International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 3, May-June 2024||

DOI:10.15662/IJRPETM.2024.0703016

AI-Based Early Warning System for Financial Scams Targeting Consumers

Lalitha Reddy Badam

Independent Researcher, University of New Haven, USA

lalithabadambvsr@gmail.com

ABSTRACT: Financial scams are aimed at consumers and are getting more advanced and use behavioral weaknesses, social engineering and rapid change frameworks. Innovative fraud-detection by rule based systems are likely to have problems in detecting the new scamp system, especially when genuine sounding transfers are being designed on an impersonation, investment as well as the elder fraud scam. This paper will present an Early Warning System (EWS) that will be essentially an AI-based system that aims to anticipate unusual financial conduct among the consumers with substantial losses. The built tool will be a hybrid of a transaction monitoring system, behavioral profiling, anomaly detection, machine learning, and generation of risk alerts to assess the abnormalities in the typical consumer transaction patterns. The system will detect the abnormal transfers associated with impersonation, investment and elder fraud by examining the frequency of the transactions, amount of transfer, characteristics of the recipient, time of transfers, geographical mismatches as well as the changes in behaviors. Explainable AI methods are also added to give transparent justifications of the generated alerts to justify an early corrective action by financial institutions and consumers. A dynamically-risk-scoring system and action-responsive are prioritized to potential fraud basing on the size of scam. The suggested approach will probably decrease the false-positives, yet enhance the level of early detection, response-time, and consumer protection. The framework provides a proactive System of smart financial fraud and can be integrated into the new banking and online payment systems.

KEYWORDS: Artificial Intelligence, Financial Scam Detection, Early Warning System, Anomaly Detection, Impersonation Scams, Investment Scams, Elder Scams.

I. INTRODUCTION

The breakneck development of the digital banking, mobile payment, and online investing services, real time funds transfer services alleviated the way people handle money. Not only are these technologies convenient and accessible but have also provided financial scammers with new ways in which they can take advantage of consumers. Currently, financial scams are more socially engineered as opposed to the previous technique of entering the premises illegally. Other tricks used by criminals are posing as trusted people, financial establishments, government officials, call center or investment consultant to persuade the victims to voluntarily consent to the current proceedings. As such, what appears to be a valid transaction according to the traditional scale of fraud detection, may be a scam that has been initiated because of trickery.

Financial frauds oriented towards consumers in particular are problematic since fraudism may not present the classic features of payment fraud. In very large percentage of cases the victims authenticate themselves, transfer monies via their own computers and send them to accounts which are not already malicious accounts. Examples of fraudulent schemes, in which use of psychological manipulation is a significant factor include impersonation scam, investment scam and scam targeted at older consumers. A victim can make a case of a single transaction to deliver a decent sum of money to a new target beneficiary or make a number of payments in a finite time or transfer money to an unknown account which the victim will not know he or she has been given false advice. These behavioral variations give valuable indications that may be detected prior to incurring huge financial damages.

Older methods of fraud detection mainly rely on pre-programmed rules, threshold, blacklists and manually-coded transaction indicators. The techniques can still be used in finding patterns which are already laid down yet they are less effective in tracking the scam-altering strategies. There would be a lot of false positives as a result of the regular rules which include a group of regular customers who could have some unusual, but true transactions. On the other hand, highly personalized scams can go unnoticed since even the transaction can be technically valid. The increasing diversity and complexity of consumer payment behavior hence requires smarter systems with some sort of knowledge

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 3, May-June 2024||

DOI:10.15662/IJRPETM.2024.0703016

on how to learn the general tendencies in behavior and power of the system to make note of the aberration in near real time.

Machine learning and Artificial Intelligence (AI) provide good prospects to deal with these weaknesses. The intelligent systems can cope with huge amounts of transactional and behavioral information and can discover relationships that can be hard to establish individually by using manually-constructed rules. A dynamic consumer risk profile can be constituted using among others, the value of the transaction, the frequency of the payment, the time, history of the recipient, geographic information, device, relationship with the account as well as not following the previous spending habits. Such activities which vary considerably with respect to the behaviour of an individual, could then be distinguished in the form of anomaly-detection designs and transactions denoted in terms of supervised learning approaches on the foundation of the already observed scam and truthful behaviour. An integration of these approaches may be employed to support a more proactive and dynamic approach to identify financial scams.

Nevertheless, the detection of suspicious transaction is inadequate to be capable of safeguarding consumers. An early warning mechanism should be able to note a threat at a relatively young age to make any type of intervention effective. This creates the need to have risk-related signals released constantly by reviewing the transactions and issuing risk-associated signals in case of suspicious changes in behavior. The significant difference between the proposed strategy and the existing approaches is that in contrast to the current approach that recognizes the transaction as being a part of its overall practices as opposed to all odd transactions being proven frauds. Transfers of high value that are recent, and recipient has recently been added onto the list, odd time of transaction, suspicious account activity, massive difference in the history of the consumer is another example of an incident that will score higher on the risk scorecard. The contextual analysis may be useful to add priority to the notifications and minimize additional interruption to the trusted customers.

