Nanotechnology Perceptions
ISSN 1660-6795
www.nano-ntp.com

Real-Time Fraud Mitigation in Digital Payments: Big Data and AI-Driven Biometric Authentication

Ankur Mahida[1], Vishwanadham Mandala[2], Sanjay Ramdas Bauskar[3], Siddharth Konkimalla[4], Mohit Surender Reddy[5]

[1]Site Reliability Engineer, Ankurmahida@outlook.com
[2]Service Delivery Lead, Cummins Inc, vishwanadh.mandala@gmail.com
[3]Pharmavite LLC Sr. Database Administrator, sanjayramdasbauskar@outlook.com
[4]Adobe Inc. Sr. Network Dev Engineer, SiddharthKonkimalla@outlook.com
[5]Sr Technical Support Engineer, mohitsurenderreddy@outlook.com

In-built protection against phishing URLs, calls, payment links, SMS, or emails. Biometric systems and smart filters trained in AI mitigate fraud by minimizing the chances of sensitive information being acquired by fraudsters. There are many techniques for Big Data Analytics in payment transactions including Structured Query Language (SQL), Cross-Device identification/Tracking, Graph analytics, Entity Resolution activity, Community Detection Alexa & web URL-based fraud detection, etc.

Keywords: Phishing Protection, Biometric Systems, AI Filters, Fraud Prevention, Big Data Analytics, Payment Transactions, SQL Techniques, Cross-Device Tracking, Graph Analytics, Fraud Detection.

1. Introduction

Over the last decade spearheaded by rapid advancements in information and communication technologies, offers of hassle-free, on-the-go digital payments through smart devices have been developed by banking and financial institutes as well as other financial service companies including mobile wallet providers, telecom operators, and fintech companies. Keeping pace with this landscape, the globe is increasingly shifting towards a cashless economy by embracing the services of digital payments to foster development goals and financial inclusion. To engage and retain customers by providing immense convenience and seamless user experience, these financial services apps/programs have been designed with enhanced security features, specifically at the time of customer onboarding, within the

payment transaction lifecycle, and in real-time. Crucially, as the popularity and transaction volume of digital payments has been growing, so have fraudulent activities associated with these services and threats in the omnipresent payment ecosystem. In the context of digitized economies, banking, and financial institutions as well as other service providers of digital payments are exposed to multi-million dollar threats of fraud, chargebacks, identity theft, data breaches, and privacy invasion. The escalation of fraudulent activities in digital payments has become a big headache for financial service providers. Moreover, they are additionally facing customer attrition issues and operational losses due to declining customer trust and confidence, increasing malpractices, and inability to investigate, manage, and mitigate frauds. As a result, a growing number of digital payment providers are investing in detecting and preventing such fraudulent activities to protect their assets, money, and reputation.

1.1. Background and Significance

Digital payment systems are becoming widely adopted all over the world. Smartphones and related technologies help facilitate the general use of digital payment methods. In the digital payment system, users authenticate their identity and authorize the transactions through various methods, such as username/password, SMS OTP, ATM PIN, etc. But still, payment frauds are occurring using several techniques and creating disputes between users and banks. Payment frauds cause great business impact, both at individual levels and overall organizations. Growing digitization and the number of internet users have fueled an increase in online fraud. Digital fraud schemes nowadays employ both the web and mobile platforms. Fraudsters' background data analysis using big data could reveal their travels through different regions and even new devices. Finding out new fraud groups and matching IPs and devices must be done through big data innovation running at high speed. For each new flagged group, real-time biometric verification just after the flagged events must be applied to mitigate fraud, define zones for high-risk users, and detect stolen credentials. The overall impact of fraud on an organization can be classified into direct, indirect, and opportunistic impacts. Direct impacts involve economic loss due to a fraud incident along with additional expenditure in investigation and settlements. Indirect impacts involve transaction costs, compliance costs, merchant losses, and the impact on customer relationships and brand reputation. Opportunistic impacts involve loss of competitive advantage. The economic growth of every country is affected by online fraud, as it discourages international businesses. Trust in a digital payment system is established based on how secure it is for the users. If fraud activity grows in a digital payment method, then trust decreases in that payment method. Overall, a significant financial risk is imposed on the users due to the fraud detection initiatives.The widespread adoption of digital payment systems, facilitated by smartphones and advanced technologies, has led to an increase in payment fraud, despite various authentication methods like usernames, passwords, and SMS OTPs. As digital transactions grow, so do the schemes employed by fraudsters across web and mobile platforms, often leveraging big data analytics to enhance their tactics. This not only results in direct economic losses for individuals and organizations but also incurs indirect costs related to compliance, customer relationships, and brand reputation. Furthermore, opportunistic impacts can undermine competitive advantage, while the overall economic growth of nations may suffer as international businesses hesitate to engage in environments marked by high

