MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1317-1339

AI-Powered Risk Scoring and Fraud Detection Frameworks in Real-Time Payment Processing Systems

Jai Kiran Reddy Burugulla, Senior Engineer, ORCID ID : 0009-0002-4189-025X

Abstract

The increasing adoption of electronic payments has given rise to new opportunities for fraudsters, posing significant challenges for the financial service industry. In this context, innovative countermeasures are essential to address their criminal activities. Card-not-present (CNP) payments, such as Internet payments or payments made over the phone, are characterized by a higher percentage of fraud attempts and a higher average number of fraud attempts per person [1]. Consequently, automatic systems are needed to analyze previous transactions and detect those transactions that deviate from the standard behavior of the user within a limited time. These systems are often designed to identify fraud by taking into account fraud behavior in a global view. However, schemes that prohibit certain numbers of transactions in a specific time window and analyze transactions directly without any consideration of the user account performance have been proposed.

Service providers commonly resort to the conventional monitoring approach: examining transaction history stored in a database and analyzing them at given time intervals to identify fraud. This approach can potentially reveal several suspicious transactions, however, it is mostly incapable of combating fraud in real-time, leaving a significant gap for other monitoring schemes. As smart devices facilitate the issuing of new accounts, attackers persevere in contributing to their wallets to avoid being investigated. Statistical analysis of earlier input transactions generally misses fraud on newly issued accounts. A case study reports a fraud scenario on user accounts having an acceptable immediate requirement for a non-negligible period of time. With the rapid assessment of the needs on different dimensions, systematic approaches for fraud detection for mass transactions have not been developed yet.

Fraud detection schemes are frequently implemented as rule-based approaches, which determine the legitimacy of the transaction based on various signatures, either pre-defined or self-learned. Some heuristic rules, however, can easily be evaded by fraudsters. Rules that analyze an immense number of aspects nevertheless may go beyond acceptable fluctuations and produce false alarms. These issues adversely affect the performance of a transaction processing system, and scalable fraud input detection instructions demand advanced monitoring systems. Real-time speeds of input processing provide a better opportunity for fraud detection schemes to reduce the probability of incorrect transactions in the batch queue while retaining significant growth in commercial success.

Keywords: AI, Machine Learning, Risk Scoring, Fraud Detection, Real-Time Processing, Anomaly Detection, Behavioral Analytics, Transaction Monitoring, Neural Networks, Predictive Modeling, Data Mining, Pattern Recognition, KYC (Know Your Customer), AML (Anti-Money Laundering), Identity Verification, Adaptive Algorithms, False Positive Reduction, Decision Engines, Blockchain Integration, Cybersecurity, Real-Time Alerts, Payment Gateways, API Integration, Model Training, Feature Engineering, Rule-Based Systems, Deep Learning, Graph Analytics, Fraud Scoring Models, Payment Fraud Prevention

1. Introduction

The increasing adoption of electronic payments is opening new perspectives to fraudsters, which incentivizes the design and development of innovative countermeasures to their criminal activities [2]. By its nature, online payment transactions have to be processed in a short time and often in an automated manner without any human intervention. Consequently, the need for automatic systems able to detect frauds from historical data became extremely pressing. This novel demand on the one hand led to a research stream on the design of intelligent and automated systems based on the use of machine learning algorithms for fraud detection in payment card transactions. On the other hand, it ignited several questions that the fraud prevention systems have to cope with: how to deal with vast amounts of transactions? how to prevent the fraudulent ones before losing any transaction? how to cope with the growing tail of new attacks? and how to feed prevention systems with automatic and intelligent engines that could learn continuously about novel attack payloads? These questions are addressed by a wide range of research works. They promote a variety of system architectures and approaches including approaches based on prediction models, graph analysis, resilience analysis, social network analysis, and many others. Among

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1317-1339

these, supervised methods that, via statistically assessing the payment requests, determine the ones that have to be considered "risky," are receiving a growing attention [3].

The credit card transaction systems considered in this work represent a scenario for supervised opinion prediction where the task is to assign to a transaction a prediction of fraud. Feedback on the true label of predictions, i.e., the actual ground-truth value of the considered transaction, becomes available only after human investigators contact the card holders. However, this feedback is shared between different payment card systems. Theoretical and practical implications for this scenario are discussed. Recognizing that nowadays, big players rely on solutions that are based on collaborative methods is not new. On the contrary, the approach proposed is original in the sense that it focuses on a supervised design to be able to boost the prediction performance and quality of a fraud detection system. Because the dominant technologies used today are supervised methods, it is intended to "steal" the design knowledge hosted at a set of peer nodes that deploy fraud detection systems. The first proposed solution is based on the trust-reputation notion, aiming at infusing the system with the estimation of fraud risk for all the transactions processed by peers. The trust-reputation system estimates the quality of the feedback and estimates a reputation score that is used to process the inflow of knowledge by weighting the impact of feedback coming from trusted peers.

2. Background

The expansion of electronic commerce and increasing customer confidence in electronic payments make fraud detection a critical factor. Several sectors are affected, such as banks and financial institutions, e-commerce companies, insurance and mortgage agencies, and online games. Fraud is the false representation of fidelity or authenticity to get compensation from a legitimate agency [2]. In particular, credit card fraud causes losses estimated in billions of dollars each year for issuers, merchants, and cardholders, and affects consumer confidence in e-commerce. In this field, card-not-present transactions are particularly fragile, because fraudsters can access card numbers, validity dates, and security codes easy in anonymity ways.

To process JD transactions per second, the payment processing system requires special architecture choices to handle a huge amount of transactions in parallel, make all parts of the system horizontally scalable in an elastic way, store and query semi-structured and non-structured data on a multi-terabyte scale, and be autonomous and self-organizing regarding to infrastructure and technology updates without deterred the system activity. For this purpose, cloud services were chosen, and for data storage and computing those services were based on open OS, open frameworks, and languages. Literature presents several examples for connection-oriented systems, data-intensive systems, data-mining, data-shipped systems, and Big Data systems. In these solutions, systems are either not customizable as a whole or reside in a single warehouse of computers which collects all processing servers and redundant data but not horizontally scalable on a distributed architecture.

Recent advances in streaming platforms and machine learning techniques open new perspectives in real-time fraud detection using Big Data tools for massive amounts of data storage and processing. The amount of transactions, which are modeled via non-linear regression on slides of fixed time intervals, is used to detect in real-time unusual spikes. The risk scores of transactions are computed using either supervised learning techniques or outlier detection algorithms relying on the local neighborhood of each transaction.

Eqn.1: Risk Scoring Function

$$\text{Risk Score} = f(\mathbf{x}) = \sigma(\mathbf{w}^T\mathbf{x} + b)$$

- $\mathbf{x} \in \mathbb{R}^n$: Feature vector (e.g., amount, location, IP, device ID)
- $\mathbf{w} \in \mathbb{R}^n$: Model weights
- b: Bias term
- $\sigma(z) = \frac{1}{1+e^{-z}}$: Sigmoid activation (maps score to [0,1])

2.1. Overview of Payment Processing Systems

The automated processing by an online payment processing system consists of a continuous, periodic and synchronous cycle with a typical duration of a few seconds. This cycle concatenates the four following sectors of processing: reception of the card transaction from the e-commerce website, authorization request sent to the issuing bank via the payment processor network, clearing request sent to the issuing bank via the payment processor network and receipt to the e-commerce website [2].

An automated analysis (the risk scoring) is performed as soon as the transaction is received from the e-commerce website. A transaction with an acceptable score is authorized and sent to the issuing bank. A transaction with an unacceptable risk score is rejected. Thereby, it is critical that the risk scoring is correct, since an incorrect score means the loss of a valid transaction (the revenue for the e-commerce website) or unnecessarily rejecting a fraud transaction (the loss for the bank). For these reasons, the automated analysis must integrate the application of the business rules and a

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1317-1339

machine learning model (or several models). In addition, when the risk scoring is complete, the consumer is notified of successful or unsuccessful processing in the web browser. The automated risk scoring resulting in strict time constraints and a latency of two seconds has a significant impact on the design of a scalable and efficient framework for the real-time payment processing system.

The automated rejection of a transaction with an unacceptable score must occur before sending the authorization request to prevent blocking a transaction by a payment processor which cannot be reverted. As soon as the authorization request is sent, the risk scoring cannot be completed within the time constraints. Since the subsequent processing sectors do not require the automated risk scoring results, the automated risk scoring must be performed in time. However, these sectors do have placement opportunities outside of the authorization interval and can tolerate smaller latencies. The time constraints can be relaxed in those sectors (e.g., one minute for the clearing process). However, both authorized transactions and cleared transactions must be analyzed due to compliance and liability reasons. Therefore, the design of the framework must have the ability to support different types of risk scoring approaches (i.e., real-time and near real-time) based on the timing constraints of each sector (or their placement).

Fig : 1 Real-Time Fraud Detection for Payments

2.2. Fraud in Payment Systems

As the e-commerce industry expands rapidly, payment fraud has become imminent. On the glitzy surface of the Internet lies the dark world of electronic crimes, a heterogeneous, ever-changing surrogate of conventional organized crime. Fraudsters send uninvited messages disguised as legitimate, yet unauthorized, emails to fish for account passwords and build their own online stores, on which users' stolen credit card information is claimed to be sold cheaply. Some fraudsters fell victim to the scheme and are untrustworthy in the eyes of merchants. Without adequate anti-fraud control, transactions are consented to be fulfilled and eventually lead to financial losses from the legitimate vendors' perspectives. Payment networks intermediarily provide payment solutions. However, fraud detection and transaction risk control is the responsibility of merchants, leading to a strong demand for effective fraud detection.

There are a great variety of schemes in online transactional payment systems. Each scheme serves for the requirement of product characteristics, transaction patterns, and regulatory compliance, as well as the extent of fraud control and latency in transactions. However, all schemes share the common characteristics of an earlier authorization stage routing transaction requests asking for the vendor's consent and fulfillment guaranteed by the system. On the authorization route of authorized transactions, once a merchant opts to intervene, a dual-stage control mechanism for fraud detection operates. In the first place, screening input transaction data is a risk scoring engine to compute numerical indices between zero and one, called the risk score. Considerable attributes, in dozens or hundreds, are queried. If the computed risk score is higher than the predetermined score-cut threshold, then rejection control is activated; otherwise, the transaction is approved. In case of rejection, in some schemes, the customer receives an automated feedback. The vendor obtains a justification feedback only when either the applicant is identified as a fraudster or the consideration of satisfied risk control is initiated after numerous premature rejections for legitimate transactions.

2.3. Importance of Real-Time Processing

The advent of e-commerce and technological upgrades in point of sale (PoS) and ATM systems, as well as mobile payments, has dramatically changed the landscape of banking systems. Consumers are shifting from cash to card payments at an unprecedented rate. This exponential growth in the use of card payments is accompanied by an increase in the number of fraudulent transactions, making fraud detection the focal challenge of these firms [2]. Fraudsters are getting motivated and using advanced technologies that require proactive detection of fraudulent transactions in real time rather than in batch. Yesterday's detected fraudulent transactions can be today's valid transactions for the same consumer. To stay ahead of this arms race, financial institutions must be flexible enough to adapt the detection capabilities of their system.