Explainability is another aspect of AI-guided financial security one would like to have. The financial institutions and consumers should know why a transaction has been detected to be suspicious especially where an alert has led to the following validation or some sort of interim intervention. Black box-based predictions which are not able to provide explanations that can be understood by people may decrease the trust and it may be difficult to operate on them. Therefore, effective AI-based early warning framework should be capable of providing explanations in a way that is understandable and informed by the right variables (behavioral and transactional). It can either be a fraud alert that fraud analysts are looking into or it can be so as to inform the consumer about potentially fraudulent situations, such explanations can become a source of investigating these situations.

This project recommends an AI-Based Early Warning System of Financial Scompulsive attacks on consumers which combines behavioral modelling, anomaly detection, risk evaluation using machine learning and explainable AI. The model is uniquely created to view unusual transfers as an impersonation, investment, elder scam and individual transaction behavior and contextual risk factors. Dynamic risk-scoring algorithm helps to prioritize suspicious processes based on their possible severity and assists in generating warning about them during the timeframe. This design is also aimed at reducing false positives and promptly identify new patterns of scams, as well as augment the elucidatability of AI-generated protocols.

The primary objective of this research is therefore to change consumer financial protection to proactive, smart and behavioural pre-emptive paradigm as opposed to the reactionary model of detecting fraud. By determining abnormal behaviors in advance or through the execution of suspicious financial transactions, the proposed structure would serve to give extra security to financial institutions against the overseen scamming schemes. Finally, the paper will also aim to illustrate that a financial ecosystem of AI can be adjusted to make it resilient in cases of early detection, how effective response is, and how more transparency can be achieved among others and how the financial and social risks involved with more sophisticated consumer-cutting-edge scams can be offset.

II. RELATED WORK

It has converted its previous criminal monetary transactions to elegant consumer oriented programs of social engineering, personification, fake investment plans and exploitative victims. Thus, a combination of behavior analysis, machine learning, authentication, and proactive prevention systems have become the focus of study recently. There is much to be found in the existing literature on which to construct an AI-driven early-sensing system of financial frauds against consumers, but there is also a blind spot between transaction-driven fraud detection and customer-centric scam-prevention model.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 3, May-June 2024||

DOI:10.15662/IJRPETM.2024.0703016

In 600 cases of online banking fraud Jansen and Leukfeldt [1] demonstrated that the perpetrator frequently aimed at exploiting the victims by using social and behavioral ways regardless of the fact that technical vulnerabilities of the victims did not exist. It is their discovery that highlights the significance of learning in the way to persuade consumers to sanction or aid in the perpetration of fraudulent transactions. It is especially the case with impersonation attacks wherein the victim may begin to send and transfer money on a valid sounding bank order unintentionally upon meeting the attacksers. Nevertheless, it is more of a research based on empirical evidence and lacks the automation of an AI process to detect some suspicious financial dealings before it is lost.

Barker [2] has highlighted the components of proactive communication and the knowledge management as a tool of ensuring further awareness of the customers on e-banking fraud. According to the paper, the training of consumers is a case that could assist in fraud prevention. This would collaborate with automated detection as the consumers would be notified in case an unusual activity can be detected. This awareness policy however is more prone to be reliant on awareness of the users and reaction to the warning message though a clever early-warning system can also be designed with a behavioral and transaction cue to cause personalized notices.

Another major issue that exposes consumers to risk of financial fraud is phishing. Abidoye and Kabaso [3] proposed a hybrid machine-learning based solution of detecting phishing attack in communication networks. Their work suggests the way machine learning can be applicable to detecting any suspicious activity in communication. The issue being investigated is not financial transactions, but the technique applied in the investigation it may be borrowed in the identification of the communication and impersonation phase, which is regarded to be a precursor in the majority of the cases of fraudulent financial transactions. An indicator-behavioral combination of a phishing indicator and a behavioral indicator is as of now the best way to achieve maximum capacity in consumer scam detection.

Maulana et al. [4] suggested an intelligent mobile code to identify fraud instances of stealing e-banking access with the help of big-data analytics and service-oriented architecture. Their article shows the possibilities of implementing analytical functionalities into the mobile banking setting. This can be more so when it comes to an early-warning structure as it is through the mobile applications that there will be an efficient avenue in sending instant notifications. However, it continues to focus more on the e-banking access fraud rather than focus on the different types of consumer scams such as impersonation, investment and senior scams.

A channel specific fraud detection has also been tackled. Khalaf Al Hattali et al. [5] came up with a system that detects and prevents ATM skimming fraud. They exhibit in their work the application of automated security measures to detect a malicious activity within a particular banking channel. In their study, Tsai and Su [6] involved both I and S servers in their research with specific concentration on stronger authentication schemes since they are the key to lock the online banking system. Authentication can help minimize cases of unauthorized access, but is not inadequate to prevent authorized access by duped consumers. This is a big disadvantage as regards scamming since the authentic account owner has the capability of transacting.

