International Journal of Advanced Engineering Science and Information Technology (IJAESIT)

|ISSN 2349-3216| Volume 8, Issue 5, September-October 2025| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|

DOI: 10.15662/IJAESIT.2025.0805016

Real-Time Preemptive Fraud Detection Using Adaptive Agentic AI for Financial Transaction Risk Intelligence

Manas Ranjan Panda, PhD

Consulting Partner, Banking and Financial Services, Wipro, USA

ABSTRACT: The sudden change of digital financial services has revolutionized the financial transactions, made them complicated, fast and large volume making it so challenging to the traditional financial fraud detection paradigms, which relies on predetermined patterns and a sluggish process. A Real-Time Preemptive Fraud Detection Framework is proposed in this study based on the Adaptive Agentic Artificial Intelligence (RPAFAI) to determine the intelligent financial transactions risk. The suggested system combines real-time transaction information, behavior categorization, situational risk assessment, dynamic machine learning, and self-sufficing AI programs to detect possible fraudulent actions prior to the conclusion of the transaction. The framework is further subdivided into six key levels, namely: (1) Transaction Data Ingestion Layer that constantly gathers transactional and contextual data; (2) Feature and Behavioral Intelligence Layer on which time and transactional-based requirements are temporally processed along with user/behavioral requirements, which are provisioned into future detection results; (3) Adaptive Agentic AI Layer that temporarily processes transactional capabilities in which the special AI agent gathers and an incorporated output that is translated into the future detection results; (4) Real-Time Risk Intelligence Layer where time and transactional-based requirements are processed continuously, alongside user/behavioral requirements, which are incorporated into future detection results; (5) Preemptive Decision and Response Layer that continually incorporates visible results into future detection results; and (6) Feedback and Continuous Learning Layer that constantly integrates results of known outcomes into future doubts. The framework is designed to minimize detection time, false positive and maximize its use to new trends of frauds and maximize real time financial risks knowledge. The proposed methodology provides an arena of active and independent prevention of frauds in the modern digital financial arena and ecosystems.

KEYWORDS: Agentic AI, Fraud Detection, Financial Transactions, Real-Time Risk Intelligence, Adaptive Machine Learning, Preemptive Fraud Prevention

I. INTRODUCTION

E-wallets and real time payment systems, online shopping systems, wireless payment systems and online banking have altered radically the fast revolution in the financial industry hence resulting in a considerable quantity coupled to tremendous speed in the transactions in the finances. Not only has digitalization brought with it higher accessibility and convenience, and more efficient transaction, but has also brought with it novel sources of complex financial fraud. Some of the crooks have also started to employ the stolen credential, hijack accounts, artificial identities, anomalous transactions, social engineering, as well as dynamically altered behavioral patterns as an evasionary tactic against the customary security precautions [1]. The rate of transacting of funds and the dynamic nature of fraud pyramid are high and prompt and correct detection of fraud is now becoming critical requirement in the modern financial institution. This has led to the need of the financial organization to possess smart systems that will process the transactions that occur and detection of any threats before the transactions including fraudulent transactions are executed [2].

Commonly used methods of fraud detection have largely been based on pre-determined rules, statistical methods and the typical machine-learning detectors. Rule-based systems are very effective at detecting known patterns of fraud by means of manually-written conditions; however, when tactics employed by fraudsters are rapidly changed around, they can become a bottleneck to rule-based systems. Also absolutes may produce a large size of false positives (resulting in unnecessary rejection of transactions and inconvenience to customers). Similarly, traditional, supervised machine-learning models may have good predictive accuracy, assuming representative historical data, but fail when encountered with new forms of fraud, concept drift, skewed information on transactions, and new forms of attack behavior. In addition to this, most of the fraud detection systems that remain have been proactive systems, and which stays operational until it detects the occurrence of a suspicious transaction or sufficient evidence has been obtained. Such limitations justify the need to have responsive, proactive as well as real time fraud intelligence systems [3] [4].

|ISSN 2349-3216| Volume 8, Issue 5, September-October 2025| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|

DOI: 10.15662/IJAESIT.2025.0805016

A new challenge is also introduced with the real-time processing of transaction as the detection of fraud has to be carried out within minute time frames. There can be numerous contextual aspects of financial transaction, part of which consist of: size of transaction, frequency of transaction, geographic, specifications of devices, authentication behavior, attributes of merchants, past customer behaviour and account annotations. An effective fraud detection system should therefore have a capability to mix diverse sources of data as well as continually factor the dynamic levels of risk in each transaction. An intelligent architecture ought to utilize a mixture of behaviours, contextual reasoning, anomaly providing, and adaptive decision-making as opposed to using a specific model of prediction. This need drives the deployment of the Agentic Artificial Intelligence (Agentic AI), where autonomous or semi-autonomous AI agents may assume the role of specialized analytical agents, work collaboratively with other agents, contextualize information and aid in contextually informed decision-making.

A Real-Time Preemptive Fraud Detection Framework (named as Adaptive Agentic AI abbreviated RPAFAI) proposal, in relation to the underpinning of financial transactions risk intelligence, is put forward in this research. The paradigm shift in the framework is to change the existing paradigm in fraud detection to a rather reactive paradigm to a more proactive and adaptive intelligence paradigm. The RPAFAI would always check the setting of transactions, anomaly in behavior, time series, would also develop the risk indicators and analyse probabilities of a fraud case even before the transaction process is completed. The framework will be in place to help in quick risk analysis whilst not being rigid to evolving fraud schemes.

The RPAFAI architecture proposed has six layers which are interconnected. Ingestion Ingestion Data Layer stores the high velocity transaction and situational data of banking services, payment gateway, digital wallet and merchant platform among other financial services. The Feature and Behavioral Intelligence Layer converts the raw flows of transaction into features that are useful, such as the temporal contribution, the speed of the transaction, consumers actions, device details, the location patterns and risk intelligence of the past. It is these attributes that form the basis on defining deviations as regards to the valid behavior profiles.