A 20% annual growth in transaction volume, reaching around 400 billion card transactions expected in 2022, means dozens of billions of transactions which need to be processed and analyzed to derive some fraudulent transactions. More than, fraud detection algorithms that were believed and widely used have given way to new complex

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1317-1339

algorithms based on machine learning because of the reduced real time nature of frauds. Fraud detection in real time has become more challenging and deserves a detailed review to lay down the future research agenda. Financial institutions have to invest huge resources to build a proper data infrastructure capable of real time processing, storage, and advanced analytics of enormous streams of data. The dynamics of real time processing is unknown and thus data management techniques are still under construction. Complexity is introduced by the trade-off between accuracy and model complexity thus data asymmetry. Most of the supervisory methods are expensive and hard to reproduce in practice.

There have been significant advancements in payment processing technology leading to more straightforward payment mechanisms, such as payment processing events occurring in real time instead of one hour batch wise. Considering a bursty pattern of transaction arrivals, transaction value, and associated costs of doing both, price negotiations between banks, merchants, and e-commerce platforms, it costs many millions of dollars a day for a financial institution to drop even 5% of transactions.

3. AI and Machine Learning in Fraud Detection

Fraud and risk scoring schemes have been proposed for traditional commerce such as online banking and credit card transaction processing for quite some time now. These schemes make use of classical method based AI models such as Support Vector Machines, AdaBoost, and Decision Trees. However, as the world moves towards faster payment processing systems in real-time for purchases made online on e-commerce sites or using smart phones, the traditional AI models have a major drawback in terms of processing new transactions and developing risk scoring in real-time. For traditional E-commerce based payment processing systems which take a couple of hours for every transaction, AI based fraud and risk scoring systems can afford to use classical voting based AI models such as Randomized Decision Trees or SVM classifiers. However these models are batch classifiers and list risk scoring based on the trained model. It is not possible to train and update the model for adapting the learnt knowledge with the incoming new transactions. Processing incoming transactions using classical models based on certain combination of votes is not possible. Hence an alternate approach has been devised where risk scoring and fraud detection together are developed to ensure that the task of fraud detection can also help provide risk scoring, which otherwise needs an individual model [2].

The problem of risk scoring by credit card companies that use credit card and online banking transactions to provide purchase payment solutions for customers is explored. Framing a solution for a different aspect of the problem statement and use case is easier with research being done in the context of the problem statement. The use case could be framed in a more generalized way, thereby with instant payments on MERCHANT-COUPON emergence of PURCHASE TRANSFER-TO-REFUNDING real time payment processing for digital assets and cryptocurrency ledgers has entered the fray of newer transaction types. This provides an opportunity to create a holistic rick scoring and fraud detection framework for this case along with aiding in intelligent decision making.

3.1. Machine Learning Techniques

Machine Learning (ML) techniques play an important role in the proposed framework for Real-Time Payments. These techniques can help detect fraud in payments, money transfers, and bank transactions in Real-Time Settlement Systems. ML's algorithms are widely used for classification problems in various domains. The below sections describe how the well-known ML techniques are used to detect fraud.

Logistic Regression: Logistic regression is one of the basic classification techniques commonly used for fraud detection. If the value of the independent feature is very high or very low the odds of making an approval will skew in total runtime prediction or payment fraud detection. It can understand the behavior of patterns for approval of transactions.

Random Forest: Random Forest is one of the techniques in the ensemble-based approach or the Bagging algorithm. It uses decision-tree classifiers as base classifiers and trains them using random subsets of the training sample. This technique is considered more effective, efficient, and versatile. Each tree is used to estimate the target function, and it will take decision votes.

Decision Trees: It is one of the most used techniques in various classification problems. It is simple to implement without many computations or parameters. It is a flow chart-like structure for making decisions. The internal nodes in the flowchart represent the attributes and the branches are the outcomes. Whereas, the leaf nodes represent class labels.

Extreme Gradient Boosting: Extreme Gradient Boosting is a popular boosting technique. In this approach, regression trees are added one after another, and at each step, a regression tree is fitted on the pseudo-residual for previously fitted trees. It is a powerful, scalable, and efficient

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1317-1339

implementation of the GBM. It accounts for missing values on each feature automatically and deals with outliers effectively.

AdaBoost: AdaBoost is one of the first boosting-based algorithms that uses a combination of decision tree classifiers as weak classifiers. It assigns weights to all training instances and increases the weight of the misclassified samples while decreasing that of the correctly classified ones. This approach is very robust against overfitting the training data but has some difficulty with noisy data.

3.2. AI Algorithms for Risk Scoring

Processing systems for real-time payments have been transformed by ambitious technological advancements that embrace open systems, standard data models, approaches to distributed developments, and non-invasive integration methods. New systems architecture involving multiple processors, application servers, an enterprise service bus, and streams/flows for data transport calls for a suitable framework for evaluation, monitoring, and adjustment of user-defined scores for the PRA (Proactive Risk Assessment) processor. An example of a risk scoring-based PRA processor capable of handling reconfiguration of inspection scores in a real-time payment processing system is outlined [1]. The processor is introduced via an end-to-end process architecture example, which also relates to the architectural area of enterprise services, structures, PICALC, pricing, risks, limits control, and customer statements. In-depth discussions of the handling of important particulars like the monitoring of fraud possibilities via transaction analytics, outbursts monitoring via statistical checks, risks nearing their prescribed maximum values via counterparty exposures, and overall limits to be kept below a user-defined maximum value are offered.

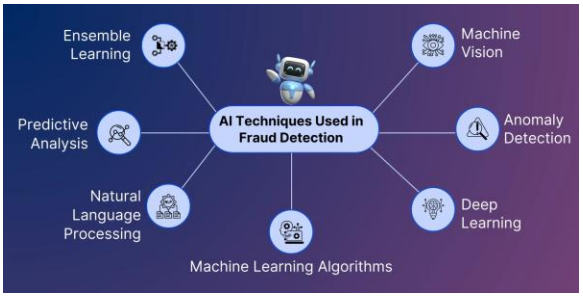

Fig : 2 AI/ML Improve Fraud Detection Accuracy

Cost-efficient real-time fraud detection could be performed using general-purpose graphics processing units (GPGPUs) with early technical adopters reaping savings estimated in tens of millions of dollars annually. However, the speedup of parallelization depends on the architecture and implementation describing the underlying computing units. For the greatest potential speedup of the massive parallel structure, up to 163,000 threads/cores, each thread should execute fewer and restricted types of operations with the fastest options (comparisons, additions) being preferred. Flexible and miss fitting options along with memory access patterns in conflict with GPU efficiency would inhibit massively parallel operations. Hence, GPGPU implementation of a fraud detection algorithm has to abide by a number of limitations to provide enough speedup:

1. Maximal execution of operations should be performed using a well-established calling structure.

2. The number of loop operations should be set to free application memory.

3. Operands should be transferred to on-board computations lattices only when really necessary, avoiding as much as possible memory copies.

4. GPGPUs should be efficiently used to process high velocity events, at least on the orders of 10^5/s.

5. Event structures should be fixed with little change probability.

6. Redundant computations/materializations should be avoided as much as possible.

7. Knowledge should be expressed in machine learning algorithms with the lowest possible complexity.

3.3. Data Sources for AI Models

There are several common approaches to modeling the data sources to be used in the AI algorithm: Tabular data table, Graph-based transaction modelling, and Generalization of complex data.

Commonly used is the tabular data model, where data is stored in tables where rows and columns represent entities and their properties. The data are often fetched in a relational context and thus making transaction analysis according to entity relations easy. A commonly applied data model stems from electronic payments and in particular bank 거래기록. Here, transactions are described by the covered attributes: transaction id (TID),

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1317-1339

transaction label (T), source account (S), target account (D), time stamp (T), monetary value (V), and transaction type (Type). Using a graph−viewing option based on these attributes reveals sophisticated schemes of money laundering cross banks [3].

When investigating anti-money laundering transactions, it proved inefficient to just maintain the single randomness of source accounts. The neglect of networked relationships of bank accounts in confrontation with anti-money laundering makes the problem more complex and generalization is desired. As a transaction model, this work focused on a directed multigraph viewing option to highlight parties by the combinations of account entities. The generated generalization metrics span across arbitrary parties consisting of nodes involved in the transactions as sources or destinations. Transaction nodes and configuration entities are mapped to real-world entities, acting as intermediates between transaction and network graph viewing options.

Eqn.2: Fraud Probability Using Logistic Regression

$$P(\text{fraud} \mid \mathbf{x}) = \frac{1}{1 + e^{-(\mathbf{w}^T \mathbf{x} + b)}}$$

Where θ is a tunable threshold (e.g., 0.8).

The reason for bending the emphasis of transaction modelling to graph-based network representation is the complexity and generality of the models. In hierarchical tree presentations only simple sequences are manually isolated, but relationships have not really been maintained through appropriate representations. This leaves the labour-intensive node modelling with a usability struggle for normal people who are unaware of their importance. Also, the evolving tree representations are complicated to a range of hundreds of square root computations when trying to scale their usability to real-world node data.

4. Framework Design

In this section, a framework utilizing Adaboost as the core architecture is designed, which is described in detail from its constitution and its implementation aspects within real-time payment processing systems.

4.1. Framework Design

The architecture of the proposed framework consists of a risk scoring engine and a fraud detection engine. For each new payment transaction, the value and content of its attributes provided by the payment processing system can be arranged and formatted into a data record denoted as x. The vector x consists of N features whose types include numerical and categorical. A flexible feature engineering unit transforms the input x into k-wise default feature combinations, denoted as C = { c1, …, ck }. Each feature combination ci is a vector representation of d-length default features. Together with their feature values, the corresponding security information objection (SIO) requesting to risk score of these features combinations is generated. The SIOs are then processed by the risk scoring engine to output real/risk scores. They represent the risk level of the transaction. This risk information is then sent back to the payment processing system. If the risk score of a transaction is higher than a pre-specified threshold denoted as THR, this transaction will be rejected. Otherwise, it will be sent to the fraud detection engine for secondary checks. To service SIO for fraud detection, the transaction in question needs to be represented differently. The following information needs to be reported: (1) its risk score; (2) the risk scoring results of the other feature combinations deemed as non-fraudulent; and (3) the log info of this transaction generated within the processing systems. Therefore, the scenario of fraud detection can be viewed as a non-standard two-class classification problem where (i) the verification transaction in question with S* = 1 and (ii) many benign transactions with S* = 0 need to be classified.

4.2. Fraud Detection Engine

The procedure of this engine involves three important components. When a SIO is received, two important tasks need to be accomplished: (1) transform the SIO into a verification instance and the corresponding fraudulent examples, and (2) call the fraud detection mechanism. The first component is responsible for accomplishing the first task. When a newly arrived SIO is received, its content is parsed first. The risk score r of the feature combinations that triggered the suspicion is first stored as an additional feature. The queries are constructed towards the storage of risk scores of the other benign transactions (marked as approved). In this way, the plausible normal samples are retrieved. Additionally, the feature value of the verification transaction and its features combinations are needed to be fetched for joining with the benign transaction in question. After that, the transformation is conducted. The original feature types of the verified transaction are known to the model, while those new from benign transactions are unknown. Hence the meta-info of the features, including the corresponding ID, type, and range of these new features, needs to be packed together and sent along with the verification transaction.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1317-1339

4.1. Architecture of the Framework

The total amount of payments processed by businesses each day is typically huge and continues to grow daily across the globe. With the rising utilization of electronic payment systems by electronic wallets, websites, and at Point of Sale (POS) terminals, new avenues for fraudulent acts are becoming available to fraudsters. Additionally, it is becoming common knowledge that innovations in new payment methods or new technical channels always involve their own set of new types of cybercrimes. Fraudsters have been targeting vulnerable systems of organizations to get an edge and thus optimize their fraud schemes [2]. Automated solutions are needed to detect fraud and apply contingency plans to minimize losses. There is hence a need for systems that are able to detect fraud as such transactions occur.