Portfolio into blockchain has been cited as a means of circumventing monetary frauds. As Hammi et al. [7] proposed, a blockchain-based solution, which helps identify and block fake check scams, could come in handy. In the plan, they demonstrate ways in which the problem of financial frauds can be minimized with the use of transaction records that cannot be altered, and decentralized technologies. Nonetheless, blockchain-based solutions might fail to considerably handle social-engineering-based scams, where victims are cheated into transferring the money to the culprits, voluntarily.

Abdul Rani et al. [8] focus on the role of financial crime intermediaries by providing a review of literature on the subject of money mules and its role, in terms of the recruitment and awareness of money mules. The results can be applied to the downstream transfer to scam proceeds. Early warning system can thus be alerted with the role of detecting an unusual transfer with regards to mule accounts. But it is primarily a systematic review but not predictive model in use.

The research on machine learning has applied a wide variety in detecting transactions level fraud. Ileberi et al. [9] had also used the genetic algorithms to select the features as a credit-card fraud model which relied on machine-learning. Their paper illustrates that it is essential to choose informative transaction characteristics to enhance the performance of detection. A black-box challenge of the fraud detection was followed up by Chaquet-Ulldemolins et al. [10], who investigated informative feature selection as well as linear models. This is particularly important in the context of

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 3, May-June 2024||

DOI:10.15662/IJRPETM.2024.0703016

warning systems that are consumer-friendly which may involve asking the consumer to tell a user as to why a transaction has been red flagged.

They have also demonstrated a tremendous potential in state-of-the-art learning models. Nguyen et al. [11] considered using a CatBoost model and a deep learning model to identify fraud, but Esenogho et al. [12] utilized a stronger model that is based on neural networks and a combination of neural networks, including feature engineering. All these are the results of the ensemble and deep-learning structures to detect high-order fraud in the pattern of transaction. However, their emphasis (primarily) is on credit-card fraud and not on the socially modified consumer fraud.

The other critical issue is that of data disparity. Gupta et al. [13] comparatively examined the balancing approaches of credit-card fraud datasets of high unbalance. This is significant in the sense that in the real-world, there exist many legitimate transactions and many of the transactions exist in excess of the false ones. Sharma et al. [14] carried out a similar study carried out an examination of machine-learning models to identify the credit-card fraud detectors and demonstrated that there can be no single classifier rather multiple algorithms need to be compared.

In general, the available studies show that phishing and bank security has made enormous strides along with transaction fraud shielding, machine learning, authentication and shopper consciousness [1] -[14]. Nevertheless, a majority of research is focused on illicit transactions, credit-card fraud, a particular set of technical attack, or post-detection fraud. There have been very few attempts hitherto to concentrate on networked consumer oriented early warning platform that can effectively spot anomalous transfers with respect to impersonation, investment and elder scam. To fill this gap, the proposed research includes transaction behavior and contextual denoting conditions, scams-related tendencies and AI-supported risk assessment in order to have a timely and implementable warning about a potentially risky financial transfer before or before its occurrence.

III. AI-BASED EARLY WARNING SYSTEM FOR FINANCIAL SCAMS

The AI-Based Early Warning System of Financial Scam on Consumer (AI-EWS) is aimed at moving the financial fraud management system of financial scams towards proactive measures rather than traditional, reactive means of fraud detection. Existing fraud detection techniques are primarily designed to identify irregular transactions that have already been processed when a red flag activity has already occurred but consumer scam is frequently done by users involved in legitimate transactions being duped to sanction the payment themselves [1], [2]. In this way, the proposed framework is designed to identify abnormalities in the behavior of consumers, transaction characteristics, relations between the recipients, and contextal hints in the context of the potentially fraudulent transfer. The system consists of the data ingestion, preprocessing, data behavioral profiling, anomaly detection, scam type, dynamic risk scoring, explainable artificial intelligence (XAI), and real-time generation of alerts.