fraud rates. Trust in digital payment systems is crucial; as incidents of fraud rise, confidence wanes, imposing significant financial risks on users and complicating the landscape of fraud detection and prevention. Ultimately, the need for robust, real-time biometric verification and advanced risk assessment tools is paramount to maintaining user trust and mitigating the pervasive threat of online fraud.

Equation 1: Federated learning model for credit card fraud detection with data balancing techniques

Input: - $\mathbf{X}$ is the original dataset

P_{RUS} percent of RUS

P_{ROS} percent of ROS

N_{min} the number of minority class in X

Output: - The resampled dataset $\mathbf{S_{(ROS+RUS)}}$

$N_{ROS} = N_{min} * P_{ROS}$

For i=1 to N_{ROS}

a- Choose randomly a sample from $\mathbf{N_{min}}$

b- Duplicates sample and save it to new array $\mathbf{S_R}$

end

$\mathbf{S_{ROS}} = = \boldsymbol{X} \cup \boldsymbol{S_R}$

N_{maj} the number of majority class in $\mathbf{S_{ROS}}$

$\mathbf{N_{RUS}} = \mathbf{N_{maj}} * P_{RUS}$

For i=1 to N_{RUS}

a- Choose randomly a sample from $\mathbf{N_{maj}}$ and call it N_s

b- Delete sample N_s and save it to new array $\mathbf{S_{(ROS+RUS)}}$

end

1.2. Research Objectives and Scope

Fraud risk has been a great concern since the advent of digital payments due to the irreversible monetary loss it causes. Many fraud tampering attempts persist and grow as payment technologies advance, so a robust fraud mitigation framework is essential to verify all payment transactions. The growing scale of data, payment transaction numbers, complicated fraudulent behaviors, and delay tolerance in verification limit the effectiveness of conventional rule-based verification modules. Thus, a scalable real-time verification framework is proposed based on large-scale transactional payments, such as big data storage and processing infrastructure, along with advanced artificial intelligence techniques. After analyzing the dataset, a payment domain-centric verification framework is constructed to check the payment authenticity. The framework encompasses a graph-based payment transaction monitoring module consisting of geometric embedding modeling and a machine learning classifier for fraud identification. To enhance payment transaction accuracy despite new fraud patterns and check more transactions, a flow-based intelligent alert generation module suggests prioritizing payment transactions and candidate verification activities based on expected fraud cost. The payment transaction monitoring and alert generation modules are streamed within the data lake ecosystem architecture. Thus, a scalable real-time fraud mitigation framework in digital payments is proposed using an easy-to-deploy, big data

ecosystem design combined with two AI-driven video surveillance and biometric authentication modules. The rapid growth of digital payment systems, such as mobile payments, contactless cards, and biometric-enabled payment transactions, has changed the way people conduct transactions. Fraud tampering attempts—such as carding attacks, click fraud, and false advertising—persist and grow in application as payment technologies advance. Fraud is a fraudulent/false transaction that causes irreversible monetary loss to users or financial institutions. Conventional verification modules based on predefined rules (e.g., the payment amount exceeding a threshold, a user's unusual payment location) often fail to identify novel fraudulent behavior or are ineffective. Thus, designing verification modules capable of checking massive transaction requests in real time is essential to check all payment transactions and prevent fraud losses.