In this work, new instances of a fraud detection system, which is scalable, accurate, and able to provide low-latency alerts, have been designed as a real-time streaming implementation of a fraud detection framework. Two unique AI-Powered Risk Scoring and Fraud Detection Frameworks for detecting fraudulent payments using historical transaction data have been proposed. Even though these fraud detection systems are based on distinct technologies, they share the same internal design for the processing of the streaming data. The internal design of the fraud detection systems has been detailed, along with the streaming and batch processing used. Some examples and use cases of these systems for a fictional doughnut brand and a gambling outlet have also been covered.

The systems presented in this work can be used as standalone solutions and help minimize fraud and aid organizations to reach a better state of maturity in terms of information security. They represent state-of-the-art systems since they are able to deal with the screening of all transactions near real-time, the batch processing of historical data, and the building, fine-tuning, and retraining of AI models. The batch processing engine is debatable, though, since there are use cases where it would be preferred not to have the batch processing in a separate system. It is additional infrastructure to maintain, which can lead to increased operation costs.

4.2. Integration with Existing Systems

Challenges related to integrating the real-time payment processing and AI-powered risk scoring and fraud detection frameworks with existing payment processing system infrastructure, architecture, core and peripheral systems, and components. The problem description and solution architecture of such frameworks are presented as a general architecture, and the needed contacts with existing systems at the locations of input aggregation and rating, post-processing of the results given in real time by the AI framework, and final fraud blocking at the payment processing and clearing component. Components and systems in both new and existing frameworks that require in-depth analysis and determination of needed development and configuration details are identified. A description of the capabilities and parameters that need to be determined to adjust selected AI-based frameworks at five levels of risk scoring and at least a start identification of a correlated set of methodologies for detection and investigation will be performed for the types of frameworks or engines that will be purchased [2]. In addition, the types of fuzzy and neurocomputing-based approaches and frameworks based on them and the supporting technologies to be investigated as pilot systems will be identified, along with initial grounds for comparative advantages. Together with the integrations mentioned above, an extensive installation and assessment work package for all four frameworks integrated with the real-time payment processing system will be outlined. Acceptance criteria for the functionality and performance assessment will be enumerated, as well as system integration, testing, and simulation strategies needed for completion of the work packages and acceptance criteria. The AI risk scoring and fraud detection frameworks will be extensively assessed also for development, installation, operationalization, and usage in-house and supplementary or alternative systems with similar purposes, but with possible types of general and specific approaches.

4.3. Scalability Considerations

In the Context of the European Union (EU) Payment Service Directive (PSD2), a new standard for authentication was recently adopted: the 3D Secure 2.0 standard. Its dynamics permit the secure exchange of a broad range of notifications, allowing online merchants to both provide more information to issuers and get responses to fraud flags, lowering the friction of legitimate cardholders. In this respect, the platform can — and must — behave as a trust router, gathering the cardholder and merchant behavior, sending as much contextual data as possible, processing utility scores, and re-routing the authorization requests. As the number of daily transactions can reach tens of millions, one of the most critical challenges is scaling the computational processes to handle the real-time requests of hundreds of thousands of merchant partners in the first hours of the system deployment, without sacrificing the detection performance. Gaining much intelligence from real-time data provides a chance of constant improvement for the fraud detection process in dynamic environments such as online payments, which are constantly evolving. For this reason, not only are distributed machine learning (ML) algorithms needed, but also streaming data structures from the very beginning of the framework design. This priority manifests

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1317-1339

interest in real-time decision making, which has a multitude of restrictions imposed on system dynamics and model design due to real-world system constraints. The SCARFF framework addresses the imbalanced distribution of classes, covariance shift over time, periodic and sudden concept drifts, and delayed feedback, all of which arise in the context of an illustrative case study on credit card fraud detection in [2]. The framework integrates open-source Big Data tools with a scalable machine learning approach, and experimental results on a real dataset are reported. This dataset consists of about 125 million credit card transactions collected over two years. Perfectly distributed across a cluster thanks to a proprietary analytics tool chain, the dataset is stored in parquet format, a standard column-oriented file format used by the Apache Arrow project. The training and evaluation of the machine learning models are performed with Apache Spark. The models and decisions are scripted using pyspark.ml, with which a straightforward integration with Apache Kafka is set up for real-time production.

5. Risk Scoring Methodologies

The primary goal of any fraud detection system is to protect the bank/card holder from any fraud attacks. Thus it is highly desirable that whenever a fraud transaction is detected it is stopped right away. In order to do that, existent solutions mostly focus either on highly selective criteria models or actors. This is in fact a very sensible choice, as whenever a model or actor is mis-classifying a fraudulent transaction as non-fraudulent (in short it produces false negatives), it can result in a credit loss for the bank as the transaction moves, so the fraudster can steal the money. Hence the evaluation of such solutions concerns first of all the false negative rates (FNRs). This is also true for one-off fraudulent scanners i.e., Voice or Trends, thus it is possible to model or characterize them for the credit card fraud detection on the basis of FNR rate.

The banks own the credit card transaction flows. However the same flows are also owned by a number of other organisations, even in the absence of sharing the flows bank to bank. A singular mathematic model can be constructed to ask other organisations the distribution of perceived types of transactions with constraints attached to it. With this it is possible to perform damage control on transactions classified as fraudulent by the multiple behaviour-based models/actors. Either the transaction is real then it is very likely that it will be green flagged across a number of actors; or the transaction is a fraud bit then it is very likely that it will be red flagged across a number of actors that are more sensitive to behaviour based clas-sis. For simple rolling average type models that count the number of transactions exceeding some thresholds as well as the number of times each account moves from green to red, these FNRs are easily characterised. It shows how the FNR of a bank increases with its model rate.

In real-time credit card fraud detection, existing models rely on an isolation forest ensemble using centroid scores and a high-yield candidate classification model trained with the filtered data. The authors of this paper use streaming summaries for each of the first-stage models. The time-weighted method minimizes the sum of false positives and running time with a minimum non-exceeding ratio of positive classes. As the trained models, the corresponding ringing and recovery times of each first-stage model also increase with their errors ([2] ; [1]).

5.1. Static vs Dynamic Scoring

Introduction of Risk Scoring and Classification Framework for Real-Time Fraud Detection in Payment Processing Systems. Payment processing systems have two important features: (1) The payment processing framework must be able to work in real-time and have fresh data received from the payment processor continuously and within milliseconds of delay, and (2) The processing model must be able to work with machine learning algorithms that have to work in a real-time manner. In view of these two features of payment processing systems, AI-powered frameworks for risk scoring and detection of fraudulent payments in real-time payment processing systems are proposed. The value of payment transactions is used for scoring the riskiness of payment transactions and fraud detection in real-time payment processing modeling. A time window approach is proposed, which consists of a scoring model and a processing model. Scoring model assigns a risk score from a pre-trained risk scoring model trained using historical payment transactions. Processing model detects frauds using a pre-trained classification model. The time-based sliding window of the payments triggered the scoring and processing models separately. Data for training the models has to be created using persistent records of a payment processor available in a more or less static form, as false records and the value of payments are generally immutable. Off-the-shelf machine learning packages can be used to train the scoring and classification models, with a few appropriate parameters to tune. Finally, the interpretation of the AI-powered models is provided using an explainable AI toolkit. An application and a dashboard for monitoring payment transactions and fraud detection is provided as a complete implementation guide.

Risk Scoring. Payment schemes and credit card brands use several methods for risk scoring, primarily based on the value of payment transactions. Merchants, the recipient of

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1317-1339

payments, including online merchants, can also use risk scoring models. Risk scoring models can assign a risk score ranging from 0 to 100 for a payment transaction, representing how likely a payment transaction is fraudulent. AI is used in scoring models, with input variables processed accordingly.

Risk Scoring Framework. Static models and non-static models can be two major categories of payment transaction risk scoring. Static models use only immutable input variables, while non-static ones can use mutable input variables. One or more input variables of the incoming data can make the risk scoring model dynamic, which can be expensive models to create and may change over time when significant events occur. A static model is proposed to score the riskiness of payment transactions, consisting of a time window approach and a scoring model for event-based risk scoring. In the proposed framework, the risk scoring is good enough as real-time, online fraud detection. The task is to utilize an AI-powered risk scoring model for risk scoring in a real-time payment processing framework.

5.2. Thresholds and Risk Levels

Ideally, the detection mechanisms should be able to avoid executing any frauds while not affecting true transactions. Due to divergences in genuine customer behaviours varying from country to country along with the pore data mining representational, the thresholds of risk control are difficult to fabricate. Hence in order to continuously improve and tune the system two cases need to be considered: changing the thresholds of the risk scores or tuning the consumer conditions without refitting and adding the perplexity. Conceivably, frequent updates are time and labour mechanics consuming, however, it is suggested that tuning the thresholds of risk control is more inclined to be adopted in practice because it varies gradually with the transaction volume change. Utilising such a threshold tuning approach, the delicately balanced control plots could be achieved under different UTC or transaction volume, which enhances the flexibility to enhance the case where too many false alerts occur [1].

Fig : 3 AI in Risk Management

With the growing usage of payment technologies and environmental factors, together with the changes in the on-line transactions volume and customer behaviours, generally speaking, in order to securely detect the frugs it is rather considered to attempt tuning the risk control levels or thresholds instead of changing the product features or deploy new models. Therefore in this study, the risk thresholds are examined against extreme transaction conditions, with both the tipping point of UTC and transaction volume changes considered. The results suggest the need of caution in threshold setting and attentions should be paid to tunes it beforehand but don't be confined thoroughly. The overall detection accuracy nearly remains unchanged within a very wide range of risk thresholds across UTC ranges, while rather inconsistently changes out of it [2].

5.3. Continuous Learning and Adaptation

Fraud detection in one of the main systems of modern financial infrastructures, real-time payment processing systems, is governed by the prediction of whether a particular transaction is unauthorized from an account's perspective. Models are trained for each account in a bank or payments provider's risk horizon. Continuous model adaptation to keep track of behavioral changes, as well as efficient deployment strategies for large portfolios and federated settings, are paramount. Solutions for model updates, parameters management, and model application in either centralized or decentralized settings are proposed. Lastly, the Stateful Model Task Service properly ties together all components of the online risk score prediction framework and plays a key role in monitoring, security, and observability [3]. The novelty of these ideas lies in the comprehensive set of framework pieces that propose, that jointly tackle all aspects relevant to efficient and scalable risk score prediction; as well as in the advanced processes, storage approaches, and learning algorithms. Flexibility and robustness in the face of unpredicted operating conditions

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1317-1339

was made a priority in order for framework parts to handle the high variability in risks for banking institutions enabling real-valued predictions, confidence estimates, automatic model audits, and on-device architecture options [4]. These considerations set non-conventional constraints over framework components that need to be tightly coupled, inducing a complex design space and research problem. Nevertheless, the framework design is generic and the proposed pieces can be easily interchanged with other ideas stemming from the vast landscape of machine learning research.