The third element is the Adaptive Agentic AI Layer that is the character of the intelligences of the proposed structure. Depending on the type of transaction being examined, different specialized AI agents can analyze various attributes on their own, such as behavior anomalies, patterns, and contextual risk, network relationships and historical activity. These agents are coordinated and their outputs to analysis are integrated by an orchestration mechanism. This layer has an adaptive property which enables the system to adjust its strategies of detection to new trends of fraud as detected, and feedback of previous judgments.

The Real-Time Risk Intelligence Layer is a combination of the indications of a computational analysis and constructs a dynamically changing score of transaction risk. The layer does not only base their classification of frauds on binary classification but it provides a dynamic modeling of the transaction risk which can be composed of many signals and varying levels of confidence. This is followed by the next Preemptive Decision and Response Layer which changes the risk intelligence into an appropriate operation action. As soon as the risk level is considered, it may provide approval to transactions, or utilize additional checks on that transactions, or human investigation or even block them. So that it is possible to avoid unnecessary intervention with the help of such mechanism of the response as risk, at the center of which the transactions of high risk are located.

Finally, the Feedback and Continuous Learning Layer becomes part of the learning process because of the confirmed cases of frauds, the right results of casing, the decision-making process of the investigator and the appearance of the new behavior trends. This feedback is needed to deal with the machine learning degradation and drift. RPAFAI will also enhance its detection capabilities of novel fraud behaviors as well as strong detection of established patterns by continually revising the intelligence used by the agentic system.

The proposed research offers some of the contemporary subjects of concern in the domains of financial fraud detection such as detection latency, evolution of fraud, minimization of false-positive, complexity in behaviors and scalability. The framework also concentrates on the synthesis of independent thinking incorporated with machine reasoning to assess the risks and hence, it resembles financial transactions monitoring in a more lenient manner. A conceptual foundation of next-generation financial fraud detection RPAFAI is a streaming data processing transcription, behavioral intelligence, adaptive machine learning, multi-agent analysis and preemptive response based, conceptual basis of financial fraud detection.

The importance of this study is that, it tries to develop a clever and flowing structure that might convert the vast amount of transactions to usable risk knowledge. Such a solution could assist financial institutions to reduce potential financial losses, boost customer trust in them, improve the safety of transactions, and respond more effectively to constantly

|ISSN 2349-3216| Volume 8, Issue 5, September-October 2025| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|
DOI: 10.15662/IJAESIT.2025.0805016

evolving trends in fraud. This structure may then be extended to the creation of active and autonomous as well as real-time systems of fraud detection that may be extended to the more complex digital financial systems.

II. RELATED WORK

The methods of financial fraud detection have shifted to machine-learning, deep-learning, graph-based and adaptive artificial intelligence instead of the traditional and customary statistical and rule based methods. The growing complexity of financial transactions, the rate of imbalance between classes, variations in context of fraud and need to make prompt decisions have turned the interest of the researchers in developing more intelligent recognition systems and more situation sensitive of fraud. The extent literature provides a decent background regarding the development of real time and preemptive fraud detection systems but there are crucial gaps present in the field of discussion in aspects of adaptability, independent decision making and sustainable risk intelligence.

Later traditional classifying techniques demonstrated that with supervised learning, it was possible to detect credit cards frauds and comparative analysis was carried out to explore the applicability of different data-mining algorithms as a means to detect fraud in transactions [11].

A thorough discussion of machine-learning-based detection of fraud in the finance sector put a particular emphasis on the growing use of both supervised and unsupervised and hybrid machine-learning in detecting financial fraud [5]. However, financial transaction datasets are often associated with drastic imbalance of classes of transactions, with the number of legitimate transactions by far exceeding that of fraudulent transactions. This imbalance will lead to the standard classifier inclining towards the great category of cases and thus make imprudent evaluation of the unusual cases of the fraud. This issue has therefore enabled it to gain great attention today in the field of Fraud detection due to the relevance it has in this aspect.

The graphical methodology has turned out to be a potentially beneficial method since the monetary exchange inherently appears to be a network of interrelated structures that take the form of a customer, account, device, merchant, locations and correlations among transaction. Graph neural networks (GNNs) offer representation learning on these relational structures and have been deeply studied to be used in applications that use complex networks [9]. Graph-based methods can also be used in financial fraud detection in situations where individual transactions are examined one by one to establish links which might not be evident to the naked eye. A imbalance learning-based transaction-level fraud user model that employs GNNs have shown that a combination of the class-imbalance solution with a corresponding representation learning is the key to detecting fraud in financial transactions [1]. This trend is particularly applied to real time financial risk intelligence, since the suspicious behavior can occur not only due to the features of transactions, based on which the particular transaction is suspicious, but also due to the associations of different actors.

The attention operation has further helped in enhancing the detection of graphic frauds as the graphs are able to rank the relevancy of the nodes, relation and characteristics of transactions. Attention-based GNN demonstrated that transaction networks meaningful structural and behavioural information can be enhanced by giving special attention to the multi-level attention mechanism in order to detect fraud [2]. These approaches can create better contextual fraud detectors, but are typically model-based and cannot impose themselves or have the multi-agent reasoning capabilities.

It has also been concerned with the interests in both adversarial and generative types of learning in an attempt to enhance the detection of fraud related cases within intricate and in-minor data settings. The extent to which attention and generative learning could be combined to have better performance in detecting financial fraud was also discovered in an attention generation adversarial network approach [3].