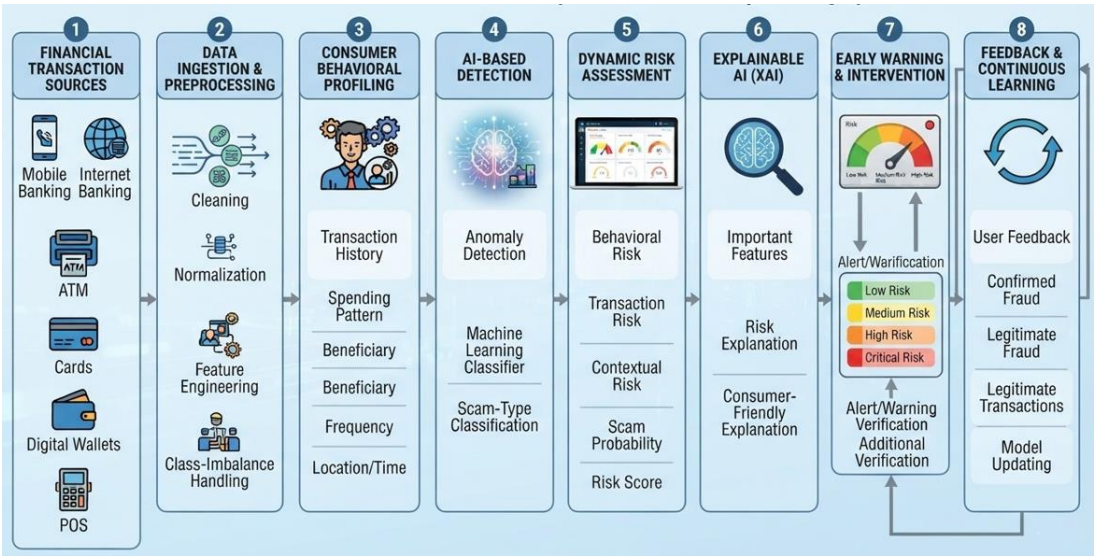

Figure 1- Overall Architecture of the Proposed AI-Based Early Warning System

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 3, May-June 2024||

DOI:10.15662/IJRPETM.2024.0703016

3.1 System Architecture

The AI-EWS consists of seven interconnected layers: **(1) Financial Data Sources, (2) Data Ingestion and Preprocessing, (3) Consumer Behavioral Profiling, (4) AI-Based Scam Detection, (5) Dynamic Risk Assessment, (6) Explainability and Alert Generation, and (7) Feedback and Continuous Learning**. The architecture would be utilized in other banking and digital-payment channels so that the information at the transaction and behavioral level can be handled by a single framework.

The initial layer intercepts information of mobile banking, Internet banking, ATM and credit/debit cards, point of sale, payment gateways/fund transfer services. Other than this contextual attribute, the information about the transaction is also considered by the framework in addition, the contextual data also contains the time of the transaction, the location of the transaction, the description of the device that was used in the transaction, the account history, age and the frequency of the transactions in addition to previous encounters with the customers. The necessity to use different data sources lies in the fact that scams nowadays may be based on a number of different communication and payment systems [3], [4].

3.2 Data Ingestion and Preprocessing Layer

The second layer does secure data ingestion and preprocessing. Normalization of incoming transactions into a standard and data cleaning, missing values, data elimination, normalization and encoding of categories are done. The reason behind storing the temporal information is that sharp changes in the frequency or even the time-period on which the transaction occurs could be helpful in producing the information on behavior.

It is followed by a feature engineering process to glean variables of deviation in the number of transactions, frequency of transfers, newness of recipients, velocity of transfers, anomaly in geographical locations, anomalous payment patterns and schedule of transfers. Freedom of feature selection is a necessity in fraud detection especially in cases where irrelevant variables may add complexity to an equation and also cause diminishing variability of a model [9], [10]. Since in general fraudulent transactions constitute a small part of overall financial activity, the imbalance in the classes is also balanced by appropriate sampling or weighting strategies of classes by their classes [13].

3.3 Consumer Behavioral Profiling

The Consumer Behavioral Profiling Module is among the key aspects of the proposed framework. The system sets dynamic behavioral base point of individual consumer rather than that of individual transaction in itself. Normal patterns of money spending and transferring money is characterised with the historical data.

The contents of this profile could include the average amount of transaction, the usual frequency of the transaction, the most frequent beneficiaries, of the frequency used channels of transaction and geographical location of the transaction mostly used, usual time of transaction and previous type and category of transaction. These profiles are constantly updated by the system as new legitimate behavior is seen. As a result, a transaction is assessed depending on the behavior pattern that a consumer has established as opposed to a set universal standard.