6. Fraud Detection Techniques

As a financial institution such as a bank, or a non-bank such as PayPal, clears payments for its merchants, it has to deal with the related fraud risk like elsewhere. Moreover, it has to comply with anti-money laundering regulations, i.e. detect and report suspicious activity of defrauded funds. Traditional risk scoring and fraud detection systems are fed with optimized features at a certain frequency. Once built, these features are not re-optimized, rendering risk scores and detections stale against new strategies. In this paper, an Artificial Intelligence-powered risk scoring and fraud detection framework that dynamically monitors and adjusts features, risk scores and fraud detections is presented. The framework has been implemented on the payment processing system of a major non-bank financial institution. By deploying a feature management module to replace the original batch system and moving features to a micro service platform using Kafka, many risk scoring features are dynamically built in near real-time. Both the design and performance under production load is described. The framework is now in production, and is believed to be the world's first AI-powered dynamic risk scoring and fraud detection framework [2]. Fraud detection is a critical factor in the expansion of electronic commerce. Safety and privacy are serious concerns regarding credit card usage on the Internet due to the rapid growth of online purchasing. Models must be created to detect fraudulent transactions made using compromised credit card credentials over the web. Detecting fraud in real time is a demanding task since transactions with high risk must be filtered out before being authorized, while legitimate ones must be updated as quickly as possible. Traditional models based on batch learning can become obsolete because of time-varying strategies adopted by fraudsters. Therefore, the development of fraud detection systems is needed for card-not-present payments that are capable of incremental learning from new labelled transactions, fast enough to keep pace with incoming data. Such techniques capable of learning from an arbitrary amount of streaming data, classified and unclassified, are scalable, efficient and useful.

6.1. Anomaly Detection

Fraudulent behavior in consumer credit cards accounts for a total of $ 17.8 Billion annually. With the rapid growth of online payments and e-commerce, it is crucial to improve fraud detection and increase user confidence [2]. Real-time fraud detection is vital because fraud prevention tools must assess the risk of online transactions before allowing them to complete. Such predictions increase user confidence in electronic payments and decrease potential losses for vendors and banks. User confidence is addressed with a focus on real-time fraud detection applied to customer credit cards accounts. Fraud detection generally consists of three main tasks: data acquisition and preprocessing, risk scoring, and risk scoring approval or disapproval, also known as blocking. Sophisticated fraud prevention systems already tackle tasks one and three using complex rules and additions. Since fraud is a minority event, the highly erroneous risk scoring output produced by these systems must be complemented with a risk scoring system capable of estimating the risk of a fraud event based on background knowledge, risk capturing, and sufficient tuning. In the banking industry, historical data must be complemented with real-time background data. Banking customers have fixed attributes that remain unchanged, and younger customers typically present larger risk scores and incidence probabilities due to their lack of history. Moreover, new customers may only be able to be risk-scored if sufficient relevant historical data is acquired. Risk-scoring knowledge is knowledge against which the behavior of transactions and customers in the system is monitored. Otherwise risk scoring must be fully data-driven, and risk scoring systems with no background knowledge are also plausible; only the risk scoring has to be monitored to keep predictive capabilities once an acceptable framework is in place. Typically there are well-established static models to fall back to in such cases, and similarly the complementing risk scoring can monitor previously unseen scoring systems at granularity. A solution approach for risk scoring with fraud detection with a rich background is presented.

Eqn.3: Anomaly Detection via Mahalanobis Distance

$$D_M(\mathbf{x}) = \sqrt{(\mathbf{x} - \boldsymbol{\mu})^T \boldsymbol{\Sigma}^{-1} (\mathbf{x} - \boldsymbol{\mu})}$$

- $\boldsymbol{\mu}$: Mean vector of legitimate transactions
- $\boldsymbol{\Sigma}$: Covariance matrix

6.2. Predictive Analytics

Predictive analytics enables organizations to make

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1317-1339

proactive decisions and mitigate potential risks by deploying a combination of data mining, statistics, machine learning, and AI techniques. Specifically, predictive modelling leverages historical data, statistical algorithms, and AI methodologies to identify the likelihood of future outcomes based on data patterns. Over a century of academic research has created modalities and methodological approaches ranging from assumptions of data distributions, algorithms, and interpretation of results that can be applied to risk scoring.

Compared to a conventional statistical approach where each model is built individually, risk scoring approaches build a model for a base event, such as detecting a credit card transaction fraud, and then to apply the model on a new event to obtain the risk score. This is similar to an anomaly detection approach, where the model learns the normal behaviour of a subject and the scores would be higher, the further such observation is from being normal [2]. A risk score is an assessment of the level of risk of a candidate event, typically expressed as a single number (between 0 and 1, 0 and 100, etc.). Generally, there are two simple ways to compute the probability of the base event given the input event features. If the base event is rare in the training set, a likelihood tensor approach is proposed, where for each event, answers to a reputation question are stored jointly in an effectively expanded event feature space. The probability (i.e., risk score) in question is computed by a simple lookup.

For a generalized case where the base event is abundant in data, there are still many machine learning methodologies that can be employed: 1) A risk scoring function w can be built using supervised learning, where takes the input event features and thresholds would return the risk score. 2) A risk scoring model can also be built using unsupervised approaches, based on learning the normal behaviour of the event features and returning the degree to which such behaviour deviates [1].

6.3. Behavioral Analysis

One of the deed integrals of a real-time payment processing system strategy involves behavioral analysis of which action provides value to the system. The former is the data of behavioral events occurring over a certain time window. The time window length is determined after the payment processing system is deployed. The gathered event-based analytics data is first formatted for input inputting into a recurrent neural network (RNN) model ([5]). Given the event-based data, there are several preprocessing steps prior to entering the RNN for analysis. These steps entail domain identification, domain encoding, and state matrix construction, all of which are performed at the event level. Each event consists of a pair of device-encoded action and domain, such as execution time, device, and location. A user behavioral interaction may engage a single or multiple actions with some degrees in the analyzer. In addition, the considerable number of features in input events increases the model complexity to unwieldy levels and makes the model detection performance unstable ([3]). The analysis procedure for encoding and auto construction of the time window-state matrix are provided hereafter.

Each input action is associated with one or more domains. A number of continuous domain quantities, e.g. lengths, limits, amounts, are candidate quantitative domain features and their uniform bins cannot capture the domain knowledge in either penalty or cost computations. Augmented with domain embeddings, each of which is a randomly assigned number of dimensions and is tuned to reduce their error rate in predicting fraudulent accounts, a continuous domain is discretized with a manual threshold for each action event element. For instance, an execution time on a window may vary in a range, over the four thousand ranges encoded in a one-hot integer feature vector. Thus each captured power on continuous and multi-valued features is reduced to in zero or higher.

Each of the behavioral actions is associated with an activity domain in addition to the action being of or on a device and the target that the action is directed. For detection on users who handling normal behavior or committing fraud, the implanted recodings perform a domain-wise event configuration, a global structure gap configuration, and Viterbi decoding.

7. Real-Time Processing Challenges

Real-time payment processing systems face several unique challenges that differ from batch processing systems. Scalability is a challenge common to many modern data systems, including data warehousing and batch processing systems. However, it takes on a different form in the real-time payment processing domain because of the stringent latency requirements. To keep the system performant, every component must be able to scale to the level of the payment. This becomes particularly difficult when employing large analytical models, such as deep learning and large ensembles. To tackle this challenge, ML solutions need to be optimal and light-weight [2].

Another challenge is data availability. Data are only available for the previous 30 days in these systems, which is not very much data when compared to non-time-sensitive domains such as e-commerce. On the contrary, some data are predetermined in real-time payment processing systems,

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1317-1339

such as the amount and the merchant. Therefore, deciding what features to capture and how to feature-engineer them is crucial.

Usability is yet another challenge. In a batch processing system, the bank needs not be concerned with the average latency of model executions. It may very well be that some states take half an hour to process. However, this is unacceptable in a real-time payment processing system. After generating models, extensive experimentation is essential to ensure that the overhead introduced by the model can still be tolerated. Some naive models may flame out in the experimentation stage due to a failure to anticipate the implications of the decisions made to keep latencies manageable.

7.1. Latency Issues

In recent years, the rising prominence of content delivery networks (CDN), luck-based protocols, ad-hoc streaming applications, and massive control storage has brought about new challenges to streaming processing software systems that should meet critical requirements while processing continuous real-time data streams. For example, financial systems process continuous data streams generated by fast trading infrastructures, which calls for low-latency systems that provide real-time agent craziness detection and forecast trading volume and balance prediction at micro basic units of a second. Traditional academic systems used for big diligent streaming tasks cannot meet such latency requirements.

Existing work has made some efforts to tackle microsecond level latency, but is not easy to be applied in various industries. Some solutions are related to avoiding data copy to minimize the processing time, which may highly couple the systems with the source frameworks and is difficult to integrate with existing standalone streaming processing systems. The real-time epsilon-balanced streaming quantiles algorithm, ensuring reporting latency, has been researched to derive accurate quality insights, but does lack of performance adjustment for multi-system usage. Other efforts have focused on developing systems with end-to-end micro second level latency, which requires special designs incompatible with existing open-source systems. Besides, query diversity has also been addressed for some specific jobs, but the tuning profits do not target the latency upper bound, and the issues of outlier patterns in data connection high variability of parallel systems usage have yet remained.

For benchmarks of streaming query performance, price and data volume are addressed, the requirements of speed, complexity, modularity and evaluation metrics based on latency are less considered, which limits their appliance for designing low-latency queries. Existing cost simulation benchmarks on high-speed systems also do not thoroughly examine query performance in microsecond ranges. Performance control for data production framework is studied, but it focuses on local systems dealing with global latency upper bound, which may not provide guidance for multiple streaming systems usage. In addition, thorough quantitative analyses on the performance and run-time characteristics of open-source streaming systems are also lacking, which makes it hard to match queries with suitable systems and parameters.