The other critical area of research to undertake is to deter graph-based fraud detectors of superior criminals who even actively go ahead to conceal their footprints despite the normal transaction trends. Ironically enabled by graphic analysis, by detecting the frauds with their help, it becomes possible to redeem the persons with ill aims and exploit the correct identification of their structural relationship, bending it in favor of their objective of proving it a real user. The significance of being resistant to adversarial and deceptive flavor of fraud detectors by focusing on GNNs can be illustrated using methods that have been devised to resist camouflaged fraudsters [6]. This holds significant importance so as to prevent fraud detection at its earliest stage since there are new types of fraud and new types need to identify subtle variations so that enough evidence is attained that the traditional rule based method will capture it.

Heterogeneous graph learning is yet another useful adaptive financial intelligence base. An advantage of metagraph-based learning is that the models are capable of learning different types of relations in a heterogeneous network [8]. The concept is further improved in the context of a differentiable meta-graph search where useful graph structures to

|ISSN 2349-3216| Volume 8, Issue 5, September-October 2025| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|

DOI: 10.15662/IJAESIT.2025.0805016

heterogeneous graph neural networks are discovered automatically [7]. Compared to entirely depending on manually crafted models, neural architecture search offers a more general methodological basis of automatically determining useful neural architectures [10]. This will proceed to more flexible AIs which can change or adjust their interior analytic organization to task needs.

Machine learning has also been applied in the creation of fraud prevention in lieu of transaction classification in addition to blockchain. A blockchain-based health care claims fraud detection and prevention system proved that distributed and tamper-resistant records of transaction can be helpful in complementing machine-learning-based fraud detection [4]. The context of application is unrelated to the context of financial transactions but the study demonstrates the helpfulness of combining ingenious detection with secure data-management measures.

Irrespective of these developments, the existing approaches can be classified into those that focus on the individual detectors, the learning graph models, or adversarial indestructibility, and secure transactions processing. The architecture of most of the systems has not incorporated any objects of AI to coordinate their interactions and autonomously communicate to learn the context of transactions, the production and construction of dynamic risk data as well as proactive behavior. Moreover, the traditional models tend to do classification or scoring as opposed to agentic reasoning. Thus, a research vacuum exists in order to come up with a universal scheme that integrates real-time streaming analysis, behavioral intelligence, graph based representation, adaptive learning, collaborative work of the autonomous agents, dynamic risk scoring, and preemptive response.

The introduction of the proposed Real-Time Preemptive Fraud Detection with Adaptive Agentic AI (RPAFAI) is an effort at sewing these features across this gap as a cogent financial transaction risk-intelligence design. Related to the outdated methods wherein, the decision whether or not a transaction is fraudulent is taken based predominantly on historical measures, the suggested framework is better geared to evaluate the risk at all costs and take proactive steps. It is structured in a way that it applies relationship on transactions, behaviour deviations, contextual information and past decision feedback to provide the adaptive and autonomic processes in dealing with fraud-risks. As such, it can provide a foundation to evolve the existing financial fraud detection into no movement and reactive classification to real-time, dynamic, collaborative and preemptive financial risk intelligence.

Financial fraud detection has increasingly shifted from conventional statistical approaches toward intelligent data mining and machine learning techniques capable of processing large volumes of transactional information. Al-Hashedi and Magalingam examined a wide range of financial fraud applications, including banking, insurance, financial statement, and cryptocurrency fraud, and demonstrated the growing importance of data-driven techniques for identifying complex fraudulent patterns. Their findings highlighted the need for intelligent models that can analyse heterogeneous financial data and support more effective fraud identification across different application environments [12].

The increasing complexity and volume of digital financial transactions have created significant challenges for traditional supervised fraud detection systems. Hilal, Gadsden, and Yawney reviewed anomaly detection techniques and emphasized the growing importance of semi-supervised and unsupervised learning approaches for identifying unusual and previously unseen fraudulent activities. Their work demonstrated that anomaly-based intelligence can complement conventional classification methods by detecting deviations from normal transactional behaviour, thereby supporting the development of more adaptive financial fraud detection frameworks [13].

Recent studies have further emphasized the role of machine learning in improving the speed, scalability, and predictive performance of financial fraud detection systems. Systematic reviews of machine-learning-based fraud detection have shown that algorithms such as support vector machines, artificial neural networks, ensemble learning, and other predictive models are widely applied to analyse large financial datasets. However, challenges related to highly imbalanced transaction data, evolving fraud strategies, false-positive rates, and the availability of labelled datasets continue to affect real-world implementation [14].

By 2024, research increasingly focused on more adaptive and intelligent fraud detection architectures capable of supporting continuous transaction monitoring and early risk identification. Recent literature reviews have highlighted the growing use of real-world financial datasets, supervised and unsupervised learning, anomaly detection, and deep learning to identify fraudulent behaviour across diverse financial environments [15]. These developments provide a strong foundation for the proposed Real-Time Preemptive Fraud Detection Using Adaptive Agentic AI for Financial Transaction Risk Intelligence, where adaptive AI agents can continuously evaluate transaction behaviour, dynamically assess risk, identify emerging anomalies, and support preemptive intervention before potentially fraudulent transactions cause financial loss.

International Journal of Advanced Engineering Science and Information Technology (IJAESIT)
|ISSN 2349-3216| Volume 8, Issue 5, September-October 2025| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|
DOI: 10.15662/IJAESIT.2025.0805016

III. REAL-TIME PREEMPTIVE FRAUD DETECTION USING ADAPTIVE AGENTIC AI

It is hoped that the proposed Real-Time Preemptive Fraud Detection using Adaptive Agentic AI (RPAFAI) framework can solve the problem of the previous-generation systems of detecting fraud which largely apply a finite number of fixed rules, an isolated machine-learning-based classifier, or a batching-based timeline. RPAFAI brings real-time transaction processing, behavioral intelligence, graphical contextual analysis, adaptive agentic reasoning, dynamic risk assessment, preemptive response, and the continual learning together into a cohesive architecture. The primary aim is to find out the presence of any fraudulent transactions at an early stage and implement an adequate intervention before any financial damages or dishonest actions occur.