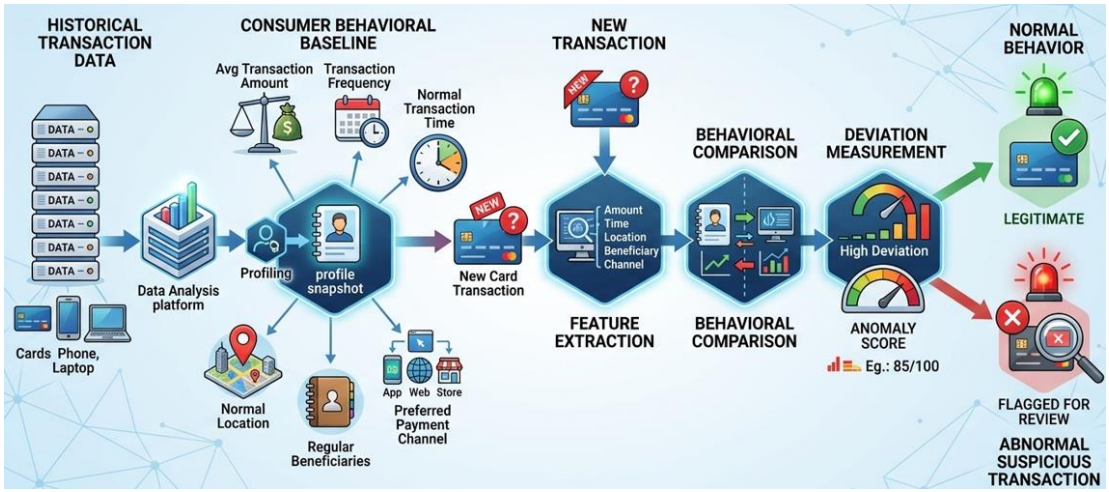

Figure 2- Consumer Behavioral Profiling and Anomaly Detection Process

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 3, May-June 2024||

DOI:10.15662/IJRPETM.2024.0703016

This is particularly crucial to consumer scams because the identical transaction may appear verifiably correct however bizarre, to a particular person. This can involve a large amount of value transfer such as depositing suddenly into an account of a new beneficiary sufficient to possibly represent an investment or an impersonation campaign although the money has gone through the regular qualification procedures.

3.4 AI-Based Scam Detection Layer

The fourth layer incorporates a number of AI models which are more likely to identify diverse forms of suspicious acts. An anomaly detecting component recognizes transactions that considerably differ with past consumer pattern. Simultaneously a machine-learning image is applied to rate transaction and contextual features to forecast the probability of fraud.

Logistic regression, random forest, gradient boosting, CatBoost and neural networks are some of the algorithms that can be implemented within the framework. The existing sources demonstrate that CatBoost and deep neural networks can be utilized in card-fraud detection [11], just as well as a series of neural-networks with feature engineering which can be found to be even more effective in detection [12]. The suggested framework, consequently, adopts a model-agnostic framework wherein various algorithms can be tried and decided upon based on their precision, computation, interpretation and implementation scenarios.

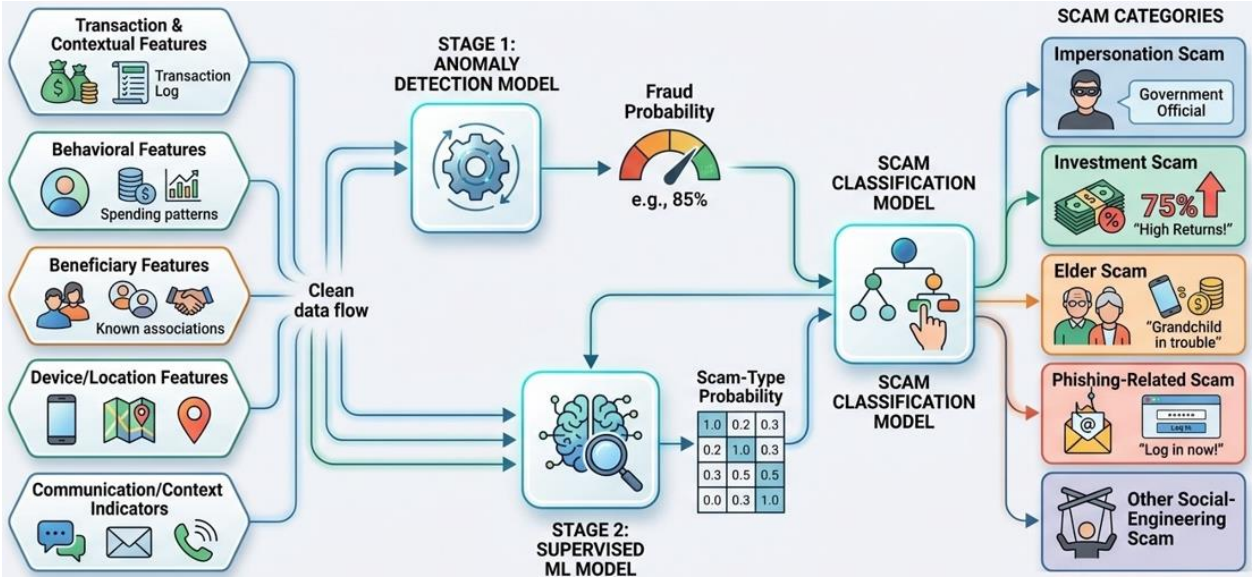

Figure 3- Multi-Stage Scam Detection and Classification Model

The other scam-specific classification module further divides the suspicious activity under a large scam category of the consumer such as impersonation scams, investment scams, elderly scams and scams in phishing and other social engineered financial scams. The classification will facilitate the system to provide contextual warnings as opposed to generic fraud warnings.

3.5 Dynamic Risk Scoring

The output of the anomaly detector and classification models is combined by the Dynamic Risk Assessment Engine. Instead of making a binary legitimate/fraudulent decision, the system puts out a weighted scoring of risk between low and high-risks on a continuous scale.