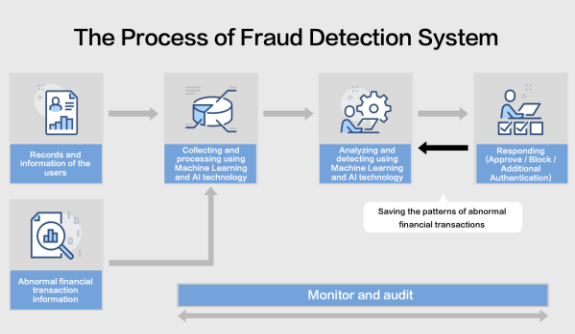

Fig : 4 Fraud Detection System (FDS)

7.2. Data Privacy Concerns

The increasingly widespread usage of online payment systems motivated the development of new ways to efficiently detect fraudulent behaviour in real-time. Understanding the type of fraud or payment risk concerns some aspects and angles: money laundering, false accounts, account hijacking, and, in a broader sense, digital identity fraud. Furthermore, frauds or fraud attempts can differ based on the payment type and therefore involve machines and humans (credit cards fake transactions versus phishing). Analysing fraud attempts or deviations relies on having background data, such as historical records of fraud cases, and detecting anomalies and abnormal behaviour. Fraud frameworks provide a risk score representative of the likelihood of payment and transaction data being fraudulent. For this purpose, several payment information features are analysed, including the amount, timestamps, currency, country, and other contextual information that may vary when payments are made. Fraud frameworks may also analyse transaction balance changes triggered by different activities (i.e. pending payments or account top-ups). Fraud patterns are inherently time-dependent, requiring time series analysis to understand deviations from historical behaviour. Payment and transaction behaviour vary significantly for each user, with each account needing a specific analysis model and protection. Thus, transactional data analysis continues and is integrated into the risk scoring frameworks' machine learning models. The risk scoring frameworks

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1317-1339

output a likelihood of fraud for additional behaviour checks (instead of immediately blocking the transaction). The probability of a payment or transaction being fraudulent is converted to a score between 0 and 100. Transactions with a score under a predefined threshold are deemed high-risk and flagged for manual review [4]. Automatically blocking fraudulent transactions is not ideal due to the high inconvenience and impact on end users. As such, the lower the score, the safer the transaction is deemed. However, post-fraud detection models, such as forensic investigations, customer servicing teams, user journey modelling, or remboursement modelling, can assist in solving frauds after they occur, affecting stakeholder engagement and customer experience.

7.3. Regulatory Compliance

The narrative of artificial intelligence (AI) is becoming more prominent throughout the world. AI may assist firms to innovate more quickly, enhance production efficiency, cut costs, and offer consumers with customized products and services. AI technology is widely utilized in a range of industries, including finance, healthcare, transportation, and energy. AI service can identify banking clients in real time, manage investment trust portfolios, automate medical diagnoses and treatments, develop semi-auto-driving automobiles, and optimize energy output and consumption, among other things. Concerns are raised as a result of the rapid growth of AI technology. There have been a slew of major AI problems. The market turmoil caused more scrutiny of the transparency and accountability of AI-empowered trading models. Instances of bias in hiring, credit, and health care A few large tech corporations' AI concerns have recently turned into front-page news. From a national perspective, technology leaders are establishing and filing AI governance policies to remain ahead of the risk curve. From the perspective of an organization, compliance team leaders and supervisors on business functions are frantically collecting stock and regulatory inner or industry white papers related to AI and other existing regulations in preparation for compliance investigations [6]. AI regulations do not only apply to AI technology at a high level; they also need to govern the model manager and AI architectures within institutions. The increasing complexity of model architectures and integration challenges among data, features, algorithms, and floor variables make compliance modeling and monitoring extremely challenging.

AI governance challenges are a potentially huge research area with numerous white space opportunities. Traditional risk controls are generally static, system-agnostic, group-oriented, and mainly comply ex-ante and ex-post with a reporting cycle from quarterly to annually. Although some important safeguards like control, validation, and transparency purposes are embedded and built into AI thanks to its data-centric and algorithmic nature, their abilities to mitigate compliance risks are still limited [7]. It is imperative that AI systems are capable of satisfying transparency requirements, diagnosing key decision variables, controlling conformant drift, and reporting to risk managers and compliance teams in a timely manner. The existing compliance frameworks are either too general or target too many specialized criteria at once, which often prevents their practical adoption. There are also limited options for real-time monitoring of procedures and models based on continual learning without the risk of information leakage. The abovementioned gambits further highlight the dire need for improved AI governance and combinations of agile architectures and adaptive modeling. However, not much work was done to assess the comprehensiveness and reusability of existing solutions and develop a system and module-level AI governance framework.

8. Case Studies

There is an expressive growth of ATM frauds across the globe using several replicated skimmers. These skimmers replicate the ATM interface and take data on the card, PIN number, and OTP details which along with these data allow the fraudster to perform cash withdrawals from the victim's account. Many automated systems are being used to detect ATM fraud and take appropriate action to mitigate ATM fraud cases. This paper proposes a real-time web-based problem of ATM fraud detection using streaming data analysis by analyzing the financial attributes, Environmental attributes, and ATM user attributes. The executive summary is also provided to malpractice scheme in place for ATM. Literature survey proposed classical approaches for ATM fraud detection and artificial intelligence approaches in a similar domain are presented. Streaming data mining techniques and their various algorithms for detecting ATM fraud cases are also proposed. This paper describes the mathematical modeling, methodology, and overall architecture of ATM fraud detection framework in detail [1]. Under the increasing adoption of electronic payments and new perspectives for fraudsters, there is a need for innovative countermeasures against criminal activities. To this end, many financial institutions have entered the fraud science circle of service providers, foreseeing academic and private research to design innovative and effective fraud detection systems to follow. Fraud detection systems must properly deal with the specific issues arising from fraud transaction classification in order to assist human intervention, including (i) massive size of the data (volume); (ii) high-dimensional and noisy feature space (variety); (iii) requirements for real-time application (velocity); (iv)

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1317-1339

multiple non-stationary data distribution (drift); and (v) incomplete ancillary data (veracity). As a result, effective fraud detection systems should be (i) accurate; (ii) robust and flexible; (iii) scalable and efficient; and (iv) fast in real-time operation [2].

8.1. Successful Implementations

Dealing with money and most of the product selling (like groceries) are done through credit cards in apartments by having an ATM in the apartment, which led to ATM fraud. Therefore, knowing about ATM fraud detection becomes a must in this new era of money transaction [1]. Now-a-days, important data is coming in real-time, and it is expected to get processed in real-time. With the increasing number of transactions, the need for the banking sector is also increasing for various reasons. One such important reason is the fraud detection. Fraud can occur in various places, like telecommunication, insurance, loans, and credit cards. It must be detected as soon as it happens to protect the consumer's monetary assets.

Real-Time Credit Card Fraud Detection System is a system that detects frauds during online shopping instantaneously. Data streams with a value of 0.68 Gb are used, that model the credit card transactions in Lisbon in real-time resembling 9 and representing the non-fraudulent transactions, with a percentage of 0.0024 and no information about the transactions that should not be permitted. SCARFF is a system that performs a near real-time reaction to mitigate risks in malformed credit card transactions based on the historical data to detect a fraud, which is usually done after a transaction has taken place [2]. The traditional fraud detection practices are unable to deal with the volume and speed of the new data in real time. Therefore it is mandatory to create a scoring engine with the architecture of SCARFF, which is a new system architecture suitable for detecting fraud during an online shopping application instantly.

8.2. Lessons Learned from Failures

Over the years, the development and deployment of various payment processing systems have been plagued by failures or vulnerabilities that badly affected a banks' operational reliability and creditability. Here, a few notable examples are discussed and the lessons learned from these failures are distilled.

To countercheck accommodating various transactions such as cashing out and loading, a risk scoring system was developed, targeting transactions at ATMs and self-service kiosks. Scoring components were built using multiple modeling techniques like decision tree, neural networks, and regression. With multiple modeling techniques built for each component, on average, seven models were used for each scoring component, scoring each model in parallel, and voting final risk score based on weighted averaging. Here lies the first design flaw: the risk scoring system took around 40 seconds to run on average for low-risk scoring components like withdrawal and transfer to a bank account, and even longer for higher risk scoring components like load cash action, which sometimes even took one minute. A similar bot attack that tried out thousands of requests with benign scores in ATMs led to huge cash out loss. Further investigation revealed unaccounted transaction typology for cash out, load cash at partner's merchant, cashing out on a non-bank ATM. Eventually, a huge fraud prevention effort was launched to harden the process. Speeding up the model scoring is of utmost priority for a real-time payment processing or anti-fraud system.

After the fraud case, a more structured method for building new scoring components in the Real-time Credit Evaluation system was implemented with the support of legacy credit scoring models. A general picture of the system is that the incoming transaction is first checked with basic card and branch rules. Transactions with no match would go to the risk scoring system. An important risk scoring component is model-built credit score. This score is then passed to scoring functions which computed risk rules on the built data set and return flags on the transaction. Another design flaw was uncovered this time. One Friday at around 6pm, transaction spikes were reported on cards with a high built credit score: all flagged with the same misclassified score. During investigation, it was discovered that the credit score component reading from the data source was faulty with corrupted data running wild in the system. A more comprehensive data quality control process was put into place post the incident to catch such gross errors immediately before scoring.

8.3. Industry Comparisons

section compares the proposed AI-powered risk scoring and fraud detection frameworks in real-time payment processing systems with the existing frameworks already implemented in the industry. The comparison will be made across four dimensions, namely, architecture, scalability, features, and performance.

The deployment of payment processing systems for real-time transaction streaming requires the adoption of cloud native architectures and solutions that allow for distributed processing of data pipelines. Within this regard, can be leveraged, as it facilitates the implementation of global payment processing systems, with support for cloud-native architectures. This framework provides major components

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1317-1339

for ingestion of data streams, event processing, model monitoring, and orchestration of AI components. It allows for the addition of any heterogeneous technology components and operationalizes, maintains, monitors, and explains the AI models. The combination of this framework together with the proposed AI-powered risk scoring and fraud detection solutions has the potential to safely deploy real-time event-driven payment processing systems.

The implementation of frameworks for AI-powered risk scoring and fraud detection approaches in the industry is often limited by the required scalability. The framework presented by [2] illustrates a reinforcement learning-based fraud detection solution on relevant technological stacks that leverage fast-scoring engines to obtain near-real-time processing of payment transactions. The proposed solutions largely exceed the provided classification performance metrics of this benchmark. In addition, the proposed ensembles of AI risk scoring and fraud detection solutions can operate in parallel in a cost-effective manner. Together with the deployment architecture and alignment with regulatory obligations, this indicates a strong competitive advantage in the market.

9. Future Trends

The rapid development of e-commerce and mobile payment, accompanied by a general increase in transaction amounts, has created conditions for the exploitation of loopholes in transaction security in recent years. Transaction frauds seriously affect the healthy development of related industries and bring huge economic losses to consumers and merchants. Transaction frauds refer to activities in which fraudsters use forged identity-related information to illegally acquire property through means such as fake payment and rollback. To reduce losses caused by transaction frauds, merchants need to develop mechanisms for fraud detection and transaction risk control. The overall architecture of an effective mechanism for fraud detection and transaction risk control consists of two core engines: a risk scoring engine and a risk control engine. The risk scoring engine is responsible for measuring the risk level of each transaction based on its attributes. High scores indicate a greater likelihood of fraud. Since certain attributes of transactions are limited and sensitive, global payment tools do not provide necessary attribute information to merchants as needed. Based on the analysis of prior works, it is found that big data and machine learning technologies improve scoring models using historical data. The risk control engine is responsible for intervening once a risk score is calculated. The risk control engine proposes risk cut-off scores, beyond which a transaction will be rejected. Attributes used for risk scoring and controls based on these risk scores are designed and established [8].