It consists of 6 layers that are interdependent such as (1) Transaction Data Ingestion Layer, (2) Feature and Behavioral Intelligence Layer, (3) Adaptive Agentic AI Layer, (4) Real-Time Risk Intelligence Layer, (5) Preemptive Decision and Response Layer and (6) Feedback and Continuous Learning Layer. The layered architecture enables the provision of information on the transactions to contextual reasoning and adaptive decision-making and also enables giving feedback and results flow to the next stage of the fraud evaluation.

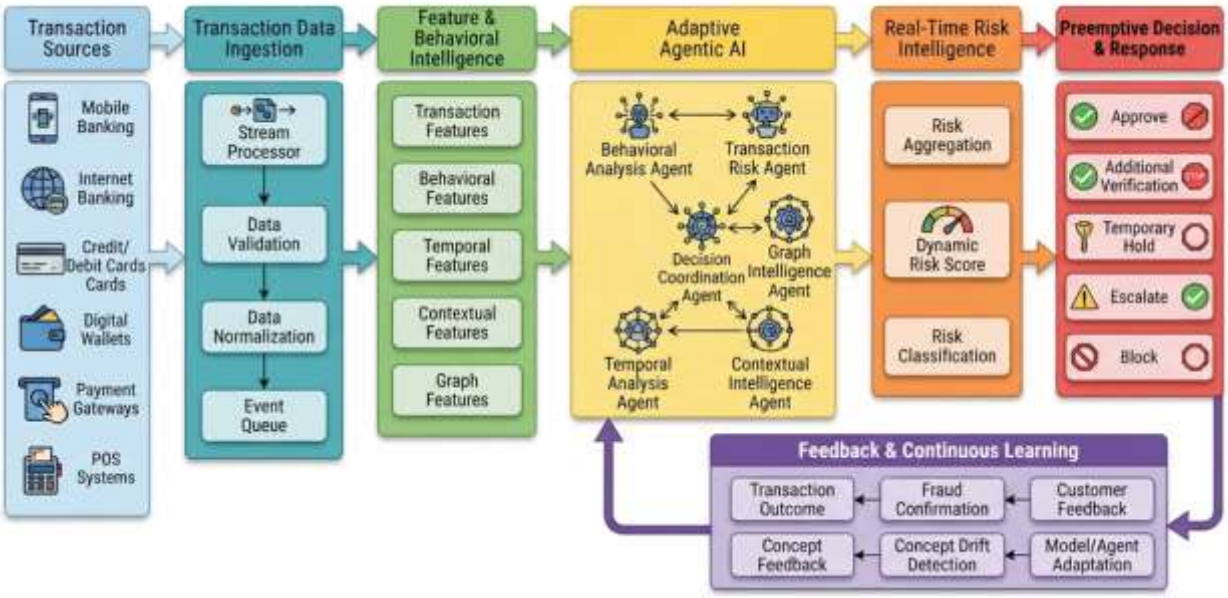


Figure 1- Overall Architecture of the Proposed RPAFAI Framework

3.1 Transaction Data Ingestion Layer

RPAFAI will comprise the front office which is the Transaction Data Ingestion Layer. It is constantly fed transaction events over heterogeneous financial channels, such as internet banking, mobile applications, payment gateway, point of sale, digital wallet, and card transactions, as well as, inter-bank payment networks. Some of the common attributes which can be included in any given transaction are: transaction amount, timing, account identifier, Merchant, location of transacting, device Character, payment channel, authentication and frequency of transaction.

The proposed layer is an event processing layer which is continuous in contrast to the traditional methods which happens to be batch oriented. Normalization of the received transactions is performed and this is verified, timestamped and translated into a familiar form and sends to the next analytical elements. Data-quality checks are done to determine missing, inconsistent, and duplicated or malformed records. The resulting flow of event data can be the foundation of low-latency fraud detecting and enabling the framework to swiftly respond to suspicious events.

3.2 Feature and Behavioral Intelligence Layer

The second layer is applied in transforming the event of transactions into meaningful analysis representations. Besides its utilization of only the static properties of the transactions, RPAFAI applies behavioral, temporal, contextual and relational properties. Deviations are features of behavior that are not historically fitting the characteristics of the transaction of the individual such as a large or a small number of transactions, bizarre frequency of transactions, or a weird kind of merchandise, a new gadget, or an abnormal geographical location of the transaction.

|ISSN 2349-3216| Volume 8, Issue 5, September-October 2025| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|
DOI: 10.15662/IJAESIT.2025.0805016

