Journal of Computing Theories and Applications ISSN:3024-9104

Research Article

Forging a User-Trust Hybrid Memetic Modular Neural Network Card Fraud Detection Ensemble: A Pilot Study

Arnold Adimabua Ojugo[1]*, Maureen Ifeanyi Akazue[2], Patrick Ogholuwarami Ejeh[3], Nwanze Chukwudi Ashioba[3], Christopher Chukwufunaya Odiakaose[3], Rita Erhovwo Ako[1] and Frances Uche Emordi[4]

[1] Department of Computer Science, Federal University of Petroleum Resources Effurun, Delta State, Nigeria; ojugo.arnold@fupre.edu.ng; ritaochuko2@gmail.com
[2] Department of Computer Science, Delta State University Abraka, Nigeria; akazue@delsu.edu.ng
[3] Department of Computer Science, Dennis Osadebay University Anwai-Asaba, Delta State, Nigeria; patrick.ejeh@dou.edu.ng; nwanze.ashioba@dou.edu.ng; osegalaxy@gmail.com
[4] Department of Cybersecurity, Dennis Osadebay University Asaba, Nigeria; frances.emordi@dou.edu.ng
* Corresponding Author: Arnold Adimabua Ojugo

Abstract: The advent of the Internet as an effective means for resource sharing has consequently, led to proliferation of adversaries, with unauthorized access to network resources. Adversaries achieved fraudulent activities via carefully crafted attacks of large magnitude targeted at personal gains and rewards. With the cost of over $1.3Trillion lost globally to financial crimes and the rise in such fraudulent activities vis the use of credit-cards, financial institutions and major stakeholders must begin to explore and exploit better and improved means to secure client data and funds. Banks and financial services must harness the creative mode rendered by machine learning schemes to help effectively manage such fraud attacks and threats. We propose a hybrid modular genetic algorithm trained neural network ensemble to detect fraud activities. The hybrid, equipped with knowledge to altruistically detect fraud on credit card transactions. Results show ensemble effectively differentiates, the benign class attacks/threats from genuine credit card transaction(s) with model accuracy of 92%.

Keywords: HyDeLMoNNE; Credit-card; Fraud detection; Reinforcement ensemble; Deep learning.

Received: September, 24th 2023
Revised: October, 11th 2023
Accepted: October, 12th 2023
Published: October, 13th 2023

1. Introduction

The birth and adoption today, of credit cards along with the added functionality of financial inclusiveness it proffers – has both, given more comfort to clients as well as attracted malicious adversaries interested in personal gains [1]. Credit-cards crimes have since become easy targets – as such crimes when therein committed and perpetrated – can and are only discovered a weeks afterwards [2], [3]. Successful credit-card fraud techniques can includes (but are not limited to): (a) card copying to acquire/steal user privacy data (on need), and (b) vendors extorting money without a card-holder's awareness [4]–[6]. Whenever banks lose money to such card-fraud, their corresponding card-holders entirely/partially reimburse such losses through reduced benefits and higher interests. Thus, it is in the best interest of both card-holders and financial institutions, to reduce card fraud as well as invest wisely in schemes to aid card-fraud prevention and detection [7], [8].

Financial crimes cost the global financial services industry $42Billion by 2018 – with the numbers growing rapidly [9]. Anticipating today's fraud systems, financial services firms must diversify via applying innovative measures to mitigate and prevent fraud. If a technical system is abused, methods are needed to detect it. Fraud prevention and detection schemes aim to identify fraud instances via anomaly detection in user behavior and logged data analysis [10], [11]. Management of fraud thus, advances preventive measures to curb fraud acts [12], [13]. Oracle offers fraud management that combines anomaly-correlation abilities with sophisticated behavior detection, analysis and case administration [14] – to result in early detection of complex fraud with enhanced client protection, and reduced reputational risk [15], [16].

Fraudsters continually seek more efficient mode with improve dynamism to evade security measures and firewalls that profiles user behavior at entry point, and minor hacks to steal client valuable data. Fraud monitors proffers combo of risk monitoring and detection analysis [17]. Ojugo and Otakore [18] notes that a detection system should intelligently gather event alerts with early multi-channel fraud detection that aims to enhance client protection, and reduce risks of fraud susceptibility [19]–[21].

The dynamism in card fraud detection continues to puzzle administrators as adversaries are continually poised with rising quest to tweak schemes to help them evade detection; while, businesses are more determined to curb such threats. These, have contributed to making such task for both business owners and policymakers, an inconclusive and continuous feature [4]. To formulate improved and better performed frameworks, studies have successfully shown that ensembles with degraded performance can be attributed to a variety of reasons such as improper feature/parameter selection, conflicts imposed by the dataset used during data encoding, selected training/testing probability distribution for underlying features of interest, etc [22]–[24]. Even with the consequent adoption and adaptations of dynamically evolved, intelligent and stochastic classifiers, card fraud persists as adversaries are continually evolving their exploit techniques [25], [26].

Our study explores a hybrid ensemble [27], [28] capable of addressing optimization issues with appropriate feature(s) selection to adequately train the ensemble such that it avoids the pitfalls of model over-fitting and over-parameterization as well as effectively resolves the conflicts in data encoding and heuristic(s) structure with the hybrid. We propose the hybrid genetic algorithm trained modular neural network ensemble to aid card-fraud detection.

2. Review of Related Literature(s)

2.1. Fraud Detection

The advent of the Internet alongside the evolution on Moore's law of computing continues to advance processing prowess/capabilities [29], [30]. These are met with cyber-attacks, which is today the single largest threat globally to individuals and businesses [31]. These attacks are targeted at resources, generated by these coy, to include intellectual property, data, devices etc – aimed ultimately at financial gains [32], [33]. A remarkable evidence of our society's digital revolution towards financial inclusion is the proliferated use of cards. This revolution has also birthed many challenges with card-fraud and is currently witnessing the era of more clever and complicated methods/techniques being adopted and adapted to dispose clients of their privacy data and money [34], [35].