With the rapid growth of credit card demand and the explosion of cardholders, fraud detection in real-time payments has become an important issue. Therefore, professionals want to improve the fraud detection performance of payment processing systems with minimal latency. However, real-time payments pose challenges to the design of fraud detection systems as they require an analysis of payment streams with a high point rate and little delay. With the advent of new technologies, there is also a growing need to process all payment cards in an environment with very low friction. As a result, vendors are finding it increasingly difficult to deploy high-performance fraud detection solutions. On the other hand, banks are under pressure to ensure compliance with a range of regulations including those from central banks, regional institutions, and international organizations. This has drawn the attention of researchers to new generation payment processing systems and their design [2].

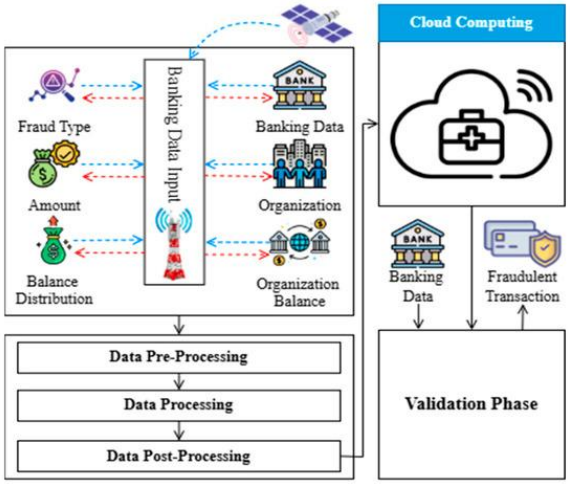

Fig : 5 Secure and Transparent Banking

9.1. Emerging Technologies

The rapid increase in adoption of instant real-time payment systems is a fertile ground for illicit activities including money laundering and fraud [8]. As the standards for payment systems change, strengthening anti-money laundering systems becomes imperative. The use of machine learning methods can allow for real-time transaction processing and fraud detection in the rapidly growing field of instant payments [2]. It is one of the first efforts that addresses fraud detection and risk scoring in instant payments elaborating on data, knowledge, and technology as well as structured machine learning and AI methods that can be applied.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1317-1339

Most of the existing methods do not cover fraud detection in the context of real-time systems, nor do they fulfil the high demands for clinical applications on safety and explainability. Time and context dependent methods are missing to cover the fast moving target of real-time payments. Fraud detection methods are restricted when it comes to considering upstream signal generation processes. As such, a shift occurs from batch auditing approaches to fast and efficient approaches enabling continuous monitoring directly during the decision-making process. Due to extensive research and time invested, a wide range of available statistical methods, such as past behaviour and normalisation approaches, can be utilized. In addition to that, there are general purpose machine-learned based methods available as known and well studied methods and ensemble methods.

Several specific machine learning methods need to be explored in greater detail to brighten the understanding of their special properties and strengths in the domain of real-time scoring and fraud detection. The options include instance-based, rule-based, decision tree learning, Bayesian networks, and neural networks which might provide frame challenging opportunities and innovations and are worth considering. These methods are readily available as open-source toolkits, but also covered under successfully deployed solutions already applied in practice.

9.2. Evolving Fraud Tactics

As online payment methods expand globally, customers are more inclined to utilize credit and debit cards for various transactions. Card acquisition processes are well structured; however, fraudsters have begun exploiting this payment method by engaging in card-not-present fraud. Accepting card payments can be risky for merchants if the transactions are not verified. Threats and fraud patterns are evolving and becoming more sophisticated and fast, leading to an increasing number of unauthorized payments and chargebacks. Understanding the plying methods of fraud will lead to the construction of an effective detection model that can accordingly offset fraudulent payments through quantification. A payment gateway requires a strong risk-scoring framework and a complex analysis of card payment fraud detection that performs online learning to adaptively approach the evolving pattern of fraudsters. The analysis space explores several fraud schemes regarding the characteristics of how fraudsters commit card payment frauds [9]. A fraudster generally possesses either a set of stolen card information or a compromised database of payment information. For each type of card fraud, three techniques are identified, with examples of how fraudsters have attempted to exploit card payments through those methods.

A major risk of the modern world economy is associated with the disruption of virtual commerce, which has continued escalating with advanced technologies such as big data, artificial intelligence, and sophisticated fraud schemes. Credit card fraud has become one of the most pressing challenges in online payment processing systems [8]. Well-designed security measures are necessary to ensure the reliability and safety of card online payment systems. Despite existing methods for card-related fraud detection, new evolving tactics of fraud exert a great failure impact on traditional detection systems. The ever-increasing value and usability of card information have made related financial crimes attractive to fraudsters and become important AI areas for the research of accurate and timely detection approaches.

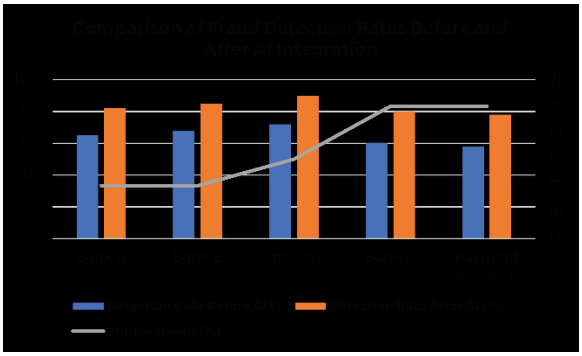

Fig : Comparison of Fraud Detection

9.3. AI Ethics in Fraud Detection

Before AI was embedded in everyday applications, models were usually based on rules that would need to be developed and tuned manually. Regional payment processing systems operated independently, and this dispersion complemented the rule-driven approach. Different processors would adopt different fee models, risk evaluation methods, and payment types. However, in recent years, the scenario has changed dramatically. 21st century fraudsters operate globally, and fraud attempts are carried out in nanoseconds that allow no time for human intervention. Rapidly growing payment volumes now exceed 5 trillion dollars a day, and payments now have to be processed in milliseconds. The regulation of space and the standardization of chargeback procedures resulted in a global payment acceptance model. Payment analytics is increasingly built around AI-based solutions. As a consequence, rule-based detection is steadily reaching its limits [7]. Deep neural networks achieve state-of-the-art performance for detecting irregular activities in payment processing systems. In order to deal with changing fraud patterns they are commonly integrated into an ensemble of models [3]. To this end, models need to be retrained, necessitating the acquisition of significant amounts of data

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1317-1339

from payment processors in different regions. The robust performance of AI-based solutions depends on the quality and quantity of the training datasets. When dealing with personal payments, datasets of sufficient quality are very hard to obtain. Furthermore, they cannot be stored entirely as sensitive data needs to be anonymized. All these challenges necessitate innovative approaches for handling data flow to model training units, as well as new methods for analyzing and visualizing the internal structures of deep learning models. Solutions have been developed for vertically federated analytics that can be assembled and utilized without data sharing. The starting point of transparent and privacy-preserving payment method detection is the hand-crafted features that obscures prior knowledge of payment types in the model. Latent feature vectors that are directly used by the model need to be encoded, which also generates an additional, lighter federated model with comparable accuracy. The latter can produce an interpretable similarity network, which summarizes latent feature information from all processors.

10. Conclusion

Until recently, the focus of payment processing systems has been on developing a number of computer processing and networking technologies that can facilitate rapid money transfers. Due to these technologies, real-time payment processing systems are on the rise. With these systems, money transfers can be settled within seconds and non-slowed down payments are likely to become the norm. However, the width, volume, and frequency of the payment ledger can be significantly overwhelming. This is important because a major goal of payment processing systems is to detect fraudulent payments. At some point, institutions running these systems may not be able to detect suspicious transactions before they are approved. The solution proposed is an AI-powered risk scoring and fraud detection framework that runs in the context of payment processing systems. The architecture is a two-level model. The first level computes risk scores that can greatly speed up fraud detection in downstream layers. The output of the first level is monitored as well as the input of the second level fraud detection model. This framework has been prototyped and some preliminary experiments in a real-life context performed that demonstrates its effectiveness and potential feasibility.

To help combat these problems, this project proposed to investigate fraud detection in payment processing systems in the context of several AI technologies. A risk scoring mechanism is proposed based on a model trained using transactions produced in a payment processing system. This risk scoring mechanism has the potential to speed up the fraud detection process in this real world as well as other similar payment processing systems. Previous machine learning models were limited in their ability to be applied in either streaming or real-time environments as well as lacking successful architectures that were capable of obtaining real-time predictions within milliseconds. The two-level architecture discussed demonstrates the feasibility of running an effective risk scoring mechanism in a near real-time manner.

The implementation of this project has several advantages. First, examining risk scoring as well as other AI technologies in payment processing systems that are real-time and large in scale may be beneficial to banking institutes in preventing fraudulent behaviours that may result in huge spurious losses. Large scale real world implementations of AI technologies also provides new ideas and architectures for future works across multiple fields beyond fraud detection in payment processing systems.

References:

[1] Challa, S. R., Malempati, M., Sriram, H. K., & Dodda, A. (2024). Leveraging Artificial Intelligence for Secure and Efficient Payment Systems: Transforming Financial Transactions, Regulatory Compliance, and Wealth Optimization. Leveraging Artificial Intelligence for Secure and Efficient Payment Systems: Transforming Financial Transactions, Regulatory Compliance, and Wealth Optimization (December 22, 2024).

[2] Revolutionizing Automotive Manufacturing with AI-Driven Data Engineering: Enhancing Production Efficiency through Advanced Data Analytics and Cloud Integration . (2024). MSW Management Journal, 34(2), 900-923.

[2] Pamisetty, A. (2024). Application of agentic artificial intelligence in autonomous decision making across food supply chains. European Data Science Journal (EDSJ) p-ISSN 3050-9572 en e-ISSN 3050-9580, 1(1).

[3] Paleti, S., Mashetty, S., Challa, S. R., ADUSUPALLI, B., & Singireddy, J. (2024). Intelligent Technologies for Modern Financial Ecosystems: Transforming Housing Finance, Risk Management, and Advisory Services Through Advanced Analytics and Secure Cloud Solutions. Risk Management, and Advisory Services Through Advanced Analytics and Secure Cloud Solutions (July 02, 2024).

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1317-1339

[4] Chakilam, C. (2024). Leveraging AI, ML, and Big Data for Precision Patient Care in Modern Healthcare Systems. European Journal of Analytics and Artificial Intelligence (EJAAI) p-ISSN 3050-9556 en e-ISSN 3050-9564, 1(1).

[5] Kummari, D. N. (2023). Energy Consumption Optimization in Smart Factories Using AI-Based Analytics: Evidence from Automotive Plants. Journal for Reattach Therapy and Developmental Diversities. https://doi.org/10.53555/jrtdd.v6i10s(2).3572

[6] Federated Edge Intelligence: Enabling Privacy-Preserving AI for Smart Cities and IoT Systems. (2024). MSW Management Journal, 34(2), 1175-1190.

[7] Koppolu, H. K. R. (2024). The Impact of Data Engineering on Service Quality in 5G-Enabled Cable and Media Networks. European Advanced Journal for Science & Engineering (EAJSE)-p-ISSN 3050-9696 en e-ISSN 3050-970X, 1(1).

[8] Sriram, H. K. (2024). A comparative study of identity theft protection frameworks enhanced by machine learning algorithms. Available at SSRN 5236625.