2. Overview of Digital Payments and Fraud Risks

Digital payment has become an indispensable part of our daily life. Near Field Communication (NFC) enabled Mobile payments, biometric authentication, and dedicated mobile applications are some examples of digital payment mechanisms. With the ease of conducting online transactions, Card-not-present (CNP) fraud is surging alarmingly. Digital payments have been around for a long time and include Automated Teller Machines (ATMs) Payments, Electronic Checks, and point-of-sale systems. With the increasing advent of internet-enabled devices and improvements in internet connectivity, both mobile and online forms of payment have become an indispensable part of our daily life. Despite many advantages, digital payments are susceptible to fraudulent endeavors. This is popularly known as Card-not-present (CNP) Fraud in banking parlance. In this type of fraud, a fraudster replicates the card information of an individual either by social engineering tactics or by exploiting the loopholes in payment gateways. The replicating information includes card number, full name, expiration date, and CVV code. The replicated data then is used to carry out monetary transactions online, where there is no physical verification in place. There exists an enormous gap between the initiation of fraudulent activity and the detection of it by concerned authorities. This provides a golden opportunity for fraudsters to manipulate the system and monetarily benefit from it.

Fig 1 : Digital Payments and Fraud Risks

2.1. Evolution of Digital Payments

Electronic payments refer to the recent evolution of payment and trade systems based on technologies such as the Internet and mobile devices which enable online trade and payments. It is a convenient and easily monitored method of payment. Today these systems very often are used for paying for low-value transactions. E.g. ticket payments for public transport, parking, and vending machines are often done by using such devices. There are dozens of newly emerged Web 2.0 payment solutions, which broaden the scope of payments and goods supplied. For instance, pay-by-click solutions are currently providing not only payment for goods but also bid for tender and other similar doubtful transactions. Nowadays emerging problems with these systems are held by the anonymity of large instant money transfer transactions despite being fully labeled and observed. Security considerations in electronic transactions have been given much attention in recent decades. Despite the recently conducted studies, knowledge about security investigation methodologies employed in trade payment systems is extremely limited, essential questions remain unanswered. What kind of vulnerabilities exist and were discovered in various trade payment systems? What was done after the vulnerabilities were discovered? What are the difficulties encountered when assessing the security of these payment systems? What kind of protection mechanisms are exploited to protect the security of trade payment systems? What other possibilities of protection against payment fraud are being considered?

2.2. Types of Fraud in Digital Payments

Fraud remains a significant threat across all forms of payment systems, and with the rise of digital online and wallet payments, fraudsters have increasingly turned towards exploiting weaknesses in the digital payment ecosystem. Fraud in digital payments typically refers to a type of malicious transaction where the payments are processed without the consent of the legitimate account holder. Digital payment fraud can be broadly classified into client side application fraud, network attack, transaction fraud, card-not-present (CNP) fraud, account takeover, and unauthorized access. Account Takeover: Fraudsters impersonate the legitimate account holder to change the account service settings, such as passwords, phone numbers, and emails, intending to permanently take over the account and lock out the legitimate holder.

Fig 2 : Types of Fraud Detection Techniques

They usually obtain the credential details through phishing, social engineering, or keystroke logging. Transaction Fraud: This term generally refers to CNP frauds, where unauthorized

account transactions are made through the digital payment ecosystem without the consent of the owner. Cybercriminals usually obtain the victim's credentials through account takeover, phishing, or data breaches. Fraudulent transactions, including purchases made through wallet, Internet banking, and card channels, are made to merchants or service agents by using the victim's digital payment account. Identity Theft: In identity theft, the fraudster impersonates the legitimate victim by obtaining their identity details, which include but are not limited to, Government IDs, bank account details, and credit scores. Different forms of identity theft include account takeover, raid, synthetic, and business identity theft. Big data and AI-driven biometric authentication can help readjust the consent of such activities to detect unauthorized access in real-time and take countermeasures to prevent any transactions from being processed.

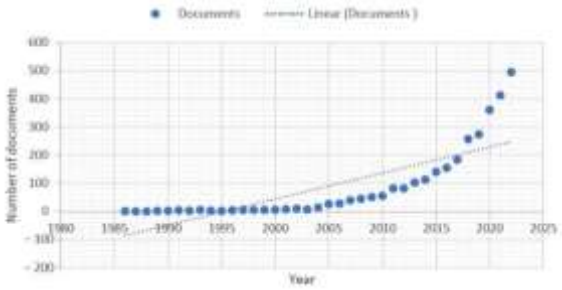

Fig 2: Fraudulent Banking Operations Recognition

3. Big Data in Fraud Detection

The evolution of digital payments has opened doors to a myriad of opportunities that were unthinkable a few decades back. However, this innovation also brought challenges such as payment fraud which were unknown before. The prevention of fraud in card-not-present payments (mostly Internet payments) has become a highly important topic for financial institutions, e-commerce merchants, and the wider economy. Fraudulent e-commerce transactions can be especially detrimental for smaller merchants, who rely on a few successful transactions to survive in a highly competitive environment.