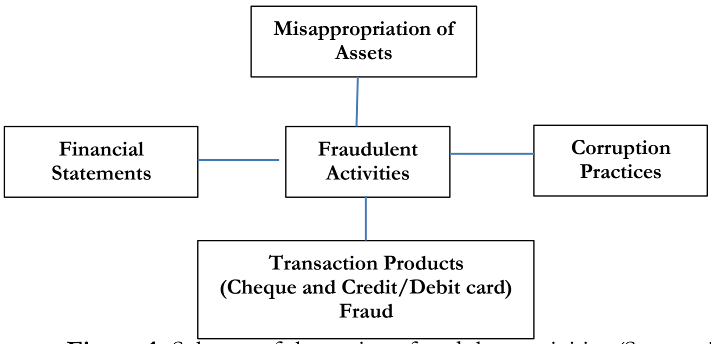

Figure 1. Schema of the various fraudulent activities (Source: [36])

Fraud seeks to illegally dispose an unsuspecting, compromised user of valuable assets herein obtained by an adversary via willful misrepresentation. From a criminal viewpoint, fraudulent charges may theft, larceny, and embezzlement [37]. It is a state where an unsuspecting, vulnerable user relies and depends on the false representative claims issued by an attacker/adversary for personal benefits [38]. Fraud is perpetuated by either an insider within an organization (as insider threat), or by an external user to compromise the workings and proper function of a system within an organization/business [39], [40]. Thus, [5] identifies fraud can be to the benefit of an individual; to part of an organization; or to the whole organization itself. Credit-card today, has improved a bank's proximity to her clients, and also ushered in more financial inclusion for customers. It has also advanced the needs for adversaries and attracted malicious attacks for gains [20]. A critical reason in the choice of credit-cards by adversaries, is that asides being an easy target – such crimes if/when committed, are often uncovered days after; while, some cases even go unreported. Successfully implemented card-fraud methods include(s): (a) cloning of card having acquired the compromised user privacy and confidential information, and (b) finance houses overcharging the cardholders even without their awareness [39]. When banks lose money to card fraud, the cardholders are made to repay such loss wholly/partly, via either reduced benefits and/or higher interest rates. Thus, it is in the best standpoint of both the banks and the various cardholders – to take the necessary precautions and action in a bid to reduce card fraud [41].

Ileberi et al. [39] trained the RBF model with 7-parameters to recognize an attack from a data packet, sent via a filter alarm. Their design created profiles using stream sample mode. And their result – shows we can: (a) accurately cluster and quantify packets as a profile, and (b) we can listen to low-error rates anomalies and correctly identify. They concluded that routers listen and trace packet exchange, they harness key parameters and underlying features of interest for each packet; And thus, allows the model to create the corresponding profiles that in turn, improved their detection rate/confidence. Artikis et al. [4] used a change aggregate tree to detect minor shocks cum anomaly in traffic data. These, they investigated and uncovered that many of such events correlate during various sessions. As such, a router actively terminates session to indicate that an attack is imminent. Aghware et al. [3] used a deep learning ensemble with 7-feats to monitor, inspect and detect packet rates; while, Ojugo et al. [42] extended [35] via an unsupervised ensemble to capture and profile packet parameters explored to group (into classes), packet patterns in a traffic session.

2.2 Learning Models

An algorithm seeks to explore a sequence of instruction to process a set of data inputs so as to yield a transformed output usually referred to as an outcome [43]. During processing, what we know as both input and output can change. We seek a system to track how the input is processed and transformed unto an output, and the changes therein achieved [44]. Thus, what we lack in knowledge is made up for in data and instruction to yield a program. The idea is to learn what constitutes an output. A model achieves this via the learning process. Learning is a system's ability to map/assign the input data points onto an output class using the underlying feats of interest, and approximate a solution for the system as the data-point changes via the actions of processing [26], [45].

Learning is classified [46]: (a) supervised learning maps an input data to an output class, whose correct values are provided by a supervisor via the use of labels, and (b) unsupervised learning maps input unto an output class without the use of labels. Its structure aims to find regularities at the input and map them unto classes, and (c) reinforcement or semi-supervised – a hybrid of the supervised and unsupervised modes [47]–[50].

2.3. Study Motivation

A remarkable evidence of the digital revolution and transformation age in our society in the recent past, is the proliferation of credit-card(s) use and adoption in a variety of exchange platforms. This revolution also ushered in the problem of credit card fraud, wherever more clever and complicated methods are used to steal considerable amounts of money [34]:

1. The constant loss in revenue by financial institutions alongside a variety of the hidden therein accrued to clients with such financial losses.
2. The rise in adoption of online purchases and e-commerce vis-à-vis the rise in adoption of credit-card to foster more financial inclusiveness has made more users complacent as they port on various platforms to aid the seamless transaction buying and selling. Wherein it should be noted that these criminals and adversaries are always, often steps ahead of many security experts.
3. Adversaries continue to leverage on user-trust patterns and susceptibility behaviours cum traits (i.e. phishing threats) to commit such crimes – since by nature, users yearn to improve their dependence and trust-level of techs that improve their living ease. The

need thus, to protect client valuable assets via the implementation of fraud prevention and detection schemes has become both critical and paramount.

4. The adoption of such techniques are often hampered due to the limited nature of fraud dataset and since, it is also very much unwise to describe in great details – the workings and structure of such fraud detection techniques and ensemble over public as these will further arm adversaries with the needed requisite knowledge to evade detection.
5. The inherent issues in performance degradation has often been triggered and attributed to features such as the improper selection of underlying parameters of interest, choice in mismatched features, data encoding anomalies, structural dependencies conflict, the use of non-optimized dataset vis-à-vis its lack thereof. Eliminating ambiguities, noise and partial truth features will further improve the classification properties of an ensemble.
6. The presentation of censored results and limited availability of datasets – has often hampered the performance of detection. Also, with the available dataset rippled with noise, partial truth, ambiguities, and imprecision, which the schemes must resolved in order to arrive at an optimal solution.
7. Card fraud can persist even with the adaptation of dynamic schemes and classifiers. New schemes must be ably address optimization tasks exploring machine learning approaches to yield ensemble unification via exploiting historic (numerical) dataset.

3. Proposed Material and Method

3.1. Data Gathering

Dataset is a transaction log file that consists of 23-fields for each record. Log file contains about 57,345-transaction records with details to include cardholder data, bank name and others as in Table 1. Transactions log consists of records to help effectively classify into genuine and fraudulent transactions. Dataset is rippled with cases of genuine and fraudulent transaction classes. The sampled (unstructured) dataset was collected for a 15-months period, with the classified records amounts to 58.2% of total data-records. The dataset is split into: training (75%) and testing (25%) respectively.

