D. R. M., & Ojugo, A. A. (2023). Rice disease recognition using transfer xception convolution neural network. Jurnal Teknik Informatika (JUTIF), 4(6), 1541–1547. https://doi.org/10.52436/1.jutif.2023.4.6.1529

Nahavandi, D., Alizadehsani, R., Khosravi, A., & Acharya, U. R. (2022). Application of artificial intelligence in wearable devices: Opportunities and challenges. Computer Methods and Programs in Biomedicine, 213(December). https://doi.org/10.1016/j.cmpb.2021.106541

Obruche, C. O., Abere, R. A., & Ako, R. E. (2024). Deployment of a virtual key-card smart-lock system: the quest for improved security, eased user mobility and privacy. FUPRE Journal of Scientific and Industrial Research, 8(1), 80–94.

Odiakaose, C. C., Emordi, F. U., Ejeh, P. O., Attoh, O., & Ashioba, N. C. (2023). A pilot study to enhance semi-urban tele-penetration and services provision for undergraduates via the effective design and extension of campus telephony. FUPRE Journal of Scientific and Industrial Research, 7(3), 35–48.

Ojugo, A. A., Aghware, F. O., Yoro, R. E., Yerokun, M. O., Eboka, A. O., Anujeonye, C. N., & Efozia, F. N. (2015). Dependable Community-Cloud Framework for Smartphones. American Journal of Networks and Communications, 4(4), 95. https://doi.org/10.11648/j.ajnc.20150404.13

Ojugo, A. A., Aghware, F. O., Yoro, R. E., Yerokun, M. O., Eboka, A. O., Anujeonye, C. N., & Efozia, F. N. (2015). Evolutionary Model for Virus Propagation on Networks. Automation, Control and Intelligent Systems, 3(4), 56. https://doi.org/10.11648/j.acis.20150304.12

Ojugo, A. A., Akazue, M. I., Ejeh, P. O., Odiakaose, C., & Emordi, F. U. (2023). DeGATraMoNN: Deep Learning Memetic Ensemble to Detect Spam Threats via a Content-Based Processing. Kongzhi Yu Juece/Control and Decision, 38(01), 667–678.

Ojugo, A. A., Ben-Iwhiwhu, E., Kekeje, O. D., Yerokun, M. O., & Iyawa, I. J. (2014). Malware Propagation on Social Time Varying Networks: A Comparative Study of Machine Learning Frameworks. International Journal of Modern Education and Computer Science, 6(8), 25–33. https://doi.org/10.5815/ijmecs.2014.08.04

Ojugo, A. A., & Eboka, A. O. (2014). A Social Engineering Detection Model for the Mobile Smartphone Clients. African Journal of Computing & ICT, 7(3). www.ajocict.net

Ojugo, A. A., & Eboka, A. O. (2018a). Assessing Users Satisfaction and Experience on Academic Websites: A Case of Selected Nigerian Universities Websites. International Journal of Information Technology and Computer Science, 10(10), 53–61. https://doi.org/10.5815/ijitcs.2018.10.07

Ojugo, A. A., & Eboka, A. O. (2018b). Comparative Evaluation for High Intelligent Performance Adaptive Model for Spam Phishing Detection. Digital Technologies, 3(1), 9–15. https://doi.org/10.12691/dt-3-1-2

Ojugo, A. A., & Eboka, A. O. (2018c). Modeling the Computational Solution of Market Basket Associative Rule Mining Approaches Using Deep Neural Network. Digital Technologies, 3(1), 1–8. https://doi.org/10.12691/dt-3-1-1

Ojugo, A. A., & Eboka, A. O. (2020a). An Empirical Evaluation On Comparative Machine Learning Techniques For Detection of The Distributed Denial of Service (DDoS) Attacks. Journal of Applied Science, Engineering, Technology, and Education, 2(1), 18–27. https://doi.org/10.35877/454ri.asci2192

Ojugo, A. A., & Eboka, A. O. (2020b). Memetic algorithm for short messaging service spam filter using text normalization and semantic approach. International Journal of Informatics and Communication Technology (IJ-ICT), 9(1), 9. https://doi.org/10.11591/ijict.v9i1.pp9-18

Ojugo, A. A., & Eboka, A. O. (2021). Empirical Bayesian network to improve service delivery and performance dependability on a campus network. IAES International Journal of Artificial Intelligence (IJ-AI), 10(3), 623. https://doi.org/10.11591/ijai.v10.i3.pp623-635

Ojugo, A. A., Eboka, A. O., Yoro, R. E., Yerokun, M. O., & Efozia, F. N. (2015a). Framework design for statistical fraud detection. Mathematics and Computers in Science and Engineering Series, 50, 176–182.