[9] Paleti, S., Singireddy, J., Dodda, A., Burugulla, J. K. R., & Challa, K. (2021). Innovative Financial Technologies: Strengthening Compliance, Secure Transactions, and Intelligent Advisory Systems Through AI-Driven Automation and Scalable Data Architectures. Secure Transactions, and Intelligent Advisory Systems Through AI-Driven Automation and Scalable Data Architectures (December 27, 2021).

[10] Singireddy, J. (2024). AI-Driven Payroll Systems: Ensuring Compliance and Reducing Human Error. American Data Science Journal for Advanced Computations (ADSJAC) ISSN: 3067-4166, 1(1).

[11] Chava, K. (2023). Integrating AI and Big Data in Healthcare: A Scalable Approach to Personalized Medicine. Journal of Survey in Fisheries Sciences. https://doi.org/10.53555/sfs.v10i3.3576

[12] Challa, K. (2024). Enhancing credit risk assessment using AI and big data in modern finance. American Data Science Journal for Advanced Computations (ADSJAC) ISSN: 3067-4166, 1(1).

[13] Pandiri, L. (2024). Integrating AI/ML Models for Cross-Domain Insurance Solutions: Auto, Home, and Life. American Journal of Analytics and Artificial Intelligence (ajaai) with ISSN 3067-283X, 1(1).

[14] Malempati, M. (2024). Leveraging cloud computing architectures to enhance scalability and security in modern financial services and payment infrastructure. European Advanced Journal for Science & Engineering (EAJSE)-p-ISSN 3050-9696 en e-ISSN 3050-970X, 1(1).

[15] Recharla, M. (2023). Next-Generation Medicines for Neurological and Neurodegenerative Disorders: From Discovery to Commercialization. Journal of Survey in Fisheries Sciences. https://doi.org/10.53555/sfs.v10i3.3564

[16] Kaulwar, P. K., Pamisetty, A., Mashetty, S., Adusupalli, B., & Pandiri, L. (2023). Harnessing Intelligent Systems and Secure Digital Infrastructure for Optimizing Housing Finance, Risk Mitigation, and Enterprise Supply Networks. International Journal of Finance (IJFIN)-ABDC Journal Quality List, 36(6), 372-402.

[17] Kalisetty, S., & Lakkarasu, P. (2024). Deep Learning Frameworks for Multi-Modal Data Fusion in Retail Supply Chains: Enhancing Forecast Accuracy and Agility. American Journal of Analytics and Artificial Intelligence (ajaai) with ISSN 3067-283X, 1(1).

[18] Chava, K., Chakilam, C., Suura, S. R., & Recharla, M. (2021). Advancing Healthcare Innovation in 2021: Integrating AI, Digital Health Technologies, and Precision Medicine for Improved Patient Outcomes. Global Journal of Medical Case Reports, 1(1), 29-41.

[19] Annapareddy, V. N., Preethish Nanan, B., Kommaragiri, V. B., Gadi, A. L., & Kalisetty, S. (2022). Emerging Technologies in Smart Computing, Sustainable Energy, and Next-Generation Mobility: Enhancing Digital Infrastructure, Secure Networks, and Intelligent Manufacturing. Venkata Bhardwaj and Gadi, Anil Lokesh and Kalisetty, Srinivas, Emerging Technologies in Smart Computing, Sustainable Energy, and Next-Generation Mobility: Enhancing Digital

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1317-1339

Infrastructure, Secure Networks, and Intelligent Manufacturing (December 15, 2022).

[20] Meda, R. (2024). Enhancing Paint Formula Innovation Using Generative AI and Historical Data Analytics. American Advanced Journal for Emerging Disciplinaries (AAJED) ISSN: 3067-4190, 1(1).

[21] Sai Teja Nuka (2023) A Novel Hybrid Algorithm Combining Neural Networks And Genetic Programming For Cloud Resource Management. Frontiers in HealthInforma 6953-6971

[22] Suura, S. R. (2024). The role of neural networks in predicting genetic risks and enhancing preventive health strategies. European Advanced Journal for Emerging Technologies (EAJET)-p-ISSN 3050-9734 en e-ISSN 3050-9742, 2(1).

[23] Kannan, S. (2024). Revolutionizing Agricultural Efficiency: Leveraging AI Neural Networks and Generative AI for Precision Farming and Sustainable Resource Management. Available at SSRN 5203726.

[24] Transforming Customer Experience in Telecom: Agentic AI-Driven BSS Solutions for Hyper-Personalized Service Delivery. (2024). MSW Management Journal, 34(2), 1161-1174.

[25] Singireddy, S. (2024). Applying Deep Learning to Mobile Home and Flood Insurance Risk Evaluation. American Advanced Journal for Emerging Disciplinaries (AAJED) ISSN: 3067-4190, 1(1).

[26] Leveraging Deep Learning, Neural Networks, and Data Engineering for Intelligent Mortgage Loan Validation: A Data-Driven Approach to Automating Borrower Income, Employment, and Asset Verification. (2024). MSW Management Journal, 34(2), 924-945.

[27] Srinivas Kalyan Yellanki. (2024). Building Adaptive Networking Protocols with AI-Powered Anomaly Detection for Autonomous Infrastructure Management . Journal of Computational Analysis and Applications (JoCAAA), 33(08), 3116–3130. Retrieved from https://eudoxuspress.com/index.php/pub/article/view/2423

[28] Transforming Customer Experience in Telecom: Agentic AI-Driven BSS Solutions for Hyper-Personalized Service Delivery. (2024). MSW Management Journal, 34(2), 1161-1174.

[29] Sriram, H. K., Challa, S. R., Challa, K., & ADUSUPALLI, B. (2024). Strategic Financial Growth: Strengthening Investment Management, Secure Transactions, and Risk Protection in the Digital Era. Secure Transactions, and Risk Protection in the Digital Era (November 10, 2024).

[30] Paleti, S. (2024). Neural Compliance: Designing AI-Driven Risk Protocols for Real-Time Governance in Digital Banking Systems. Available at SSRN 5233099.

[31] Sriram, H. K., Challa, S. R., Challa, K., & ADUSUPALLI, B. (2024). Strategic Financial Growth: Strengthening Investment Management, Secure Transactions, and Risk Protection in the Digital Era. Secure Transactions, and Risk Protection in the Digital Era (November 10, 2024).

[32] Pamisetty, V. (2023). Leveraging AI, Big Data, and Cloud Computing for Enhanced Tax Compliance, Fraud Detection, and Fiscal Impact Analysis in Government Financial Management. International Journal of Science and Research (IJSR), 12(12), 2216–2229. https://doi.org/10.21275/sr23122164932

[33] Komaragiri, V. B. Harnessing AI Neural Networks and Generative AI for the Evolution of Digital Inclusion: Transformative Approaches to Bridging the Global Connectivity Divide.

[34] Annapareddy, V. N. (2024). Leveraging Artificial Intelligence, Machine Learning, and Cloud-Based IT Integrations to Optimize Solar Power Systems and Renewable Energy Management. Machine Learning, and Cloud-Based IT Integrations to Optimize Solar Power Systems and Renewable Energy Management (December 06, 2024).

[35] Pamisetty, A. (2024). Leveraging Big Data Engineering for Predictive Analytics in Wholesale Product Logistics. Available at SSRN 5231473.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1317-1339

[36] Dodda, A. (2024). Integrating Advanced and Agentic AI in Fintech: Transforming Payments and Credit Card Transactions. European Advanced Journal for Emerging Technologies (EAJET)-p-ISSN 3050-9734 en e-ISSN 3050-9742, 1(1).

[37] Gadi, A. L., Kannan, S., Nanan, B. P., Komaragiri, V. B., & Singireddy, S. (2021). Advanced Computational Technologies in Vehicle Production, Digital Connectivity, and Sustainable Transportation: Innovations in Intelligent Systems, Eco-Friendly Manufacturing, and Financial Optimization. Universal Journal of Finance and Economics, 1(1), 87-100.

[38] Adusupalli, B., & Insurity-Lead, A. C. E. The Role of Internal Audit in Enhancing Corporate Governance: A Comparative Analysis of Risk Management and Compliance Strategies. Outcomes. Journal for ReAttach Therapy and Developmental Diversities, 6, 1921-1937.

[39] Suura, S. R., Chava, K., Recharla, M., & Chakilam, C. (2023). Evaluating Drug Efficacy and Patient Outcomes in Personalized Medicine: The Role of AI-Enhanced Neuroimaging and Digital Transformation in Biopharmaceutical Services. Journal for ReAttach Therapy and Developmental Diversities, 6, 1892-1904.

[40] Kummari, D. N. (2023). AI-Powered Demand Forecasting for Automotive Components: A Multi-Supplier Data Fusion Approach. European Advanced Journal for Emerging Technologies (EAJET)-p-ISSN 3050-9734 en e-ISSN 3050-9742, 1(1).

[41] Sheelam, G. K. (2024). Deep Learning-Based Protocol Stack Optimization in High-Density 5G Environments. European Advanced Journal for Science & Engineering (EAJSE)-p-ISSN 3050-9696 en e-ISSN 3050-970X, 1(1).

[42] AI-Powered Revenue Management and Monetization: A Data Engineering Framework for Scalable Billing Systems in the Digital Economy . (2024). MSW Management Journal, 34(2), 776-787.

[43] Sriram, H. K. (2023). The Role Of Cloud Computing And Big Data In Real-Time Payment Processing And Financial Fraud Detection. Available at SSRN 5236657.

[44] Paleti, S., Burugulla, J. K. R., Pandiri, L., Pamisetty, V., & Challa, K. (2022). Optimizing Digital Payment Ecosystems: Ai-Enabled Risk Management, Regulatory Compliance, And Innovation In Financial Services. Regulatory Compliance, And Innovation In Financial Services (June 15, 2022).

[45] Singireddy, J. (2024). AI-Enhanced Tax Preparation and Filing: Automating Complex Regulatory Compliance. European Data Science Journal (EDSJ) p-ISSN 3050-9572 en e-ISSN 3050-9580, 2(1).

[46] Karthik Chava. (2022). Harnessing Artificial Intelligence and Big Data for Transformative Healthcare Delivery. International Journal on Recent and Innovation Trends in Computing and Communication, 10(12), 502–520. Retrieved from https://ijritcc.org/index.php/ijritcc/article/view/11583

[47] Challa, K. Dynamic Neural Network Architectures for Real-Time Fraud Detection in Digital Payment Systems Using Machine Learning and Generative AI.

[48] Lahari Pandiri. (2023). Specialty Insurance Analytics: AI Techniques for Niche Market Predictions. International Journal of Finance (IJFIN) - ABDC Journal Quality List, 36(6), 464-492.

[49] Recharla, M., & Chitta, S. AI-Enhanced Neuroimaging and Deep Learning-Based Early Diagnosis of Multiple Sclerosis and Alzheimer's.

[50] Malempati, M. (2023). A Data-Driven Framework For Real-Time Fraud Detection In Financial Transactions Using Machine Learning And Big Data Analytics. Available at SSRN 5230220.

[51] Pandiri, L., Paleti, S., Kaulwar, P. K., Malempati, M., & Singireddy, J. (2023). Transforming Financial And Insurance Ecosystems Through Intelligent Automation,

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1317-1339

Secure Digital Infrastructure, And Advanced Risk Management Strategies. Educational Administration: Theory and Practice, 29 (4), 4777–4793.