Table 1. Historic Dataset with features such as Data Description, Types and Format

Features	Description of Features	Data Type	Format
User Name	Account Holder's Name	Object	abcd
Bank Name	Bank of Account Holder	Object	abcd
NUBAN Account	Nigerian Universal Bank Number e-channel Trans.	Int	1234
Billing Address	Account holder's local bank address of withdrawal, hotel	Object	abcd
Transaction Amount	Amount of transactions adjusted in the bank's currency	Float	12.34
Transaction Type	Local, International, and/or e-Commerce as type	Object	abcd
Date/Time	Transaction Date and Time	Float	M:D:Y
Transaction Channel	Channel (payment terminal and/or merchant application)	Object	abcd
Merchant	Hotels, Restaurants, etc	Object	Abcd
Transaction Gap Time	Duration from last transaction to the current transaction	Float	M:D:Y
Daily Transaction	Daily average transactions performed by a cardholder	Int	1234
Daily Transaction Limit	The daily limit of the amount that cardholders can do daily	Float	12.34
Freq. Trans. Types	Average frequency of transactions by cardholder	Int.	1234

3.2. Hybrid Memetic Modular Neural Network Ensemble (HyGAMoNNE)

It is known fact that hybrid (reinforcement) ensembles are always proven to better than single models. There is however, the issue of resolving conflicts that arise from encoding data as data flows and is transcribed from one heuristics to another. There is also the issue of structural dependencies imposed on the ensemble. These must be adequately and effectively resolved. We use a hybrid modular ensemble as in Figure 2, which shows the ensemble as a 3-block model-view adapted from [51] as: (a) unsupervised modular Kohonen neural network, (b) the supervised cultural genetic algorithm, and (c) a knowledgebase.

1. The Cultural Genetic Algorithm: Basically, 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. A variant of GA is the Cultural GA (CGA), which uses 4-belief spaces to define its solution space namely: (a) normative

belief which defines the specific value ranges to which a gene is bound, (b) domain belief contains knowledge about the task being undertaken, (c) temporal belief contains knowledge about the available problem space, and (d) spatial belief contains knowledge about the task's topography. Furthermore, it uses the influence function to bridge the belief spaces and its gene pool to ensure any modified genes still conform to the belief space(s). The CGA yields a pool that does not violate its belief space and assist in reducing the number of genes generated until an optimum is discovered [52], [53].

2. The Unsupervised Kohonen Modular Network is a grid-like, feed-forward neural network whose first layer accepts input, and re-sends unbound to its second layer, which uses the transfer function to offer competitive computation. The competitive layer maps similar patterns into relations, which is used to determine training results. We modify these parameters to carefully create our Kohonen MNN via a deep-learning architecture [54].

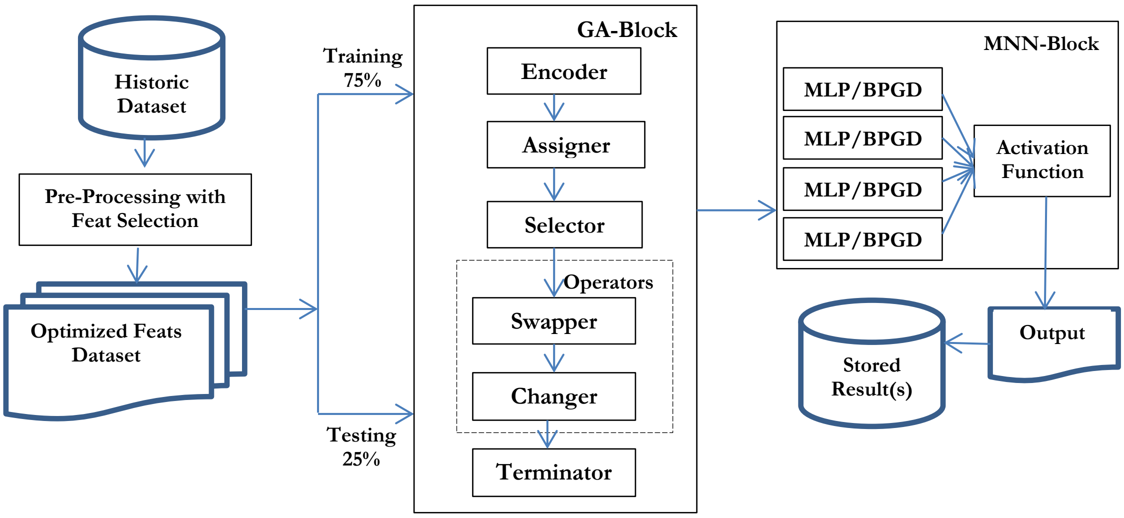

Figure 2. Hybrid Genetic Algorithm Trained Modular Neural Network Ensemble

3.3. Data Encoding

Unstructured and unclassified data must be formatted to be used by the appropriate heuristics. This will help clean up the dataset and reduce its ambiguities, noise, partial truth, non-available and incomplete data, amongst other imprecise and inconsistent feats. With the fusion of both heuristics (i.e. the genetic algorithm and Modular neural network) – it yields a conflict for encoding data. Our ensemble must appropriately filter the dataset records, and map onto the required form that the hybrid can effectively and easily understand. To resolve this conflict and adequately encode the selected feats of interest, we transform our dataset of Table 1 using the Pandas Library as in listing 1. This will help the ensemble to modulate the raw data unto the require dataset – and even if data is retrieved from a variety of sources, will be adequate for analysis.

Listing 1. Data Description and Encoding for HyGAMoNNE Algorithm

```
INPUT: Select Parameters of interest
OUTPUT: Format parameters to appropriate data_type
For Each selected parameter DO
    if selected parameter is non-numerical then data_type category is generated
   End if
End For
```

3.4. Training Phase & Tuning of Hyper-Parameters

In training, the selected parameters are tuned (i.e. hyper-parameters) with values outside an ensemble's bounds [55]–[57], which impacts its behavior via targeted learning to yield an optimal solution. Our choice ensemble will help to learn feats directly so as to help resolve the data encoding and structural conflicts imposed on the ensemble by the native heuristics used, and avoid over-fit, over-parameterization and poor generalization of ensemble [58], [59]. For hyper-parameters in our proposed ensemble is as [60] thus:

1. Learning rate regulates the neuron's bias and weights, and ensures amount to be modified via gradient loss. It denotes how easy an ensemble may abandon its belief for new norms. A small learning rate value denotes faster learning and implies how easily the ensemble can quickly identify important feats. It enables an ensemble to easily and more quickly adapt to change. To minimize ensemble over-fit and over-training, we choose a learning rate of 0.2, which is suitably adjusted for the ensemble.
2. Batch size is the training size used. It is of 3-modes: (a) batch is when iteration and epoch sizes are equal, (b) mini – when the iteration is greater than epoch size, and (c) stochastic is when the gradient and network features are updated and recalibrated after iteration.