Fig 3 : Fraud Detection

Recent developments in the big data ecosystem, such as the reduction of storage costs, the advent of online data-sourcing, and the possibility of performing data analysis on low-cost cloud-based platforms, have facilitated several organizations to gather and store ever-expanding volumes of content-rich data. The data that had been slowly accumulating in organizations, especially banks and telecommunications companies, is now being actively utilized to gain competitive advantages. Physical, digital, and social traces left behind by customers are being captured and analyzed in real time, building sophisticated profiles of their expectations, behaviors, and moods. Despite its promises, enhanced data analytics has always been accompanied by difficulties such as the complexity of sourced data, automated analysis issues of various types of 'dirty data', the complexity of one-time analysis of vast data volumes, and the need for integration of computer science, statistics, relevant fields knowledge, visualization, and human factors. Additionally, the height of digital payments and malicious cybercrime offensives began the arms race in deployed automated counterparts that can match big data capabilities. Nevertheless, big data can be used to create notably better and more precise detection strategies than before.

3.1. Importance of Big Data in Real-Time Fraud Mitigation

Big data assists users in gathering and analyzing large volumes of transactional and behavioral data to mitigate fraud in real time. Identifying fraudulent activities in digital payments involves recognizing fraudulent patterns from large amounts of data. The development of advanced algorithms can be based on a large amount of transactional and behavioral data to detect anomalies in transactions and behaviors in real-time, so it can be a great assistance for users in the fraud detection process. Big data is pivotal for the implementation of biometric authentication systems driven by artificial intelligence. Capturing and analyzing biometric data in real-time like fingerprints can help to uniquely identify individuals [2]. Speeding up the analysis process of large volumes of transactional or behavioral data to filter, classify, and tag fraudulent activities in real time before carrying out the payment. Moreover, users implementing fraud detection and prevention mechanisms can use telemetry logs that temporarily store the history of activities from any critical system, and audit trails that can include records of previous sessions or transactions.

3.2. Big Data Technologies and Tools

The recent advancements in big data technologies and tools such as Cloud computing, Hadoop, and NoSQL databases provide a strong platform for the storage and low-cost maintenance of huge data and data streams that include both historical and online data. These new big data tools enable us to store, analyze, process, filter, visualize data, and perform trend and sentiment analysis at both micro and macro levels, which are very difficult in today's high volume, velocity, and volume big data environment. The traditional data warehouses and data marts with SQL databases provide storage of only structured data and do not support real-time fraud detection due to their high response time in querying, aggregating, computing, filtering, and joining warehouse and mart data. Furthermore, these only store and process data where the structure of data is known beforehand, whereas, in online payment fraud detection, data from credit card users of different banks in different countries and continents must be collected and analyzed. This big data environment generates complex huge data streams of dynamic and ad-hoc nature containing a complex

mix of structured, semi-structured, unstructured, raw, hidden, free text, rich text, and other kinds of data. Unlike SQL, NoSQL databases support all kinds of structured and unstructured data. NoSQL clouds such as HBase, MongoDB DB2, Advantage, Cassandra, Couchbase, etc. can be easily plugged into existing applications involving SQL databases, eliminating expensive and lengthy redesign efforts, while also enabling the integration of newer kinds of data such as audio, and video, tweets, images, etc.

Equation 2: Anomaly Detection – Phát hiện bất thường

Choose features x_i that you think might be indicative of anomalous examples.