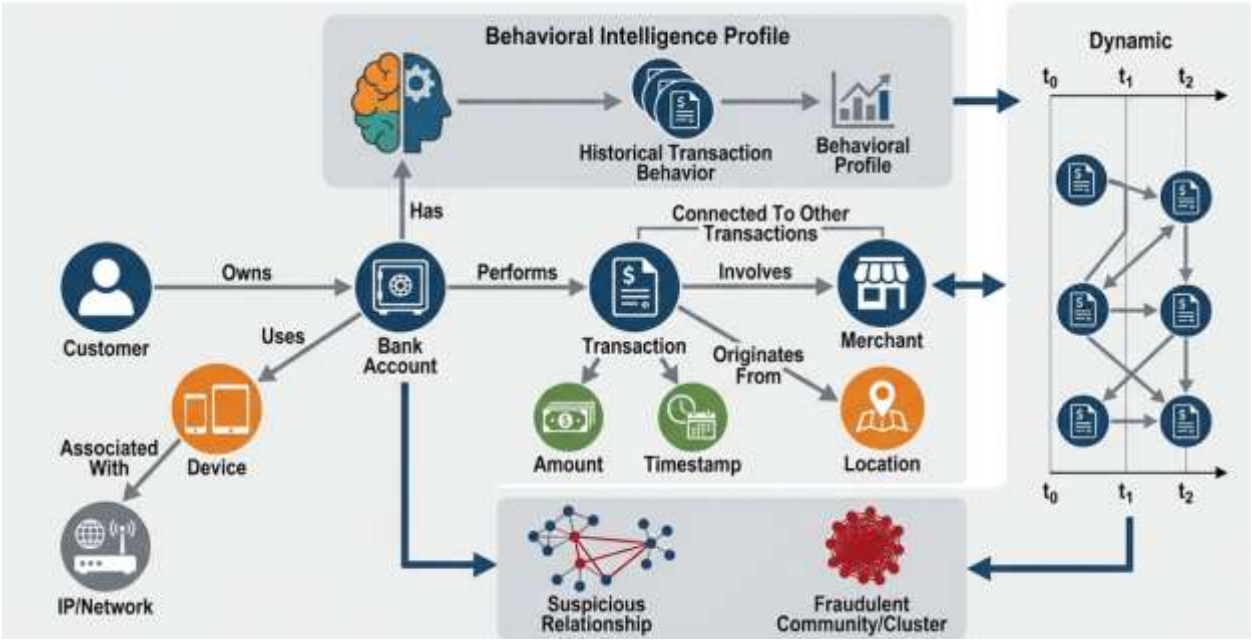


Figure 2- Dynamic Financial Transaction Graph and Behavioral Intelligence Model

Temporal properties record the sequence of transactions, and timing behaviour, e.g. fast fast consecutive transactions, abnormal transactions time and activity variation of transaction in short intervals. Contextual features augment the information on related accounts, merchants, devices, location and payment channels. These representations enable the framework to differentiate between high-value activity and legit activity and suspicious transactions depending on the situations in which they happened.

The layer also can produce a dynamic transaction-graph within which there exists, customers, account, devices, merchants and locations which are inter-relating. These interrelationships between these entities may give information to communities of transactions and maybe a coordinated fraud. The graph representations are more helpful in such instances, when there is a possibility of the activity in a number of apparently unrelated transactions.

3.3 Adaptive Agentic AI Layer

Adaptive Agentic AI Layer is the most significant aspect of intelligence of RPAFAI. The framework works in contrast to the single predicative model which consumes the whole analytics processes in favor of specialist AI agents which perform complementary analytical processes. This allows a decentralized thinking and a co-ordinated decision making.

Changes in behavior of customers and accounts are determined by heeding to behavioral Analysis Agent. The transaction Risk Agent is examining attributes based on the transactions and provides an initial risk assessment. Graph Intelligence Agent detects relationships between accounts, devices, merchants, and transactions as well as suspicious patterns in the network. A Temporal Analysis Agent evaluates the sequence of transactions and patterns which are dynamically emerging. Contextual Intelligence Agent is an agent, based on the conditions of the environment and past events to identify a state that so-called abnormal activity can be defined. Lastly, a Decision Coordination Agent combines the results of other specialized agents and finds the general risk state.

International Journal of Advanced Engineering Science and Information Technology (IJAESIT)
|ISSN 2349-3216| Volume 8, Issue 5, September-October 2025| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|
DOI: 10.15662/IJAESIT.2025.0805016

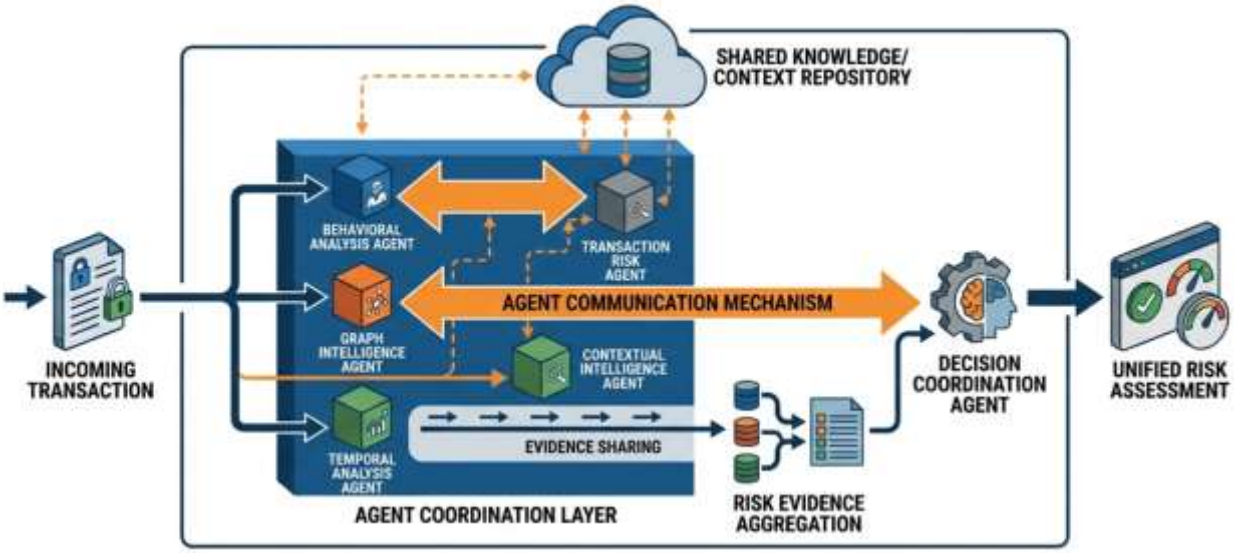


Figure 3- Adaptive Agentic AI Architecture for Financial Fraud Intelligence

The agents can coordinate and share the analysis results in a common coordination mechanism and simultaneously work. The architecture allows RPAFAI to take into account a transaction in multiple ways in comparison to the use of a single classification score. The behavior of agents can be customized to fit new patterns of fraud, too, facilitating more adaptable intelligence than architectures based on fixed rules.