Using trial-n-error in tuning the hyper-parameters, we used the best fit values of 0.2 and 500-epochs for learning_rate and batch_size respectively during training (and re-implemented during test phase). This is found to be in agreement with [61]–[63].

4. Results and Discussion

4.1. Ensemble Testing Phase Performance and Evaluation

To compute the sensitivity, specificity, and accuracy of the ensemble [64], [65] we evaluate its performance using Eq. 1 to Eq. 3 respectively as thus:

$$Sensitivity = \frac{TP}{TP + FN} \tag{1}$$

$$Specificity = \frac{TN}{TN + FP} \tag{2}$$

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{3}$$

The resultant confusion matrix classification report is given in the Table 2 and 3 respectively. Table 2 shows that the ensemble has a prediction accuracy of 0.99 (i.e., 99%) with data inclusion that were not originally used to train the ensemble, from the outset.

Table 2. Classification report for Test-Dataset

Parameters	Sensitivity	Specificity	Accuracy	Support
0	0.98	1.00	0.99	11,411
1	1.00	0.98	0.99	1,059
Avg/Total	0.99	0.99	0.99	12,500

Table 3 shows that from the test dataset, 11,411-cases of the 12,500 records were correctly classified as fraudulent in the class (label 0). It implies the ensemble correctly identified and classified appropriately as true-positives the transactions of the class 0. Also, 31-cases of incorrectly classified fraudulent transaction were marked false-positive; While, we have 1,059 benign transactions in the class (label 1); for which, 776-incorrectly classified fraud transactions was marked false-negative, and 283-correctly classified fraud was marked true-negative. Note: (a) true-positive, ensemble predicted positive, and it was true, (b) true-negative, ensemble predicted negative and it was true, (c) false-positive, ensemble predicted positive and it was false, and lastly, (d) false-negative, ensemble predicted negative and it was false. This, is as seen in Table 3 and agrees with [28].

Table 3. Classification report for Test Data (predicted versus actual values)

Parameters	Actual	Values
Predicted	11,411	31
Values	776	283

4.2. Result Findings

Simulation test-beds with a single-layered net of 1-to-10 neurons yields highest f-score and least training loss time to result in the best number of layers. Adding a second hidden layer yielded good results with the highest number of neurons yielding the best scores and agrees with [66], [67]. Table 4 shows the first layer configuration with 10 neurons and extra 2 neurons for optimal extra processing. The hidden layer of 9,11-neurons resulted in a 99% accuracy and 0.39 training loss value. The ensemble favors the adoption and consequent use of a second hidden layer with a greater value for the accuracy as in agreement with [61], [68].

Table 4. Accuracy result with 2-hidden layers

Hidden Layer	Sensitivity	Specificity	Accuracy	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 5. Predicted results values of selected transaction rule log

Transaction Rule(s)	Duration	Attack	Confusion Matrix
0.24069543	0.12secs	Yes	TP
0.92057455	0.13secs	Yes	TP
1.19477387	0.13secs	Yes	TP
0.54475628	0.21secs	Yes	TP
0.54754170	0.19secs	Yes	TP
1.49257306	0.20secs	Yes	TP
1.68077918	0.25secs	Yes	TP
1.46754675	0.30secs	Yes	TP
0.98409124	1.13secs	No	FN
1.58973958	1.09secs	No	FN
1.19001043	0.26secs	Yes	TP
0.73513175	1.16secs	No	FN
1.47307977	2.01secs	Yes	TP
1.94126630	0.93secs	Yes	TP
0.68066651	0.82secs	Yes	TP
0.78385333	0.45secs	Yes	TP
0.95404663	1.34secs	No	FN
0.76097431	0.98secs	Yes	TP
1.25818485	0.23secs	Yes	TP
1.34559804	0.43secs	Yes	TP
0.97082850	0.23secs	Yes	TP
1.42120613	1.49secs	No	FN
1.41576289	1.60secs	No	FN
1.25585408	0.21secs	Yes	TP
1.44015847	1.20secs	Yes	TP
1.20401244	2.01secs	No	FN
1.67491842	0.12secs	Yes	TP
1.61675307	0.31secs	Yes	TP
2.08888464	0.24secs	Yes	TP
1.95249323	2.76secs	No	FN

Table 5 yields the false-positive and true-negative error classification rates. Result shows that from the 57,345-instances of the records retrieved from the dataset with 23-fields (all of which has been pre-processed), 22-out-of-the-30 recorded data were correctly classified (i.e. result of the test dataset) where 52,560 cases are genuine, and over 5,411 benign cases were in the first class labeled 0. Ensemble successfully identified 5,210-cases as correctly classified as benign true-positive instance; But, 8-out-of-30 cases were incorrectly classified as genuine transactions, and marked as false-positive instance in the class labeled 1. Also, 276-cases were incorrectly identified as fraud transactions as false-negative, and 233-cases correctly identified malicious instances of them were marked as true-negative; And this agrees with [69], [70]. Thus, (a) for true positive, model predicted positive, which is true, (b) for true negative, model predicted negative and it was true, (c) for false positive**,** model predicted positive and it was false, and (d) for false negative, the model predicted negative and it was false. Thus, it can be concluded on the premise of the results achieved that the proposed HyGAMoNNE.

4.2. Discussion of Findings

The fight against card-fraud will always require a concerted effort. Many detection filters, schemes and heuristics often profiles transaction requests using adopted parametric feats of interest to analyze the created profiles as well as pro-actively decide, if a profile packet data is (un)compromised vis-à-vis yield safety actions as further measures. Their performance is often hindered by the misclassification of unidentified data-points. The needed ensemble should correctly and effectively group all profiled request data packets (into the various classes of genuine and fraudulent transactions) with zero-tolerance for errors. Again, we can thus, conclude on the premise of the results achieved therein – that, our proposed HyGAMoNNE ensemble can effectively classify transactions into the various classes.