The risk score can be formulated as:
R=w1A+w2B+w3C+w4S+w5HR = w_1A + w_2B + w_3C + w_4S + w_5H
where AA represents the anomaly score, BB represents behavioral deviation, CC represents contextual risk, SS represents scam-type probability, and HH represents historical risk indicators. The weights w1,…,w5w_1,\ldots,w_5 can be optimized during model training.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 3, May-June 2024||

DOI:10.15662/IJRPETM.2024.0703016

This is further classified into low-risk, middle-risk and high-risk and critical-risk transaction. It is carried out in normal fashion when the transaction is low-risk but when it is a more risky transaction, it can be subjected to more verification or warning consumers according to the policies of the banking institution.

3.6 Explainable AI and Early Warning Generation

Explainability is a critical aspect since the consumers are concerned and also the financial institutions, would be aware of why a transaction has been raised. The proposed structure thus consists of an XAI module, defining the most important factors of a risk score. Attributing features can be done by identifying attributes of transactions and behavior that are influential, e.g. with Shapley-value-based explanations [10].

They are free to provide a demonstrative instance why the transaction is suspect and no longer a generic response like theirs; transaction seems suspicious when compared to the generic message. This will enhance awareness of the user and facilitate this decision making.

The Early Warning Engine transforms the model outputs to the relevant interventions. Based on the severity of advancement of the risk, it may create informational warnings, confirmation inquiries, more thorough authentication warnings or warnings that necessitate the consumer to reevaluate the act. This is a prevention means that is proactive and complementary to the awareness-based prevention means mentioned by Barker [2].

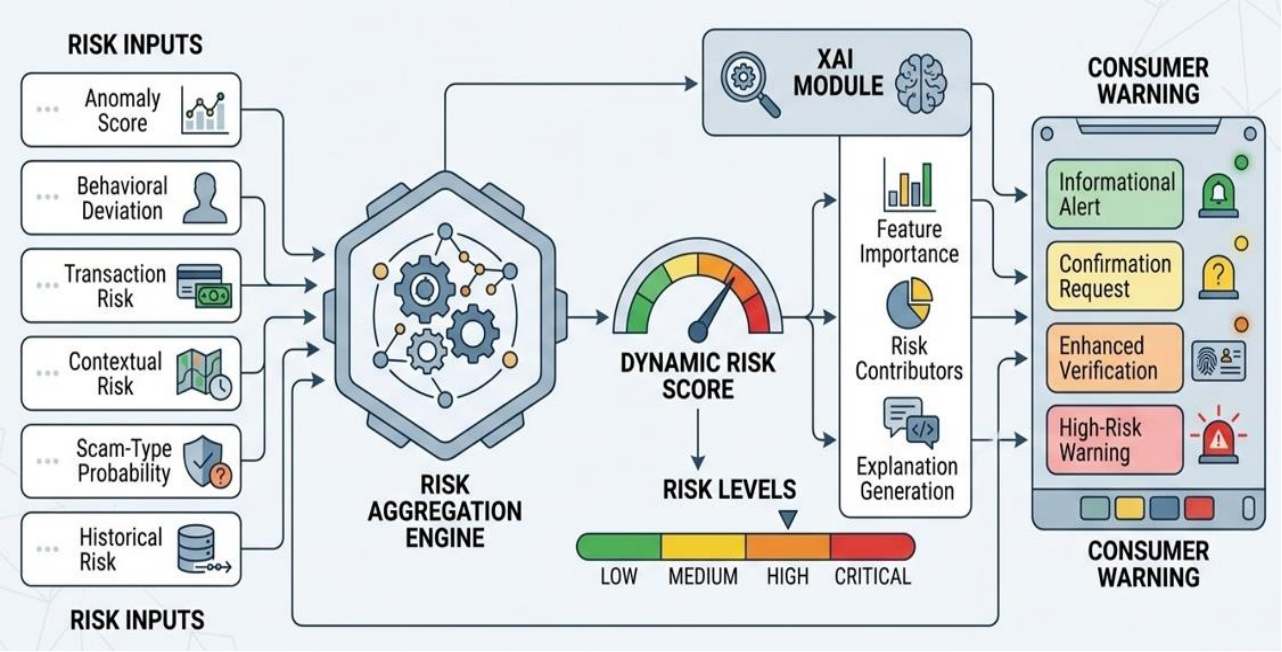

Figure 4- Dynamic Risk Scoring and Explainable Early-Warning Mechanism

3.7 Feedback and Continuous Learning

The last layer will capture the results of the alert, user confirmations, investigation and post-conduct of fraud. Data, legitimate and fraudulent is passed into the learning loop to continue re-training and re-calibrating the models. This will help the system to adapt to evolving scamming behavior, evolving consumer behavior and emerging consumer-risk behavior.