Ojugo, A. A., Eboka, A. O., Yoro, R. E., Yerokun, M. O., & Efozia, F. N. (2015b). Hybrid model for early diabetes diagnosis. Mathematics and Computers in Industry, 50(3–5), 55–65. https://doi.org/10.1109/MCSI.2015.35

Ojugo, A. A., & Ekurume, E. O. (2021a). Deep Learning Network Anomaly-Based Intrusion Detection Ensemble For Predictive Intelligence To Curb Malicious Connections: An Empirical Evidence. International Journal of Advanced Trends in Computer Science and Engineering, 10(3), 2090–2102. https://doi.org/10.30534/ijatcse/2021/851032021

Ojugo, A. A., & Ekurume, E. O. (2021b). Predictive Intelligent Decision Support Model in Forecasting of the Diabetes Pandemic Using a Reinforcement Deep Learning Approach. International Journal of Education and Management Engineering, 11(2), 40–48. https://doi.org/10.5815/ijeme.2021.02.05

Ojugo, A. A., & Nwankwo, O. (2021). Spectral-Cluster Solution For Credit-Card Fraud Detection Using A Genetic Algorithm Trained Modular Deep Learning Neural Network. JINAV: Journal of Information and Visualization, 2(1), 15–24. https://doi.org/10.35877/454RI.jinav274

Ojugo, A. A., Obruche, C. O., & Eboka, A. O. (2021). Quest For Convergence Solution Using Hybrid Genetic Algorithm Trained Neural Network Model For Metamorphic Malware Detection. ARRUS Journal of Engineering and Technology, 2(1), 12–23. https://doi.org/10.35877/jetech613

Ojugo, A. A., & Otakore, D. O. (2018a). Redesigning Academic Website for Better Visibility and Footprint: A Case of the Federal University of Petroleum Resources Effurun Website. Network and Communication Technologies, 3(1), 33. https://doi.org/10.5539/nct.v3n1p33

Ojugo, A. A., & Otakore, O. D. (2018b). Improved Early Detection of Gestational Diabetes via Intelligent Classification Models: A Case of the Niger Delta Region in Nigeria. Journal of Computer Sciences and Applications, 6(2), 82–90. https://doi.org/10.12691/jcsa-6-2-5

Ojugo, A. A., & Otakore, O. D. (2020a). Computational solution of networks versus cluster grouping for social network contact recommender system. International Journal of Informatics and Communication Technology (IJ-ICT), 9(3), 185. https://doi.org/10.11591/ijict.v9i3.pp185-194

Ojugo, A. A., & Otakore, O. D. (2020b). Intelligent cluster connectionist recommender system using implicit graph friendship algorithm for social networks. IAES International Journal of Artificial Intelligence, 9(3), 497~506. https://doi.org/10.11591/ijai.v9.i3.pp497-506

Ojugo, A. A., & Otakore, O. D. (2021). Forging An Optimized Bayesian Network Model With Selected Parameters For Detection of The Coronavirus In Delta State of Nigeria. Journal of Applied Science, Engineering, Technology, and Education, 3(1), 37–45. https://doi.org/10.35877/454RI.asci2163

Ojugo, A. A., & Oyemade, D. A. (2021). Boyer moore string-match framework for a hybrid short message service spam filtering technique. IAES International Journal of Artificial Intelligence, 10(3), 519–527. https://doi.org/10.11591/ijai.v10.i3.pp519-527

Ojugo, A. A., Oyemade, D. A., Allenotor, D., Longe, O. B., & Anujeonye, C. N. (2015). Comparative Stochastic Study for Credit-Card Fraud Detection Models. African Journal of Computing & ICT, 8(1), 15–24. www.ajocict.net