4.3. Tradeoff for Ensemble Implementation

Several trade-off were noticed in our aim to benchmark these simulations results, and these fall under the following classes and agrees with [71]–[73]:

1. **Censored Result(s)**: Modelers often build newer ensembles rather than investigate older ones by re-evaluating their limitations/bias. They also fail to report negative results on the premise that they are less valuable. Thus, they showcase 'incorrect' results with misleading images on their level of agreement with known successful solutions [74], [75].
2. **Test-beds** – Modelers employ graphs that are further discussed to allude to or convey how well their simulations agree with the squeezed and available limited (historic) data that often yield results that are not easily distinguishable. Some studies do not even provide numeric dataset; however, their model agrees with the observations. A measure of goodness does not provide the relevant knowledge for the task at hand [76], [77].
3. **Insufficient Tests** – Validation compares computed versus observed values. Many studies use inadequate data. If a model seeks to simulate results of a task, such capability cannot be demonstrated with unfounded/misleading result from limited data and misleading conclusions [78], [79].

5. Conclusions

Fraud schemes/techniques usually filters a credit card transaction request, analyzes it to decide uncompromised and compromised packets, and met out safety measures for further actions. This performance can be hindered by the error rate for incorrectly classified and unidentified rules that the scheme/model generates. An ideal scheme will correctly classify all request and packets with almost zero error rates of false positive/negative – through tradeoffs between the number of false positives and false negatives.

To implement hybrid ensemble, a modeler must carefully select the appropriate feats to be used for, choose an efficient encoding scheme for the dataset (so as not to lose data via pre-processing), effectively explore the observed data in the domain in interest and to yield an optimal solution. The dataset used must be encoded within model's structured learning – to resolve all statistical dependencies as well as highlight implications for such a multi-agent model so as to avoid over-fit, over-training etc. Modelers must acknowledge that these agents create or enforce their own behavioral rules on the adopted heuristics, and dataset; Thus, impacting differently on hybrid ensemble other than intended.

Model must provide enough new data with feedback logic that aid valuable comprehension of the adopted rules. Thus, modelers must provide the needed balance required to easily understand and manage between model's complexity and its navigation – to help study other processes. Thus, we posit that: (a) parameters are a major source of uncertainty in predictions. Model should have input ranges rather than single values, (b) multi-criteria training with adequate datasets helps reduce parameter uncertainty, and (c) prediction is of limited practical use, without clear data about reliability and accuracy.

Author Contributions: Conceptualization: A.A. Ojugo and M.I. Akazue; methodology, A.A. Ojugo., P.O. Ejeh and N.C. Ashioba; software: R.E. Ako., and M.I. Akazue; validation: A.A. Ojugo and F.U. Emordi; formal analysis: M.I. Akazue; investigation: A.A. Ojugo; resources: P.O. Ejeh; data curation: C.C. Odiakaose; writing—original draft preparation: F.U. Emordi; writing—review and editing: N.C. Ashioba; visualization: A.A. Ojugo; supervision: A.A. Ojugo; project administration: A.A. Ojugo; funding acquisition: All.

Conflicts of Interest: The authors declare no conflict of interest

References

[1] R. Broadhurst, K. Skinner, N. Sifniotis, and B. Matamoros-Macias, "Cybercrime Risks in a University Student Community," *SSRN Electron. J.*, no. May, 2018, doi: 10.2139/ssrn.3176319.
[2] R. E. Yoro, F. O. Aghware, B. O. Malasowe, O. Nwankwo, and A. A. Ojugo, "Assessing contributor features to phishing susceptibility amongst students of petroleum resources varsity in Nigeria," *Int. J. Electr. Comput. Eng.*, vol. 13, no. 2, p. 1922, Apr. 2023, doi: 10.11591/ijece.v13i2.pp1922-1931.
[3] F. O. Aghware, R. E. Yoro, P. O. Ejeh, C. C. Odiakaose, F. U. Emordi, and A. A. Ojugo, "DeLClustE: Protecting Users from Credit-Card Fraud Transaction via the Deep-Learning Cluster Ensemble," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 6, pp. 94–100, 2023, doi: 10.14569/IJACSA.2023.0140610.
[4] A. Artikis *et al.*, "A Prototype for Credit Card Fraud Management," in *Proceedings of the 11th ACM International Conference on Distributed and Event-based Systems*, Jun. 2017, pp. 249–260. doi: 10.1145/3093742.3093912.
[5] I. Benchaji, S. Douzi, B. El Ouahidi, and J. Jaafari, "Enhanced credit card fraud detection based on attention mechanism and LSTM deep model," *J. Big Data*, vol. 8, no. 1, p. 151, Dec. 2021, doi: 10.1186/s40537-021-00541-8.
[6] R. E. Yoro, F. O. Aghware, M. I. Akazue, A. E. Ibor, and A. A. Ojugo, "Evidence of personality traits on phishing attack menace among selected university undergraduates in Nigerian," *Int. J. Electr. Comput. Eng.*, vol. 13, no. 2, p. 1943, Apr. 2023, doi: 10.11591/ijece.v13i2.pp1943-1953.
[7] L. De Kimpe, M. Walrave, W. Hardyns, L. Pauwels, and K. Ponnet, "You've got mail! Explaining individual differences in becoming a phishing target," *Telemat. Informatics*, vol. 35, no. 5, pp. 1277–1287, Aug. 2018, doi: 10.1016/j.tele.2018.02.009.
[8] M. I. Akazue, R. E. Yoro, B. O. Malasowe, O. Nwankwo, and A. A. Ojugo, "Improved services traceability and management of a food value chain using block-chain network : a case of Nigeria," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 29, no. 3, pp. 1623–1633, 2023, doi: 10.11591/ijeecs.v29.i3.pp1623-1633.
[9] R. Brause, F. Hamker, and J. Paetz, "Septic Shock Diagnosis by Neural Networks and Rule Based Systems," 2002, pp. 323–356. doi: 10.1007/978-3-7908-1788-1_12.
[10] S. M. Albladi and G. R. S. Weir, "User characteristics that influence judgment of social engineering attacks in social networks," *Human-centric Comput. Inf. Sci.*, vol. 8, no. 1, p. 5, Dec. 2018, doi: 10.1186/s13673-018-0128-7.
[11] A. Algarni, Y. Xu, and T. Chan, "An empirical study on the susceptibility to social engineering in social networking sites: the case of Facebook," *Eur. J. Inf. Syst.*, vol. 26, no. 6, pp. 661–687, Nov. 2017, doi: 10.1057/s41303-017-0057-y.
[12] M. Al-Qatf, Y. Lasheng, M. Al-Habib, and K. Al-Sabahi, "Deep Learning Approach Combining Sparse Autoencoder With SVM for Network Intrusion Detection," *IEEE Access*, vol. 6, pp. 52843–52856, 2018, doi: 10.1109/ACCESS.2018.2869577.
[13] E. R. Altman, "Synthesizing Credit Card Transactions," Oct. 2019, [Online]. Available: http://arxiv.org/abs/1910.03033
[14] I. Correia, F. Fournier, and I. Skarbovsky, "The uncertain case of credit card fraud detection," in *Proceedings of the 9th ACM International Conference on Distributed Event-Based Systems*, Jun. 2015, pp. 181–192. doi: 10.1145/2675743.2771877.
[15] J. R. Amalraj and R. Lourdusamy, "A Novel distributed token-based algorithm using secret sharing scheme for secure data access control," *Int. J. Comput. Networks Appl.*, vol. 9, no. 4, p. 374, Aug. 2022, doi: 10.22247/ijcna/2022/214501.
[16] I. A. Anderson and W. Wood, "Habits and the electronic herd: The psychology behind social media's successes and failures," *Consum. Psychol. Rev.*, vol. 4, no. 1, pp. 83–99, Jan. 2021, doi: 10.1002/arcp.1063.
[17] M. Barlaud, A. Chambolle, and J.-B. Caillau, "Robust supervised classification and feature selection using a primal-dual method," Feb. 2019.
[18] A. A. Ojugo and O. D. Otakore, "Mitigating Social Engineering menace in Nigerian Universities," *J. Comput. Sci. Appl.*, vol. 6, no. 2, pp. 64–68, 2018, doi: 10.12691/jcsa-6-2-2.
[19] A. A. Ojugo, A. Osika, I. J. Iyawa, and M. O. Yerokun, "Information and communication technology integration into science, technology, engineering and mathematic (STEM) in Nigeria," *West African J. Ind. Acad. Res.*, vol. 4, no. 1, pp. 22–30, 2012, [Online]. Available: https://www.ajol.info/index.php/wajiar/article/view/86904/76697