The proposed AI-EWS will consist of behavioral profiling, anomaly detection, machine learning, classification based on the type of scam, dynamic risk scoring, XAI, and proactive intervention in one architecture. The scheme as opposed to the classical system of frauds which is founded on transactions [9], [11], [12] offers a strategy to a consumer and consumer behaviour and also it detects the socially-friendly financial fraud at an early age. This is what makes it particularly suitable in determining the abnormal transfers in terms of impersonation, investment and elder scams and the retrospective fraud-investigation would change the view of a proactive consumer protection of money.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 3, May-June 2024||

DOI:10.15662/IJRPETM.2024.0703016

IV. SCAM-AWARE RISK EVALUATION AND EARLY-WARNING VALIDATION

The proposed Early Warning System, which is an AI-based technical detection and consumer-protection approach is taken into account. Unlike the conventional fraud detection systems that primarily aim at detecting the level of classification accuracy, the proposed framework must also demonstrate itself to detect uncharacteristic consumer transfers, various scam schemes, reducing the false alarms, and timely and understandable warning. Predictive performance, risk discrimination, explainability, operational responsiveness are thus considered in the assessment.

4.1 Detection Performance Evaluation

The initial dimension of assessment is applied to check the effectiveness of the AI models to differentiate between the legitimate transactions and the possible fraudulent transactions. Standardized scores (accuracy, precision, recall, F1-score and area under ROC curve (AU C -ROC) are taken. Additional consideration is given to recall due to a blind spot in regard to a concrete scam project, a huge loss of the consumer can occur. Precision: It is also useful because with excessive false positives you may experience alert fatigue, and consumer confidence. This comparison is founded on the comparison of separately trained machine-learning models with the proposed integrated architecture to presuppose whether performance in the approaches of additional behavioral, contextual and transaction-level features improves the detection. Class-balances are also considered as fraudulent transaction normally constitutes a small portion of the financial records [9], [13].

4.2 Scam-Type and Behavioral Evaluation

The second dimension would be the capacity of the structure to detect the impersonation, the investment and transfers of elder-scam. All types of scams gauge performance to determine the effectiveness of the system in different behavioural patterns. When it comes to predicting risk, behavior deviation indicators such as odd transactions, introduction of new beneficiaries, odd rate transactions, new address and strange time transactions are evaluated. This is particularly important since authentic transactions initiated by authorized transactions may be referred to as fraudulent acts, which could be initiated by the victims and used in lieu of technically non-authorizing account activity [1].

4.3 Risk Scoring and Early-Warning Effectiveness

The dynamic risk engine is gauged based on its capability to prioritize transactions based on their possible scam risk. The various risk related transactions (low, medium, high and critical) are analyzed to identify whether the level of escalating risk level is linked to increasing rates of detected activity levels of suspiciousness. Measures of the capacity to detect early are the alert latency, capacity to predict the completion, the proportion of risky transactions happening preceding the detection and the degree to which a purchase transpiration happens preceding the currency loss. Another issue discussed is the intervention strategy of the system in order to decide that there should be a matching in the warnings to the supposed system risk.

4.4 Explainability and Operational Robustness

Lastly, the framework is assessed in terms of the quality of the explanation and reliability. The results of the XAI are to gauge whether they can describe the major risk factors in such a straightforward and succinct manner. This is notable because black-box behavior can lead to a reduction in the trust of the automated decisions about fraud [10]. The building may also be put to test based on the various quantity of transactions, moving indicators of fake, and even novel and unfamiliar behavioral traits. Observed stability of model effectiveness (as new confirmed cases of fraud and legal cases are added) is also used to measure continuous-learning performance. A combination of these measurements will establish the effectiveness of the proposed system in offering viable and accurate, real-time, responsive, and interpretative early alerts regarding consumer -centered financial frauds.

V. CONCLUSION AND FUTURE WORK

This study solved the shortcomings of the conventional approaches to fraud detection by laying out an Artificial Intelligence Based Early Warning System to Financial Scams against Consumers. The given framework takes into account not only the behavioral but also the contextual specifics of consumer initiated transfers, rather than focusing on those transactions, which are not approved. It consists of transactional information, behaviour-based consumer profile, machine intelligence based scam ranking, real-time risk rating, explainable AI, proactive warnings. The framework is aimed specifically at detecting the presence of unusual transfer which might relate to impersonation scams, investment scams and older financial scams.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 3, May-June 2024||

DOI:10.15662/IJRPETM.2024.0703016

The added importance of the framework is that the framework can provide tailor-made predetermined levels of behavior, which will determine the abnormality of normal financial management. The facilities of dynamic risk scoring and courageous suspicious transactions a priority based on estimating their risks and the XAI element provide the rank of the sensible explanations of generated warnings. The proposed plan can hence help the banks and the customers to make the right decision on time before the suspicious transfer can result into huge losses. Feedback and continuous learning can also be incorporated into the framework to allow adjustment to new scam trends and evolve consumer behavior. Overall, the given architecture will be used to change the financial scam management paradigm to be more focused on the financial scams prevention and prevention instead of being reactiveness-based to detect and eliminate such scams**.**

The template will be applied in subsequent designs, to experimentally validate it on a large, real world and synthetic financial transaction data set of various consumer scam scenarios. Deep-learning, graphical systems may be viewed to model complex consumer, beneficiary, device, account and interact systems. It can also include federated learning to allow the development of models across financial institutions collaboratively and minimize the necessity of centrally distributing sensitive data on transactions.