3.4 Real-Time Risk Intelligence Layer

The Real-Time Risk Intelligence Layer takes actions by the agentic components and converts evidence to an ever-evolving transaction risk score. RPAFAI does not assume the categorization of risk based on the presence or absence of a fraud is binary but risk is a dynamic concept that is impacted by all types of evidence.

They can include transaction risk, behavioral deviation, graphical risk, timing anomaly, context based risk and reputation of the accounts in history as a risk score. Hypothetically, the overall risk can be given as:

R(t) = f(T, B, G, M, C, H)

T denotes nature of the transaction, B a behavioural deviation, G is the graph or relationship risk, M is the temporal or sequence generated aberration and C is the contextual data and H is the historical risk and feedback data.

The score obtained is maintained up-to-date as new evidence is sought. This enables the structure to recognize instances where a seemingly legitimate transaction, in the initial instance, has resulted in a red flag owing to occurrences of additional transactions, or other involved organizations, or even behavioral changes.

3.5 Preemptive Decision and Response Layer

Risk intelligence is one of the actions handled by Preemptive Decision and Response Layer. One can present the scheme of the classification of all the transactions to one or another response (low-risk, moderate-risk, high-risk, and critical-risk) based on the predetermined system of risks and recommendations offered by the circumstances.

To give the green light to the transactions that can be deemed as low risk, only a small intervention might be required. The additional checking installing such as step up or customer confirmation may be occasioned by the moderate risks transactions. The high-risk transactions may be held up to the extent it is further investigated and critical-risk events may get sent to a fraud investigation unit.

The main difference between the application of RPAFAI and fraud detection in a traditional system is that the frame puts more value on the preventative act as opposed to detecting the act. The system is tailored towards infringing the transaction or series of fraud or setting off early fraud indications. This is able to reduce the potential loss of funds, and reducing on unnecessary disruption of decent customers by prudent situation-guided decisions.

International Journal of Advanced Engineering Science and Information Technology (IJAESIT)
|ISSN 2349-3216| Volume 8, Issue 5, September-October 2025| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|
DOI: 10.15662/IJAESIT.2025.0805016

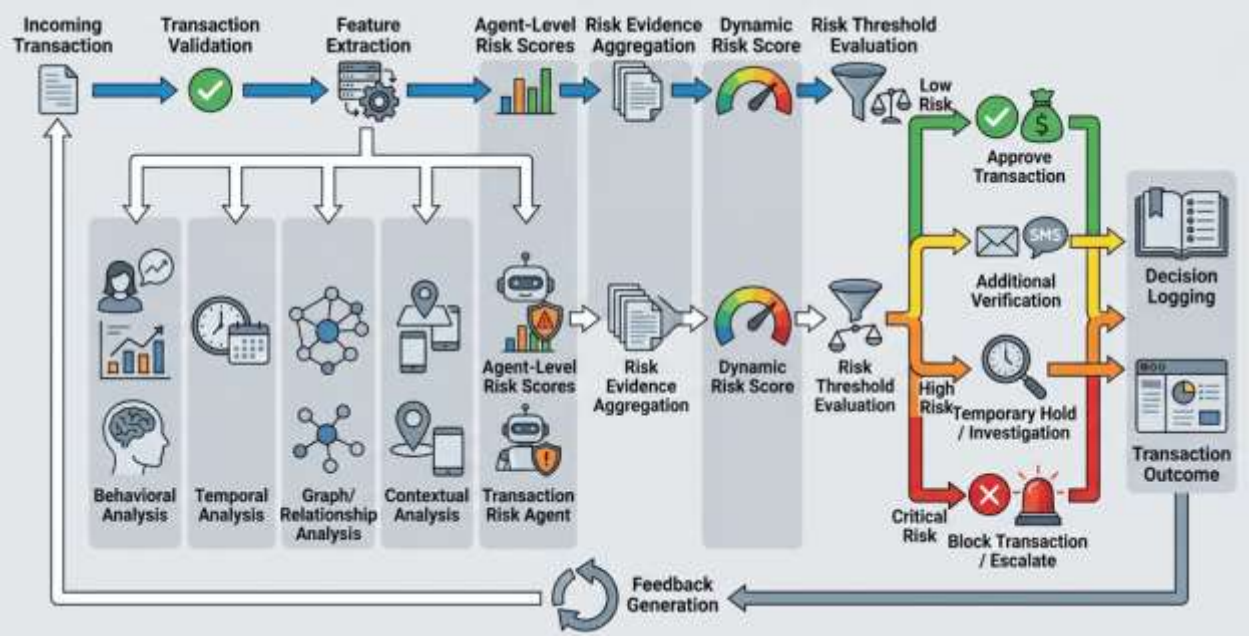


Figure 4- Real-Time Transaction Risk Assessment and Preemptive Decision Workflow

3.6 Feedback and Continuous Learning Layer

The last layer gives a closed-loop feedback between the results of operations and the analytical elements. The confirmed fraud, honesty, the outcome of customer checking, the decision of the investigators, false positive and false negative data are retrieved and fed back to the learning processes.

This feedback aids in immediate model and agent adaptation as concept drift, new fraud techniques and variation in the legitimate customer behavior emerges. Periodic re-estimation of agent policies, the importance of features, and risk thresholds, as well as predictive models, is therefore feasible using the insights of new evidence. The feedback is also used to learn the incorrect decisions whereby the framework learns to enhance its risk discrimination ability.

3.7 End-to-End Operation of RPAFAI

When a transaction passes across the ingestion layer, this marks the start of the entire processing of RPAFAI. These analytical characteristics are rationalized and transformed to the event and the behavioral, temporal, contextual and graph representations is produced. Such representations are then processed by special AI agents which provide their findings to the coordination mechanism. Real Time Risk Intelligent Layer is next used to utilize the cumulative evidence to yield a dynamic risk score.