Ojugo, A. A., Ugboh, E., Onochie, C. C., Eboka, A. O., Yerokun, M. O., & Iyawa, I. J. B. (2013). Effects of Formative Test and Attitudinal Types on Students' Achievement in Mathematics in Nigeria. African Educational Research Journal, 1(2), 113–117. http://search.ebscohost.com/login.aspx?direct=true&db=eric&AN=EJ1216962&site=ehost-live

Ojugo, A. A., & Yoro, R. E. (2013). Computational Intelligence in Stochastic Solution for Toroidal N-Queen. Progress in Intelligent Computing and Applications, 1(2), 46–56. https://doi.org/10.4156/pica.vol2.issue1.4

Ojugo, A. A., & Yoro, R. E. (2020a). Forging A Smart Dependable Data Integrity And Protection System Through Hybrid-Integration Honeypot In Web and Database Server. Technology Report of Kansai University, 62(08), 5933–5947.

Ojugo, A. A., & Yoro, R. E. (2020b). Predicting Futures Price And Contract Portfolios Using The ARIMA Model: A Case of Nigeria's Bonny Light and Forcados. Quantitative Economics and Management Studies, 1(4), 237–248. https://doi.org/10.35877/454ri.qems139

Ojugo, A. A., & Yoro, R. E. (2021a). Extending the three-tier constructivist learning model for alternative delivery: ahead the COVID-19 pandemic in Nigeria. Indonesian Journal of Electrical Engineering and Computer Science, 21(3), 1673. https://doi.org/10.11591/ijeecs.v21.i3.pp1673-1682

Ojugo, A. A., & Yoro, R. E. (2021b). Forging a deep learning neural network intrusion detection framework to curb the distributed denial of service attack. International Journal of Electrical and Computer Engineering, 11(2), 1498–1509. https://doi.org/10.11591/ijece.v11i2.pp1498-1509

Okobah, I. P., & Ojugo, A. A. (2018). Evolutionary Memetic Models for Malware Intrusion Detection: A Comparative Quest for Computational Solution and Convergence. International Journal of Computer Applications, 179(39), 34–43. https://doi.org/10.5120/ijca2018916586

Okonta, E. O., Ojugo, A. A., Wemembu, U. R., & Ajani, D. (2013). Embedding Quality Function Deployment In Software Development: A Novel Approach. West African Journal of Industrial & Academic Research, 6(1), 50–64.

Okonta, E. O., Wemembu, U. R., Ojugo, A. A., & Ajani, D. (2014). Deploying Java Platform to Design A Framework of Protective Shield for Anti– Reversing Engineering. West African Journal of Industrial & Academic Research, 10(1), 50–64.

Okperigho, S. ., Nwozor, B., & Geteloma, V. . (2024). Deployment of an IoT Storage Tank Gauge and Monitor. FUPRE Journal of Scientific and Industrial Research, 8(1), 55–68.

Oladele, J. K., Ojugo, A. A., Odiakaose, C. C., Emordi, F. U., Abere, R. A., Nwozor, B., Ejeh, P. O., & Geteloma, V. O. (2024). BEHeDaS: A Blockchain Electronic Health Data System for Secure Medical Records Exchange. Journal of Computing Theories and Applications, 2(1), 1–12. https://doi.org/10.33633/jcta.v2i19509

Omede, E., & Okpeki, U. K. (2023). Design and implementation of autotech resource sharing system for secondary schools in Delta State. Journal of Nigerian Association of Mathematical Physics, 51(5), 325–337.

Ometov, A., Shubina, V., Klus, L., Skibińska, J., Saafi, S., Pascacio, P., Flueratoru, L., Gaibor, D. Q., Chukhno, N., Chukhno, O., Ali, A., Channa, A., Svertoka, E., Qaim, W. Bin, Casanova-Marqués, R., Holcer, S., Torres-Sospedra, J., Casteleyn, S., Ruggeri, G., … Lohan, E. S. (2021). A Survey on Wearable Technology: History, State-of-the-Art and Current Challenges. Computer Networks, 193, 108074. https://doi.org/10.1016/j.comnet.2021.108074