Future research must concern multimodal scam detectors, such as transactional behaviour, and appropriate textual, communication and contextual facts. The development of adaptive risk levels and individual intervention plans might help to minimize the false positives and misleading alarms. Other tests that would be applicable in the future on the framework is running experiments of real time deployment, longitudinal test, adversarial scam test and human centred usability. Lastly, additional explainability, privacy protection, equity test, and regulatory enforcements shall also be considered to make sure that this system is not only accurate, but it can as well be trusted, open, and utilizable in the financial-sector.

REFERENCES

[1] J. Jansen and R. Leukfeldt, “How people help fraudsters steal their money: An analysis of 600 online banking fraud cases,” in *Proc. Workshop Socio-Technical Aspects Security and Trust (STAST)*, Verona, Italy, Jul. 2015, pp. 24–31, doi: 10.1109/STAST.2015.12.

[2] R. Barker, “The use of proactive communication through knowledge management to create awareness and educate clients on e-banking fraud prevention,” *S. Afr. J. Bus. Manag.*, vol. 51, no. 1, Art. no. a1941, 2020, doi: 10.4102/sajbm.v51i1.1941.

[3] A. P. Abidoye and B. Kabaso, “Hybrid machine learning: A tool to detect phishing attacks in communication networks,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 6, pp. 559–569, 2020, doi: 10.14569/IJACSA.2020.0110668.

[4] L. R. Maulana, A. N. Fajar, and Meyliana, “Extending the design of smart mobile application to detect fraud theft of E-banking access using big data analytic and SOA,” in *Proc. 2021 IEEE 5th Int. Conf. Inf. Technol., Inf. Syst. Electr. Eng. (ICITISEE)*, Purwokerto, Indonesia, Nov. 2021, pp. 360–364, doi: 10.1109/ICITISEE53823.2021.9655805.

[5] S. S. Khalaf Al Hattali, S. M. Hussain, and A. Frank, “Design and development for detection and prevention of ATM skimming frauds,” *Indones. J. Electr. Eng. Comput. Sci.*, vol. 17, no. 3, pp. 1224–1231, 2019, doi: 10.11591/ijeecs.v17.i3.pp1224-1231.

[6] C. Tsai and P. Su, “The application of multi-server authentication scheme in internet banking transaction environments,” *Inf. Syst. e-Bus. Manag.*, vol. 19, pp. 77–105, 2021, doi: 10.1007/s10257-020-00481-5.

[7] B. Hammi, S. Zeadally, Y. C. E. Adja, M. Di Giudice, and J. Nebhen, “Blockchain-based solution for detecting and preventing fake check scams,” *IEEE Trans. Eng. Manag.*, vol. 69, pp. 3710–3725, 2022, doi: 10.1109/TEM.2021.3087112.

[8] M. I. Abdul Rani, S. N. F. Syed Mustapha Nazri, and S. Zolkaflil, “A systematic literature review of money mule: Its roles, recruitment and awareness,” *J. Financ. Crime*, 2023, doi: 10.1108/JFC-10-2022-0243.

[9] 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, Art. no. 24, 2022, doi: 10.1186/s40537-022-00573-8.

[10] J. Chaquet-Ulldemolins, F.-J. Gimeno-Blanes, S. Moral-Rubio, S. Muñoz-Romero, and J.-L. Rojo-Álvarez, “On the black-box challenge for fraud detection using machine learning (I): Linear models and informative feature selection,” *Appl. Sci.*, vol. 12, no. 7, Art. no. 3328, 2022, doi: 10.3390/app12073328.

[11] N. Nguyen, T. Duong, T. Chau, V.-H. Nguyen, T. Trinh, D. Tran, and T. Ho, “A proposed model for card fraud detection based on CatBoost and deep neural network,” *IEEE Access*, vol. 10, pp. 96852–96861, 2022, doi: 10.1109/ACCESS.2022.3205416.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 3, May-June 2024||

DOI:10.15662/IJRPETM.2024.0703016

[12] E. Esenogho, I. D. Mienye, T. G. Swart, K. Aruleba, and G. Obaido, "A neural network ensemble with feature engineering for improved credit card fraud detection," *IEEE Access*, vol. 10, pp. 16400–16407, 2022, doi: 10.1109/ACCESS.2022.3148298.

[13] P. Gupta, A. Varshney, M. R. Khan, R. Ahmed, M. Shuaib, and S. Alam, "Unbalanced credit card fraud detection data: A machine learning-oriented comparative study of balancing techniques," *Procedia Comput. Sci.*, vol. 218, pp. 2575–2584, 2023, doi: 10.1016/j.procs.2023.01.231.

[14] P. Sharma, S. Banerjee, D. Tiwari, and J. C. Patni, "Machine learning model for credit card fraud detection—A comparative analysis," *Int. Arab J. Inf. Technol.*, vol. 18, no. 6, pp. 789–796, 2021, doi: 10.34028/iajit/18/6/6.