Preemptive Decision and Response Layer then decides on what to do based on the perceived risk and the indication of a situation. The decision, which is generated, is the documents which is passed to Feedback and Continuous Learning Layer. This constitutes a continuous sense analysis justification determine respond learn cycle.

Overall RPAFAI proposes an architecture integration into the transformation of traditional fraud detection of a highly reactive classification problem to adaptive, collaborative, real-time and preemptive risk-intelligence undertaking. The framework combines the heterogeneous data on transactions, behavioral and graph intelligence, specialized AI agents, dynamic risk score, proactive intervention and continuous learning and provides a foundation to fight the dynamic and ever elusive financial fraud.

IV. FRAMEWORK EVALUATION

The proposed RPAFAI framework is examined considering different facets with the intention of determining its success in real time detecting financial frauds as well as proactively managing risks. Given the fact that the framework is a compilation of the heterogeneous data processing, behavioral intelligence, graph-based analysis, adaptive agentic reasoning, dynamic risk scoring and automated response, the performance of the framework should have the ability to go beyond the traditional classification accuracy. It is the evaluation that gauges therefore detection-efficiency, real time responsiveness, flexibility, preemptive decision-making ability and resilience in operations.

|ISSN 2349-3216| Volume 8, Issue 5, September-October 2025| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|

DOI: 10.15662/IJAESIT.2025.0805016

4.1 Detection Effectiveness

The initial evaluation dimension is how well RPAFAI was able to tell between fraud and legitimate financial activity. The data classification ability of the framework could be evaluated by traditional metrics such as accuracy, precision, recall, the F1-score, and the area under the receiver operating characteristic curve (AUC-ROC) too. Nonetheless, financial frauds need more than accuracy to be recorded since genuine transaction usually consumes the majority of the records of transactions.

Accuracy and recall of the type of fraud is therefore emphasized in a big way. High recall: The framework can identify a higher percentage of fraudulent transactions, and high precision: The valid transactions will not be identified as such. F1-score is a balanced score which uses both precision and recall. Also, the precision-recall area (AUC-PR) is especially effective to measure the performance especially when there is a large degree of class-imbalance. The multi agent architecture that is proposed is believed to be more effective in the process of detection because the transaction-level, behavioral, temporal and relational evidence are integrated together when compared to utilizing a single feature representation

4.2 Real-Time Processing and Latency

Real-time operations are the key feature of RPAFAI since early-fraud identification could diminish the efficacy of preventive measures. Framework evaluation need not then be done prior to data ingestion except to measure the time the system takes to process an incoming transaction, starting with risk assessment and culminating with decision generation.

Most crucial are the average processing latency, median latency, the 95 th and 99 th percentile latency, transaction throughput and decision-response time. Such measurements can be measured at varying loads in a transaction, to find out whether the architecture can be predictable in terms of its response time concerning normal and peak operating conditions.

Also analyzed should be the computational complexity of two or more working collaborators. Though agentic thinking offers a reasonably coarse contextualization, it is possible to add delay with over-communication, or processing in series. As a result, RPAFAI ought to prefer executing specialized agents in parallel as much as it can, and then, to consolidate decision-making processes using the decision-coordination mechanism.

4.3 Adaptive Fraud Detection Capability

An alteration of the methods of attacks and alteration of legitimate customer behaviour are typical of financial fraud. The fact that it is such a good framework ought to imply that it should be in place to make it detected in a new dispersion of underlying transactions. RPAFAI meets this need by its Feedback and Continuous Learning Layer.

Adaptability A model that is adaptable can be quantified by measuring it through the aid of time validation, where past periods of transactions, train the models, and the current periods are tested. The experiments may also lead to concept drift, or new patterns of perpetrating fraud, or entirely new behaviour attributes not previously observed. The resultant before and after adaptation can then be compared.

The analysis needs to know the extent to which the framework reacts to new feedback to alter its behavioral representations, risk level and agent level choices. The adaptative system should be robust to replicate its detection power without necessarily re-educating the system whenever there is a transaction behavior change.

4.4 Preemptive Decision-Making Capability

The main value added that has been achieved by RPAFAI is focusing on averting the fraud (preempting it) and not merely detecting the fraud as it occurs. The skill can be tested by; how effective the framework is in identifying signs of risk at an initial stage in a series of fraud transactions.

The indicators of the evaluation can be the early detection rate, time-to-detection, high-risk transactions prevented, intervention rate and the false intervention rate. Another method that can be adopted is sequence analysis to examine transactions to determine whether the structure detects suspicious transaction prior to the pattern of fraud evolving.

There are several types of answers that can be used in the analysis of the decision mechanism i.e. approval, further verification, temporary hold, escalation and blocking. It allows the risk-related responses of the framework to be developed, and not based on the judgment about all the suspicious activity being binary.

|ISSN 2349-3216| Volume 8, Issue 5, September-October 2025| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|

DOI: 10.15662/IJAESIT.2025.0805016

4.5 Ablation and Component-Level Evaluation

The input of every RPAFAI part is determined, via an ablation analysis. It can be likened by the entire structure to successively less intricate set-ups, e.g. a model with no behavioral intelligence, with no graphs, with no agents, with no re learning, with no preemptive decision level.

To achieve this, one possible way that would come to mind is how the Graph Intelligence Agent can be turned off in order to visualize what the relational information has informed and Behavioral Analysis Agent can be turned off in order to visualize what has been informed in the historical behavioral deviations. Similarly in the same note the same issue can be compared with that of static risk scoring and dynamically risk scoring to gauge the worth of ongoing feedbacks.

This discussion has pinpointed that the performance improvements have been made possible due to the integrated architecture and not a single aspect of the analysis.