Oyemade, D. A., & Ojugo, A. A. (2020). A Property Oriented Pandemic Surviving Trading Model. International Journal of Advanced Trends in Computer Science and Engineering, 9(5), 7397–7404. https://doi.org/10.30534/ijatcse/2020/71952020

Oyemade, D. A., & Ojugo, A. A. (2021). An Optimized Input Genetic Algorithm Model for the Financial Market. International Journal of Innovative Science, Engineering and Technology, 8(2), 408–419. https://ijiset.com/vol8/v8s2/IJISET_V8_I02_41.pdf

Oyemade, D. A., Ureigho, R. J., Imouokhome, F. ., Omoregbee, E. U., Akpojaro, J., & Ojugo, A. A. (2016). A Three Tier Learning Model for Universities in Nigeria. Journal of Technologies in Society, 12(2), 9–20. https://doi.org/10.18848/2381-9251/CGP/v12i02/9-20

Pantazi, X. E., Moshou, D., Alexandridis, T., Whetton, R. L., & Mouazen, A. M. (2016). Wheat yield prediction using machine learning and advanced sensing techniques. Computers and Electronics in Agriculture, 121, 57–65. https://doi.org/10.1016/j.compag.2015.11.018

Said, H., Tawfik, B. B. S., & Makhlouf, M. A. (2023). A Deep Learning Approach for Sentiment Classification of COVID-19 Vaccination Tweets. International Journal of Advanced Computer Science and Applications, 14(4), 530–538. https://doi.org/10.14569/IJACSA.2023.0140458

Tomar, N., & Manjhvar, A. K. (2015). A Survey on Data Mining Optimization Techniques. IJSTE-International Journal of Science Technology & Engineering |, 2(06), 130–133. www.ijste.org

Urbanowicz, R. J., Meeker, M., La Cava, W., Olson, R. S., & Moore, J. H. (2018). Relief-based feature selection: Introduction and review. Journal of Biomedical Informatics, 85, 189–203. https://doi.org/10.1016/j.jbi.2018.07.014

Wemembu, U. R., Okonta, E. O., Ojugo, A. A., & Okonta, I. L. (2014). A Framework for Effective Software Monitoring in Project Management. West African Journal of Industrial and Academic Research, 10(1), 102–115. http://www.ajol.info/index.php/wajiar/article/view/105798

Yoro, R. E., Aghware, F. O., Akazue, M. I., Ibor, A. E., & Ojugo, A. A. (2023). Evidence of personality traits on phishing attack menace among selected university undergraduates in Nigerian. International Journal of Electrical and Computer Engineering, 13(2), 1943. https://doi.org/10.11591/ijece.v13i2.pp1943-1953

Yoro, R. E., Aghware, F. O., Malasowe, B. O., Nwankwo, O., & Ojugo, A. A. (2023). Assessing contributor features to phishing susceptibility amongst students of petroleum resources varsity in Nigeria. International Journal of Electrical and Computer Engineering (IJECE), 13(2), 1922. https://doi.org/10.11591/ijece.v13i2.pp1922-1931

Yoro, R. E., & Ojugo, A. A. (2019a). An Intelligent Model Using Relationship in Weather Conditions to Predict Livestock-Fish Farming Yield and Production in Nigeria. American Journal of Modeling and Optimization, 7(2), 35–41. https://doi.org/10.12691/ajmo-7-2-1

Yoro, R. E., & Ojugo, A. A. (2019b). Quest for Prevalence Rate of Hepatitis-B Virus Infection in the Nigeria: Comparative Study of Supervised Versus Unsupervised Models. American Journal of Modeling and Optimization, 7(2), 42–48. https://doi.org/10.12691/ajmo-7-2-2

Yuan, S., & Wu, X. (2021). Deep learning for insider threat detection: Review, challenges and opportunities. Computers and Security, 104. https://doi.org/10.1016/j.cose.2021.102221

Zareapoor, M., & Shamsolmoali, P. (2015). Application of Credit Card Fraud Detection: Based on Bagging Ensemble Classifier. Procedia Computer Science, 48, 679–685. https://doi.org/10.1016/j.procs.2015.04.201

` ` ` ` ` ` ` ` ` ` ` ` ` ` ` ` ` ` ` ` w