[20] M. Fatahi, M. Ahmadi, A. Ahmadi, M. Shahsavari, and P. Devienne, "Towards an spiking deep belief network for face recognition application," in *2016 6th International Conference on Computer and Knowledge Engineering (ICCKE)*, Oct. 2016, pp. 153–158. doi: 10.1109/ICCKE.2016.7802132.

[21] M. Gratian, S. Bandi, M. Cukier, J. Dykstra, and A. Ginther, "Correlating human traits and cyber security behavior intentions," *Comput. Secur.*, vol. 73, pp. 345–358, Mar. 2018, doi: 10.1016/j.cose.2017.11.015.

[22] C. Li, N. Ding, H. Dong, and Y. Zhai, "Application of Credit Card Fraud Detection Based on CS-SVM," *Int. J. Mach. Learn. Comput.*, vol. 11, no. 1, pp. 34–39, 2021, doi: 10.18178/ijmlc.2021.11.1.1011.

[23] S. Goel, K. Williams, and E. Dincelli, "Got Phished? Internet Security and Human Vulnerability," *J. Assoc. Inf. Syst.*, vol. 18, no. 1, pp. 22–44, Jan. 2017, doi: 10.17705/1jais.00447.

[24] T. Halevi, J. Lewis, and N. Memon, "A pilot study of cyber security and privacy related behavior and personality traits," in *Proceedings of the 22nd International Conference on World Wide Web*, May 2013, pp. 737–744. doi: 10.1145/2487788.2488034.

[25] A. A. Ojugo, D. A. Oyemade, D. Allenotor, O. B. Longe, and C. N. Anujeonye, "Comparative Stochastic Study for Credit-Card Fraud Detection Models," *African J. Comput. ICT*, vol. 8, no. 1, pp. 15–24, 2015, [Online]. Available: www.ajocict.net

[26] M. I. Akazue, A. A. Ojugo, R. E. Yoro, B. O. Malasowe, and O. Nwankwo, "Empirical evidence of phishing menace among undergraduate smartphone users in selected universities in Nigeria," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 28, no. 3, pp. 1756–1765, Dec. 2022, doi: 10.11591/ijeecs.v28.i3.pp1756-1765.

[27] A. A. Ojugo and O. D. Otakore, "Intelligent cluster connectionist recommender system using implicit graph friendship algorithm for social networks," *IAES Int. J. Artif. Intell.*, vol. 9, no. 3, p. 497~506, 2020, doi: 10.11591/ijai.v9.i3.pp497-506.

[28] Y. Gao, S. Zhang, J. Lu, Y. Gao, S. Zhang, and J. Lu, "Machine Learning for Credit Card Fraud Detection," in *Proceedings of the 2021 International Conference on Control and Intelligent Robotics*, Jun. 2021, pp. 213–219. doi: 10.1145/3473714.3473749.

[29] C. L. Udeze, I. E. Eteng, and A. E. Ibor, "Application of Machine Learning and Resampling Techniques to Credit Card Fraud Detection," *J. Niger. Soc. Phys. Sci.*, p. 769, Aug. 2022, doi: 10.46481/jnsps.2022.769.

[30] A. E. Ibor, E. B. Edim, and A. A. Ojugo, "Secure Health Information System with Blockchain Technology," *J. Niger. Soc. Phys. Sci.*, vol. 5, no. 992, pp. 1–8, 2023, doi: 10.46481/jnsps.2022.992.

[31] A. A. Ojugo, A. O. Eboka, E. O. Okonta, R. E. Yoro, and F. O. Aghware, "Predicting Behavioural Evolution on a Graph-Based Model," *Adv. Networks*, vol. 3, no. 2, p. 8, 2015, doi: 10.11648/j.net.20150302.11.

[32] S. K. Stevens, "Tracing the Food Safety Laws and Regulations Governing Traceability: A Brief History of Food Safety and Traceability Regulation," in *Food Traceability*, Cham: Springer International Publishing, 2019, pp. 13–26. doi: 10.1007/978-3-030-10902-8_2.

[33] Y. Abakarim, M. Lahby, and A. Attioui, "An Efficient Real Time Model For Credit Card Fraud Detection Based On Deep Learning," in *Proceedings of the 12th International Conference on Intelligent Systems: Theories and Applications*, Oct. 2018, pp. 1–7. doi: 10.1145/3289402.3289530.

[34] A. Abbasi, F. M. Zahedi, and Y. Chen, "Phishing susceptibility: The good, the bad, and the ugly," in *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, Sep. 2016, pp. 169–174. doi: 10.1109/ISI.2016.7745462.