[52] Lakkarasu, P. (2024). Advancing Explainable AI for AI-Driven Security and Compliance in Financial Transactions. Journal of Artificial Intelligence and Big Data Disciplines, 1(1), 86-96.

[53] Gadi, A. L., Kannan, S., Nanan, B. P., Komaragiri, V. B., & Singireddy, S. (2021). Advanced Computational Technologies in Vehicle Production, Digital Connectivity, and Sustainable Transportation: Innovations in Intelligent Systems, Eco-Friendly Manufacturing, and Financial Optimization. Universal Journal of Finance and Economics, 1(1), 87-100.

[54] Meda, R. (2023). Developing AI-Powered Virtual Color Consultation Tools for Retail and Professional Customers. Journal for ReAttach Therapy and Developmental Diversities. https://doi.org/10.53555/jrtdd.v6i10s(2).3577

[55] Nuka, S. T., Annapareddy, V. N., Koppolu, H. K. R., & Kannan, S. (2021). Advancements in Smart Medical and Industrial Devices: Enhancing Efficiency and Connectivity with High-Speed Telecom Networks. Open Journal of Medical Sciences, 1(1), 55-72.

[55] Suura, S. R. Artificial Intelligence and Machine Learning in Genomic Medicine: Redefining the Future of Precision Diagnostics.

[56] Kannan, S., & Seenu, A. (2024). Advancing Sustainability Goals with AI Neural Networks: A Study on Machine Learning Integration for Resource Optimization and Environmental Impact Reduction. management, 32(2).

[57] Motamary, S. (2022). Enabling Zero-Touch Operations in Telecom: The Convergence of Agentic AI and Advanced DevOps for OSS/BSS Ecosystems. Kurdish Studies. https://doi.org/10.53555/ks.v10i2.3833

[58] Singireddy, S. (2024). Predictive Modeling for Auto Insurance Risk Assessment Using Machine Learning Algorithms. European Advanced Journal for Emerging Technologies (EAJET)-p-ISSN 3050-9734 en e-ISSN 3050-9742, 1(1).

[59] Mashetty, S. (2024). The role of US patents and trademarks in advancing mortgage financing technologies. European Advanced Journal for Science & Engineering (EAJSE)-p-ISSN 3050-9696 en e-ISSN 3050-970X, 1(1).

[60] Yellanki, S. K. (2024). Leveraging Deep Learning and Neural Networks for Real-Time Crop Monitoring in Smart Agricultural Systems. American Data Science Journal for Advanced Computations (ADSJAC) ISSN: 3067-4166, 1(1).

[61] Challa, S. R. (2024). Behavioral Finance in Financial Advisory Services: Analyzing Investor DecisionMaking and Risk Management in Wealth Accumulation. Available at SSRN 5135949.

[62] Paleti, S. (2023). Data-First Finance: Architecting Scalable Data Engineering Pipelines for AI-Powered Risk Intelligence in Banking. Available at SSRN 5221847.

[63] Pamisetty, V., Dodda, A., Singireddy, J., & Challa, K. (2022). Optimizing Digital Finance and Regulatory Systems Through Intelligent Automation, Secure Data Architectures, and Advanced Analytical Technologies. Jeevani and Challa, Kishore, Optimizing Digital Finance and Regulatory Systems Through Intelligent Automation, Secure Data Architectures, and Advanced Analytical Technologies (December 10, 2022).

[64] Komaragiri, V. B., Edward, A., & Surabhi, S. N. R. D. Enhancing Ethernet Log Interpretation And Visualization.

[65] Kannan, S., Annapareddy, V. N., Gadi, A. L., Kommaragiri, V. B., & Koppolu, H. K. R. (2023). AI-Driven Optimization of Renewable Energy Systems: Enhancing Grid Efficiency and Smart Mobility Through 5G and 6G Network Integration. Available at SSRN 5205158.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1317-1339

[66] Kommaragiri, V. B., Preethish Nanan, B., Annapareddy, V. N., Gadi, A. L., & Kalisetty, S. (2022). Emerging Technologies in Smart Computing, Sustainable Energy, and Next-Generation Mobility: Enhancing Digital Infrastructure, Secure Networks, and Intelligent Manufacturing. Venkata Narasareddy and Gadi, Anil Lokesh and Kalisetty, Srinivas.

[67] Pamisetty, V. (2022). Transforming Fiscal Impact Analysis with AI, Big Data, and Cloud Computing: A Framework for Modern Public Sector Finance. Big Data, and Cloud Computing: A Framework for Modern Public Sector Finance (November 30, 2022).

[68] Paleti, S. (2023). Trust Layers: AI-Augmented Multi-Layer Risk Compliance Engines for Next-Gen Banking Infrastructure. Available at SSRN 5221895.

[69] Rao Challa, S. (2023). Revolutionizing Wealth Management: The Role Of AI, Machine Learning, And Big Data In Personalized Financial Services. Educational Administration: Theory and Practice. https://doi.org/10.53555/kuey.v29i4.9966

[70] Machine Learning Applications in Retail Price Optimization: Balancing Profitability with Customer Engagement. (2024). MSW Management Journal, 34(2), 1132-1144.

[71] Someshwar Mashetty. (2024). Research insights into the intersection of mortgage analytics, community investment, and affordable housing policy. Journal of Computational Analysis and Applications (JoCAAA), 33(08), 3377–3393. Retrieved from https://www.eudoxuspress.com/index.php/pub/article/view/2496

[72] Lakkarasu, P., Kaulwar, P. K., Dodda, A., Singireddy, S., & Burugulla, J. K. R. (2023). Innovative Computational Frameworks for Secure Financial Ecosystems: Integrating Intelligent Automation, Risk Analytics, and Digital Infrastructure. International Journal of Finance (IJFIN)-ABDC Journal Quality List, 36(6), 334-371.

[72] Implementing Infrastructure-as-Code for Telecom Networks: Challenges and Best Practices for Scalable Service Orchestration. (2021). International Journal of Engineering and Computer Science, 10(12), 25631-25650. https://doi.org/10.18535/ijecs.v10i12.4671

[73] Kannan, S. The Convergence of AI, Machine Learning, and Neural Networks in Precision Agriculture: Generative AI as a Catalyst for Future Food Systems.

[74] Suura, S. R. (2024). Agentic artificial intelligence systems for dynamic health management and real-time genomic data analysis. European Journal of Analytics and Artificial Intelligence (EJAAI) p-ISSN 3050-9556 en e-ISSN 3050-9564, 1(1).

[75] Meda, R. (2022). Integrating IoT and Big Data Analytics for Smart Paint Manufacturing Facilities. Kurdish Studies. https://doi.org/10.53555/ks.v10i2.3842

[76] Nandan, B. P., & Chitta, S. (2022). Advanced Optical Proximity Correction (OPC) Techniques in Computational Lithography: Addressing the Challenges of Pattern Fidelity and Edge Placement Error. Global Journal of Medical Case Reports, 2(1), 58-75.

[77] Lakkarasu, P. (2023). Designing Cloud-Native AI Infrastructure: A Framework for High-Performance, Fault-Tolerant, and Compliant Machine Learning Pipelines. Journal for ReAttach Therapy and Developmental Diversities. https://doi.org/10.53555/jrtdd.v6i10s(2).3566

[78] Kaulwar, P. K. (2022). Securing The Neural Ledger: Deep Learning Approaches For Fraud Detection And Data Integrity In Tax Advisory Systems. Migration Letters, 19, 1987-2008.

[79] Pandiri, L., Paleti, S., Kaulwar, P. K., Malempati, M., & Singireddy, J. (2023). Transforming Financial And Insurance Ecosystems Through Intelligent Automation, Secure Digital Infrastructure, And Advanced Risk MaRecharla, M., & Chitta, S. (2022). Cloud-Based Data Integration and Machine Learning Applications in Biopharmaceutical Supply Chain

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 34 Issue 2, July-Dec 2024, Pages: 1317-1339

Optimization.nagement Strategies. Educational Administration: Theory and Practice, 29 (4), 4777–4793.

[80] Pandiri, L., Paleti, S., Kaulwar, P. K., Malempati, M., & Singireddy, J. (2023). Transforming Financial And Insurance Ecosystems Through Intelligent Automation, Secure Digital Infrastructure, And Advanced Risk Management Strategies. Educational Administration: Theory and Practice, 29 (4), 4777–4793.

[81] Challa, K. (2023). Optimizing Financial Forecasting Using Cloud Based Machine Learning Models. Journal for ReAttach Therapy and Developmental Diversities. https://doi.org/10.53555/jrtdd.v6i10s(2).3565

[82] Chava, K. (2020). Machine Learning in Modern Healthcare: Leveraging Big Data for Early Disease Detection and Patient Monitoring. International Journal of Science and Research (IJSR), 9(12), 1899–1910. https://doi.org/10.21275/sr201212164722

[83] Kalisetty, S., & Singireddy, J. (2023). Optimizing Tax Preparation and Filing Services: A Comparative Study of Traditional Methods and AI Augmented Tax Compliance Frameworks. Available at SSRN 5206185.

[84] Sriram, H. K. (2022). Integrating generative AI into financial reporting systems for automated insights and decision support. Available at SSRN 5232395.

[85] Koppolu, H. K. R. Deep Learning and Agentic AI for Automated Payment Fraud Detection: Enhancing Merchant Services Through Predictive Intelligence.

[86] Sheelam, G. K. (2023). Adaptive AI Workflows for Edge-to-Cloud Processing in Decentralized Mobile Infrastructure. Journal for Reattach Therapy and Development Diversities. https://doi.org/10.53555/jrtdd.v6i10s(2).3570ugh Predictive Intelligence.

[87] End-to-End Traceability and Defect Prediction in Automotive Production Using Blockchain and Machine Learning. (2022). International Journal of Engineering and Computer Science, 11(12), 25711-25732. https://doi.org/10.18535/ijecs.v11i12.4746

[88] Chakilam, C. (2022). Integrating Machine Learning and Big Data Analytics to Transform Patient Outcomes in Chronic Disease Management. Journal of Survey in Fisheries Sciences. https://doi.org/10.53555/sfs.v9i3.3568

[89] Pamisetty, A. (2024). Leveraging Big Data Engineering for Predictive Analytics in Wholesale Product Logistics. Available at SSRN 5231473.

[90] Gadi, A. L. (2022). Connected Financial Services in the Automotive Industry: AI-Powered Risk Assessment and Fraud Prevention. Journal of International Crisis and Risk Communication Research, 11-28.

[91] Dodda, A. (2023). AI Governance and Security in Fintech: Ensuring Trust in Generative and Agentic AI Systems. American Advanced Journal for Emerging Disciplinaries (AAJED) ISSN: 3067-4190, 1(1).

[92] Pamisetty, A. Optimizing National Food Service Supply Chains through Big Data Engineering and Cloud-Native Infrastructure.

[93] Challa, K. (2022). The Future of Cashless Economies Through Big Data Analytics in Payment Systems. International Journal of Scientific Research and Modern Technology, 60–70. https://doi.org/10.38124/ijsrmt.v1i12.467

[94] Pamisetty, A. (2023). Cloud-Driven Transformation Of Banking Supply Chain Analytics Using Big Data Frameworks. Available at SSRN 5237927.