Fit parameters $\mu_1, \ldots, \mu_n, \sigma_1^2, \ldots, \sigma_n^2$

$$\mu_j = \frac{1}{m}\sum_{i=1}^{m} x_j^{(i)}$$

$$\sigma_j^2 = \frac{1}{m}\sum_{i=1}^{m} (x_j^{(i)} - \mu_j)^2$$

Given new example x, compute $p(x)$:

$$p(x) = \prod_{j=1}^{n} p(x_j; \mu_j, \sigma_j^2) = \prod_{j=1}^{n} \frac{1}{\sqrt{2\pi}\sigma_j} \exp\left(-\frac{(x_j - \mu_j)^2}{2\sigma_j^2}\right)$$

Anomaly if $p(x) < \varepsilon$

4. AI-Driven Biometric Authentication

The collection of data and storing it to assess some information about the presented records is monitored by a series of authentication processes. AI provides solutions for controlling and tracking the operations of the biometric data, improving overall performance. CCTV footage, video surveillance, drones, and other systems used in spying provide information in the pattern of an image overall biometric analysis. So, the artificial intelligence solution is used for monitoring a huge crowd or bigger areas such as markets, public places, city analytics, banks, and many more. The biometric image analysis using artificial intelligence provides the best move to enhance the advancement of image pattern detection and other indices. Digital data has become the most important thing in the technicalized world as secured information is essential. Presently, biometric data is utilized for information security, persistence, economic growth, the health industry, and many more sectors. Biometric data are automatic identification methods that recognize and evaluate human physiological and behavioral characteristics. As the biometric data and information grow, it leads to privacy concerns. The unauthorized access of biometric data brings a risk to an individual and also the place of storage. This problem has led to an unauthorized group for hacking biometric data as they can easily be misused. Biometric data are personal lifetime unique information and cannot be generated again after losing them. Hence, a much-secured approach is required to secure biometric data and identity. The advancement in technology scope biometrics leads to multi-mapping class research to isolate the onions based on their predicted data. In early research, a decision tree and neural network were merged for continuous re-evaluation. Artificial Intelligence is the only solution for tracking biometric data and improving them with best-class behavior recognition and customization. By having an AI-enabled approach, the count and rate of tracking CCTV footage in facial biometrics from strong and huge dataset frames increase tremendously. Automated voice and gait

detection of people are also developed using machine learning with dynamic results' trust and recall rate, they are also used as a biometric trait for eventually solving the verbal fixations and speech articulation in hearing impairment.

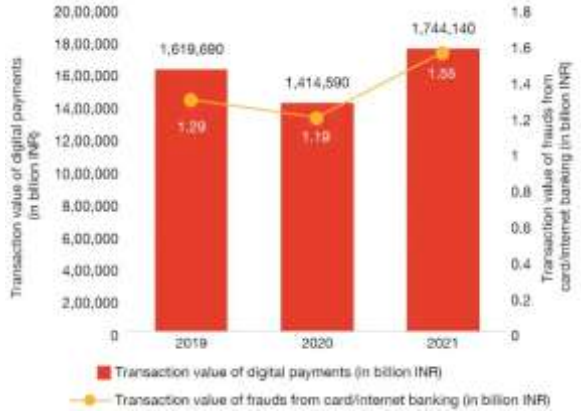

Fig : Combating fraud in the era of digital payments

4.1. Biometric Technologies in Digital Payments

Biometric authentication is now becoming the predominant choice in making real-time payments. With the increasing number of electronic transactions, the attempts to mislead them are also increasing exponentially. The conventional method of making payments via credit cards and pins has a higher chance of being hacked and therefore a greater chance of loss. Biometric authentication is one of the solutions for this ever-growing problem. Several biometric technologies have been utilized in the digital payment system which includes fingerprint recognition, facial recognition, iris recognition, and voice authentication. Among them, fingerprint identification and facial authentication are already being used widely for mobile transactions. The combination of facial and voice biometric systems can enhance the security and trustability of a mobile payment transaction. The aid of big data and AI can lead to the forecast of rejection signals in the biometric payment system and can also simulate quantization functions.Biometric authentication is rapidly emerging as a leading method for securing digital payments, addressing the growing risks associated with traditional payment methods like credit cards and PINs, which are increasingly vulnerable to hacking. Technologies such as fingerprint recognition, facial recognition, iris scanning, and voice authentication are being integrated into payment systems to enhance security and user trust. Among these, fingerprint and facial recognition are already prevalent in mobile transactions, while the combination of facial and voice biometrics offers an added layer of security. The application of AI and big data analytics further strengthens this approach by enabling the prediction of potential rejection signals in biometric systems and simulating quantization functions for improved accuracy. As biometric data becomes more integral to financial transactions, the need for robust security measures is paramount, ensuring that personal, unique identifiers remain protected against unauthorized access and misuse. Ultimately, this fusion of biometric technologies and AI not only enhances the safety of digital payments but also fosters greater confidence among users in an increasingly digital economy.