[35] A. A. Ojugo and E. O. Ekurume, "Deep Learning Network Anomaly-Based Intrusion Detection Ensemble For Predictive Intelligence To Curb Malicious Connections: An Empirical Evidence," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 10, no. 3, pp. 2090–2102, Jun. 2021, doi: 10.30534/ijatcse/2021/851032021.

[36] D. Mao, F. Wang, Z. Hao, and H. Li, "Credit Evaluation System Based on Blockchain for Multiple Stakeholders in the Food Supply Chain," *Int. J. Environ. Res. Public Health*, vol. 15, no. 8, p. 1627, Aug. 2018, doi: 10.3390/ijerph15081627.

[37] H. Tingfei, C. Guangquan, and H. Kuihua, "Using Variational Auto Encoding in Credit Card Fraud Detection," *IEEE Access*, vol. 8, pp. 149841–149853, 2020, doi: 10.1109/ACCESS.2020.3015600.

[38] D. Huang, Y. Lin, Z. Weng, and J. Xiong, "Decision Analysis and Prediction Based on Credit Card Fraud Data," in *The 2nd European Symposium on Computer and Communications*, Apr. 2021, pp. 20–26. doi: 10.1145/3478301.3478305.

[39] E. Ileberi, Y. Sun, and Z. Wang, "A machine learning based credit card fraud detection using the GA algorithm for feature selection," *J. Big Data*, vol. 9, no. 1, p. 24, Dec. 2022, doi: 10.1186/s40537-022-00573-8.

[40] T. Edirisooriya and E. Jayatunga, "Comparative Study of Face Detection Methods for Robust Face Recognition Systems," *5th SLAAI - Int. Conf. Artif. Intell. 17th Annu. Sess. SLAAI-ICAI 2021*, no. December, 2021, doi: 10.1109/SLAAI-ICAI54477.2021.9664689.

[41] M. Laavanya and V. Vijayaraghavan, "Real Time Fake Currency Note Detection using Deep Learning," *Int. J. Eng. Adv. Technol.*, vol. 9, no. 1S5, pp. 95–98, 2019, doi: 10.35940/ijeat.a1007.1291s52019.

[42] A. A. Ojugo, A. O. Eboka, R. E. Yoro, M. O. Yerokun, and F. N. Efozia, "Framework design for statistical fraud detection," *Math. Comput. Sci. Eng. Ser.*, vol. 50, pp. 176–182, 2015.

[43] A. A. Ojugo and R. E. Yoro, "Predicting Futures Price And Contract Portfolios Using The ARIMA Model: A Case of Nigeria's Bonny Light and Forcados," *Quant. Econ. Manag. Stud.*, vol. 1, no. 4, pp. 237–248, 2020, doi: 10.35877/454ri.qems139.

[44] A. A. Ojugo, R. E. Yoro, E. O. Okonta, and A. O. Eboka, "A Hybrid Artificial Neural Network Gravitational Search Algorithm for Rainfall Runoffs Modeling and Simulation in Hydrology," *Prog. Intell. Comput. Appl.*, vol. 2, no. 1, pp. 22–34, 2013, doi: 10.4156/pica.vol2.issue1.2.

[45] V. Filippov, L. Mukhanov, and B. Shchukin, "Credit card fraud detection system," in *2008 7th IEEE International Conference on Cybernetic Intelligent Systems*, Sep. 2008, pp. 1–6. doi: 10.1109/UKRICIS.2008.4798919.

[46] A. A. Ojugo, M. I. Akazue, P. O. Ejeh, C. Odiakaose, and F. U. Emordi, "DeGATraMoNN : Deep Learning Memetic Ensemble to Detect Spam Threats via a Content-Based Processing," *Kongzhi yu Juece/Control Decis.*, vol. 38, no. 01, pp. 667–678, 2023.

[47] G. M. Friesen, T. C. Jannett, M. A. Jadallah, S. L. Yates, S. R. Quint, and H. T. Nagle, "A comparison of the noise sensitivity of nine QRS detection algorithms," *IEEE Trans. Biomed. Eng.*, vol. 37, no. 1, pp. 85–98, 1990, doi: 10.1109/10.43620.

[48] A. A. Ojugo and A. O. Eboka, "Empirical Bayesian network to improve service delivery and performance dependability on a campus network," *IAES Int. J. Artif. Intell.*, vol. 10, no. 3, p. 623, Sep. 2021, doi: 10.11591/ijai.v10.i3.pp623-635.