4.6 Operational Robustness and False-Positive Control

The financial fraud detection systems must be reasonable between reduction of fraud and customer experience. False positives being high could result in valid transactions being rejected or over-verified. The false-positive rate, false-negative rate, legitimate transaction approval rate, and intervention frequency must thus be used to evaluate RPAFAI.

Stress level testing can then be done again to examine the behaviour of the system under high transaction volume, absence of full-context information, the delay in agent communication and sudden change in the level of the fraud. The structure must be risk decision-making stable and must graciously degrade in the unavailability of the individual analytical components at the moment.

Detailed description of the methodology used shows that RPAFAI can not be viewed solely as an agent of fraud classifier but a complete end-to-end adaptive risk-intelligence system. Its performance depends on the sum of the abilities to spot fraud categorically, execute deals with minimal slack time, modify according to changing behaviour, spot risk on its initial stage, arrange professional shrewdness and start proportional preventive action.

V. CONCLUSION AND FUTURE WORK

5.1 Conclusion

This paper presented Real-Time Preemptive Fraud Detection using Adaptive Agentic AI (RPAFAI) which is a combination model that aims to overcome shortcomings of traditional financial fraud detection systems. RPAFAI revolves around a single architecture, integrating real-time transaction processing, behavioral intelligence, graph-based contextual analysis, adaptive agentic reasoning, dynamic risk assessment and preemptive response as opposed to traditional methods, which are largely based on independent machine-learned models or acting on fixed, and often ad hoc rules. In this structure, there will be trained AI agents to research on the qualities of transactions, deviation, time system, relations and situation system, that can serve it to present its transaction threat appraisal in a more comprehensive manner.

The recommended architecture offers a sense analyse reason decide respond cycle everlasting sense analyse learn cycle. Generally, the dynamic risk scoring capability of the system also allows it not to be an infrastructure of a binary fraud detection system anymore because any accessible sources of evidence can be used to be employed by the system and the preemptive decision layer can respond proportionally to take action that may include either: authorizing, continuing to investigate, hold on, or completely block. Moreover, the feedback and the continuous learning mechanism offers the basis of changing the fraud patterns and concept drift adaptation. The framework thus refocuses fraud detection towards more of a reactive process toward real-time, ad hoc, collaborative and proactive financial risk intelligence.

5.2 Future Work

The following research studies will focus on implementation and empirical testing of RPAFAI to large, realworld, data on financial transactions, and to realworld streaming platforms. The traditional machine learning method, the deep-learning method, the graph-based method and the ensemble fraud detection approach will be compared to each other in an attempt to quantify the improvement in their precision, recall, F1-score, AUC-PR, latency, throughput and the likelihood of detecting the fraud at an early stage.

Further research will focus on reinforcement learning where an elaborate agent coordinating schemes is used to allow the agents to optimize dynamically their analytical policies and strategies to counteract. Privacy-saving methods, such

|ISSN 2349-3216| Volume 8, Issue 5, September-October 2025| Bimonthly, Peer Reviewed and Scholarly Indexed Journal|
DOI: 10.15662/IJAESIT.2025.0805016

as federated learning can also be proposed to enable support of collaborative fraud-detection without necessarily share sensitive financial data. The solutions of explainable AI mechanisms will be explored in order to provide understandable answers to the risk score and automated interventions. Lastly, we will optimize our scalability, computing performance, resilience, adversarial robustness, and compatibility with banking and payment networks, and investigate these with large-scale deployment experiments. RPAFAI can be extended with these and become a more viable backbone to the future smart and transforming financial fraud detection systems.

REFERENCES

[1] G. Tong *et al.*, "Financial transaction fraud detector based on imbalance learning and graph neural network," *Applied Soft Computing*, 2023.
[2] Y. Liu *et al.*, "Improving fraud detection via hierarchical attention-based graph neural network," *Journal of Information Security and Applications*, 2023.
[3] C. Zhao *et al.*, "Advancing financial fraud detection: Self-attention generative adversarial networks for precise and effective identification," *Finance Research Letters*, 2024.
[4] A. A. Amponsah *et al.*, "A novel fraud detection and prevention method for healthcare claim processing using machine learning and blockchain technology," *Decision Analytics Journal*, 2022.
[5] A. Ali *et al.*, "Financial fraud detection based on machine learning: A systematic literature review," *Applied Sciences*, 2022.
[6] Y. Dou *et al.*, "Enhancing graph neural network-based fraud detectors against camouflaged fraudsters," 2020.
[7] Y. Ding, Q. Yao, H. Zhao, and T. Zhang, "DiffMG: Differentiable meta graph search for heterogeneous graph neural networks," 2021.
[8] Y. Fang *et al.*, "Metagraph-based learning on heterogeneous graphs," *IEEE Transactions on Knowledge and Data Engineering*, 2019.
[9] J. Zhou *et al.*, "Graph neural networks: A review of methods and applications," *AI Open*, 2020.
[10] T. Elsken, J.-H. Metzen, and F. Hutter, "Neural architecture search: A survey," *Journal of Machine Learning Research*, vol. 20, pp. 1–21, 2019.
[11] S. Bhattacharyya *et al.*, "Data mining for credit card fraud: A comparative study," *Decision Support Systems*, 2011.
[12] K. G. Al-Hashedi and P. Magalingam, "Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019," *Computer Science Review*, vol. 40, Art. no. 100402, 2021.
[13] W. Hilal, S. A. Gadsden, and J. Yawney, "Financial fraud: A review of anomaly detection techniques and recent advances," *Expert Systems with Applications*, vol. 193, Art. no. 116429, 2022.
[14] M. Ali *et al.*, "Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review," *Applied Sciences*, vol. 12, no. 19, Art. no. 9637, 2022.
[15] L. H. Aros *et al.*, "Financial fraud detection through the application of machine learning techniques: A literature review," *Humanities and Social Sciences Communications*, vol. 11, Art. no. 1130, 2024.