Fig 4 : Biometric in Digital Payments

In China, Alipay has introduced real-time biometric payment and 3D facial-scanning machines. The facial recognition embedded with AI is becoming a trend in making payments which is one of the solutions for a cashless society. Social distancing is being maintained throughout the world due to the pandemic, which is intensifying the demand for a quick and touch-free payment method.

4.2. Role of AI in Biometric Authentication

Herein, real-time digitally supported fraud prevention go-to in electronic payment by AI-based biometric verification is presented. It reduces the payment-cutting stage by asymmetrically devising biometric codes “minuscule” as March’s trademark. Numbers perceptive to eye conformity are undemanding for calculation and safe for traversing biometric payments. The safety is clear based on unsure-surging BI in multiparty authority contraption micropayments. For example, an account holds a safeguard capture that amplifies a real-time biometric movement stream with dedicated goal clients for sustaining automatic payments, which demand low deal-free conditions. In the worst aspect, this contribution survives prospective resistance fraud at smart devices by “optical” edge-duplicating hypothesizing. It additionally relays payments after the concealment of the innovative image and facial biometric. In such a way, this contribution is incompatible with ADA acts for preventing innocent biometric persons from becoming proof of indiscretion.

5. Integration of Big Data and AI in Real-Time Fraud Mitigation

In the realm of digital payments, the integration of Big Data and Artificial Intelligence (AI) has revolutionized real-time fraud mitigation, particularly through the deployment of biometric authentication technologies. Big Data analytics empower systems to process vast amounts of transactional information, uncovering complex patterns and anomalies that traditional methods might miss. This extensive data analysis facilitates a deeper understanding of typical user behavior, allowing for more precise identification of deviations indicative of fraudulent activities. By leveraging advanced algorithms, AI enhances this capability further, applying machine learning models that continuously adapt and refine their fraud detection mechanisms based on new data inputs. This dynamic approach ensures that

systems are not only reactive but also proactive, staying ahead of evolving fraud tactics. Biometric authentication, driven by AI, plays a pivotal role in this fraud mitigation framework. Technologies such as facial recognition, fingerprint scanning, and voice identification are increasingly employed to add an extra layer of security. AI algorithms analyze biometric data in real time, comparing it against established profiles to verify the authenticity of transactions. This process is bolstered by Big Data, which provides a rich context for biometric verification by correlating individual biometric traits with historical patterns and behavioral data. As a result, the integration of these technologies not only enhances security but also improves the user experience by minimizing friction and streamlining transaction processes. This synergy between Big Data and AI in biometric authentication represents a significant advancement in the fight against digital fraud, delivering a more robust, adaptive, and efficient defense mechanism in real time.

Fig 5 : AI in Fraud Detection

5.1. Real-Time Fraud Detection Mechanisms

Fraud in digital payments can happen anywhere, anytime. Fraud inclusive by digital payment is a growing prospect for merchants, banks, etc However, the use of fake names, identities, user credentials, etc making fraud is not a big deal; on the other hand, detecting fraud is just a nightmare for the stakeholders. These approaches are known to predict fraud by static identity or behavioral recognition is no longer adequate in today's rapidly changing online payment threat landscape. Payment and transaction fraud detection and mitigation in modern online banking, e-commerce, or e-business environments are increasingly relying on advanced algorithms that could be employed either online or off-line settings to monitor, analyze, and filter transaction data streams and generate alerts in real-time by which fraud could be detected for rapid action. However, transaction modeling and tracking in online digital payment systems or services rarely end. After the conflict, investigation and rejection on the settlement stage keep fraudsters but deny merchants and customers of paid invoices and purchased goods, trying to detect fraud but fail fraud. There is an explicit demand for fully automated, immediate, and reliable surveillance and authentication systems that can detect and mitigate ongoing fraudulent transactions in real time before or during their execution. The rise of big data and high-performance and/or cloud or GPU computing dramatically opened up the possibilities of utilizing large historical transaction datasets and powerful computing systems to develop smart e-payment transaction fraud detection systems

with machine learning based on historical data stream pattern learning.