[49] S. Nosratabadi, F. Imre, K. Szell, S. Ardabili, B. Beszedes, and A. Mosavi, "Hybrid Machine Learning Models for Crop Yield Prediction," Mar. 2020, [Online]. Available: http://arxiv.org/abs/2005.04155
[50] A. A. Ojugo and O. D. Otakore, "Computational solution of networks versus cluster grouping for social network contact recommender system," *Int. J. Informatics Commun. Technol.*, vol. 9, no. 3, p. 185, 2020, doi: 10.11591/ijict.v9i3.pp185-194.
[51] G. Behboud, "Reasoning using Modular Neural Network," *Towar. Data Sci.*, vol. 34, no. 2, pp. 12–34, 2020.
[52] X. Lin, P. R. Spence, and K. A. Lachlan, "Social media and credibility indicators: The effect of influence cues," *Comput. Human Behav.*, vol. 63, pp. 264–271, Oct. 2016, doi: 10.1016/j.chb.2016.05.002.
[53] F. O. Aghware, R. E. Yoro, P. O. Ejeh, C. C. Odiakaose, F. U. Emordi, and A. A. Ojugo, "Sentiment analysis in detecting sophistication and degradation cues in malicious web contents," *Kongzhi yu Juece/Control Decis.*, vol. 38, no. 01, p. 653, 2023.
[54] R. J. Urbanowicz, M. Meeker, W. La Cava, R. S. Olson, and J. H. Moore, "Relief-based feature selection: Introduction and review," *J. Biomed. Inform.*, vol. 85, pp. 189–203, Sep. 2018, doi: 10.1016/j.jbi.2018.07.014.
[55] M. Zanin, M. Romance, S. Moral, and R. Criado, "Credit Card Fraud Detection through Parenclitic Network Analysis," *Complexity*, vol. 2018, pp. 1–9, 2018, doi: 10.1155/2018/5764370.
[56] K. Kuwata and R. Shibasaki, "Estimating crop yields with deep learning and remotely sensed data," in *2015 IEEE International Geoscience and Remote Sensing Symposium (IGARSS)*, Jul. 2015, pp. 858–861. doi: 10.1109/IGARSS.2015.7325900.
[57] Z. Karimi, M. Mansour Riahi Kashani, and A. Harounabadi, "Feature Ranking in Intrusion Detection Dataset using Combination of Filtering Methods," *Int. J. Comput. Appl.*, vol. 78, no. 4, pp. 21–27, Sep. 2013, doi: 10.5120/13478-1164.
[58] S. Khaki and L. Wang, "Crop Yield Prediction Using Deep Neural Networks," *Front. Plant Sci.*, vol. 10, May 2019, doi: 10.3389/fpls.2019.00621.
[59] S. Khaki, L. Wang, and S. V. Archontoulis, "A CNN-RNN Framework for Crop Yield Prediction," *Front. Plant Sci.*, vol. 10, Jan. 2020, doi: 10.3389/fpls.2019.01750.
[60] S. Xuan, G. Liu, Z. Li, L. Zheng, S. Wang, and C. Jiang, "Random forest for credit card fraud detection," in *2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC)*, Mar. 2018, pp. 1–6. doi: 10.1109/ICNSC.2018.8361343.
[61] M. Zareapoor and P. Shamsolmoali, "Application of Credit Card Fraud Detection: Based on Bagging Ensemble Classifier," *Procedia Comput. Sci.*, vol. 48, pp. 679–685, 2015, doi: 10.1016/j.procs.2015.04.201.
[62] N. Valaei, S. R. Nikhashemi, H. Ha Jin, and M. M. Dent, "Task Technology Fit in Online Transaction Through Apps," in *Optimizing e-participation initiatives via social media*, IGI Global, 2018, pp. 236–251. doi: 10.4018/978-1-5225-5326-7.ch010.
[63] I. Sohony, R. Pratap, and U. Nambiar, "Ensemble learning for credit card fraud detection," in *Proceedings of the ACM India Joint International Conference on Data Science and Management of Data*, Jan. 2018, pp. 289–294. doi: 10.1145/3152494.3156815.
[64] A. Vishwanath, "Habitual Facebook Use and its Impact on Getting Deceived on Social Media," *J. Comput. Commun.*, vol. 20, no. 1, pp. 83–98, Jan. 2015, doi: 10.1111/jcc4.12100.
[65] E. O. Yeboah-Boateng and P. M. Amanor, "Phishing , SMiShing & Vishing : An Assessment of Threats against Mobile Devices," *J. Emerg. Trends Comput. Inf. Sci.*, vol. 5, no. 4, pp. 297–307, 2014.
[66] S. S. Verma *et al.*, "Collective feature selection to identify crucial epistatic variants," *BioData Min.*, vol. 11, no. 1, p. 5, Dec. 2018, doi: 10.1186/s13040-018-0168-6.
[67] D. Zhang, B. Bhandari, and D. Black, "Credit Card Fraud Detection Using Weighted Support Vector Machine," *Appl. Math.*, vol. 11, no. 12, pp. 1275–1291, 2020, doi: 10.4236/am.2020.1112087.
[68] S. Yuan and X. Wu, "Deep learning for insider threat detection: Review, challenges and opportunities," *Comput. Secur.*, vol. 104, 2021, doi: 10.1016/j.cose.2021.102221.
[69] G. G. Akin, A. F. Aysan, G. I. Kara, and L. Yildiran, "The failure of price competition in the Turkish credit card market," *Emerg. Mark. Financ. Trade*, vol. 46, no. SUPPL. 1, pp. 23–35, 2010, doi: 10.2753/REE1540-496X4603S102.
[70] H. Yildiz Durak, "Human Factors and Cybersecurity in Online Game Addiction: An Analysis of the Relationship Between High School Students' Online Game Addiction and the State of Providing Personal Cybersecurity and Representing Cyber Human Values in Online Games," *Soc. Sci. Q.*, vol. 100, no. 6, pp. 1984–1998, Oct. 2019, doi: 10.1111/ssqu.12693.
[71] A. Jayatilaka, N. A. G. Arachchilage, and M. A. Babar, "Falling for Phishing: An Empirical Investigation into People's Email Response Behaviors," *arXiv Prepr. arXiv* …, no. Fbi 2020, pp. 1–17, 2021.
[72] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong, "Teaching Johnny not to fall for phish," *ACM Trans. Internet Technol.*, vol. 10, no. 2, pp. 1–31, May 2010, doi: 10.1145/1754393.1754396.
[73] S. V. S. . Lakshimi and S. D. Kavila, "Machine Learning for Credit Card Fraud Detection System," *Int. J. Appl. Eng. Res.*, vol. 15, no. 24, pp. 16819–16824, 2018, doi: 10.1007/978-981-33-6893-4_20.
[74] D. Nahavandi, R. Alizadehsani, A. Khosravi, and U. R. Acharya, "Application of artificial intelligence in wearable devices: Opportunities and challenges," *Comput. Methods Programs Biomed.*, vol. 213, p. 106541, Jan. 2022, doi: 10.1016/j.cmpb.2021.106541.
[75] G. Sasikala *et al.*, "An Innovative Sensing Machine Learning Technique to Detect Credit Card Frauds in Wireless Communications," *Wirel. Commun. Mob. Comput.*, vol. 2022, pp. 1–12, Jun. 2022, doi: 10.1155/2022/2439205.
[76] O. V. Lee *et al.*, "A malicious URLs detection system using optimization and machine learning classifiers," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 17, no. 3, p. 1210, Mar. 2020, doi: 10.11591/ijeecs.v17.i3.pp1210-1214.
[77] D. Wang, B. Chen, and J. Chen, "Credit card fraud detection strategies with consumer incentives," *Omega*, vol. 88, pp. 179–195, Oct. 2019, doi: 10.1016/j.omega.2018.07.001.
[78] T. Ma, F. Wang, J. Cheng, Y. Yu, and X. Chen, "A Hybrid Spectral Clustering and Deep Neural Network Ensemble Algorithm for Intrusion Detection in Sensor Networks," *Sensors*, vol. 16, no. 10, p. 1701, Oct. 2016, doi: 10.3390/s16101701.
[79] T. Sahmoud and D. M. Mikki, "Spam Detection Using BERT," Jun. 2022, doi: 10.48550/arXiv.2206.02443.