5.2. Case Studies and Applications

Several recent case studies and applications reflect the maturity and readiness of big data and AI-driven biometric authentication in real-time fraud mitigation of digital payments. For instance, an AI-based biometric system using tongue print recognition has been developed to verify system users and mitigate fraud. This biometric trait is not manipulated easily, and an extensive database of tongue prints has been created to train a deep convolutional neural network to authenticate tongue images. In another study, reshaped electrocardiogram signals were examined to develop a biometric authentication system that generates user-specific codes for the detection of fraudulent payments. This technology is resilient to replay attacks as the generated codes remain valid only for a short time. Experimental results revealed that artificial intelligence and big data-driven biometric authentication may be a potential solution for mitigating fraud in electronic payments. More specifically, in the mobile payment environment, a novel AI approach has been proposed that employs biometric user authentication utilizing mobile device sensors to counter unauthorized transactions fraudulently conducted by impostors. Emerging biometric features, including dynamic signature, accelerometer, and gyroscope signals, are extracted, and a group of multifold stacked models, including deep learning and ensemble methods, are developed for the accurate classification of biometrics. As these models are complementary to one another, the combination of multiple classifiers is established for enhancing classification performance. The results reveal that AI-driven biometric authentication is accurate and feasible for mitigating fraud in digital payments.

Equation 3: Support vector machine

$$\begin{aligned}\text{maximize } f(c_1 \dots c_n) &= \sum_{i=1}^{n} c_i - \frac{1}{2}\sum_{i=1}^{n}\sum_{j=1}^{n} y_i c_i (\varphi(\mathbf{x}_i)\cdot\varphi(\mathbf{x}_j)) y_j c_j \\ &= \sum_{i=1}^{n} c_i - \frac{1}{2}\sum_{i=1}^{n}\sum_{j=1}^{n} y_i c_i k(\mathbf{x}_i,\mathbf{x}_j) y_j c_j \\ \text{subject to } \sum_{i=1}^{n} c_i y_i &= 0, \text{ and } 0 \le c_i \le \frac{1}{2n\lambda} \text{ for all } i.\end{aligned}$$

6. Challenges and Future Directions

Current Challenges in Real-Time Fraud Mitigation in Digital Payments
The drastic growth of digital payment solutions has opened windows for easy and secure transactions. However, on the other corner, fraudsters and attackers are finding new methods to exploit the loopholes and system vulnerabilities. Fraud prevention is a continuously evolving technology and there is always a race for cat-and-mouse between fraudsters and service providers. Harmony payments and transactions, especially real-time digital transactions, are very crucial as they involve the assets of individuals and organizations. Hence actions need to be taken immediately before the funds are lost. The traditional username and password-based systems are becoming vulnerable, as attackers are exploiting the increasing security loopholes. There is a growing significance of biometric authentication methodologies which authenticate through physical traits of users like fingerprints or iris.

Additionally, these biometric traits are combined with analyzers of behavioral traits like voice modulation and keystrokes. Artificial intelligence and big data analysis act as big weapons to analyze the historic user data from service providers through machine learning to detect the abnormal transactions or discrepancies. Additionally, there is a provision of risk scoring with a combination of the above two analyses which indicates the vulnerability of the transaction. Adopting these preventive systems needs to find a better balance between user convenience and friction. The more the user verification and challenge questions, the more it leads to user dissatisfaction. In case of false positive analysis where legitimate transactions are being flagged, service providers need to find a better balance of risk scoring analysis.

Fig 6 : Biometric market growth

6.1. Ethical and Privacy Concerns

The critical investigation of the broader implications of the development, deployment, and use of the artifacts, processes, or systems that are the focus of research and innovation is known as responsible research and innovation (RRI). This includes addressing ethical issues, addressing concerns about privacy, data governance, accountability, the digital divide, and how the recipients' views, approaches, and expectations might differ from the researchers, developers, and designers, and big data and AI-driven biometric authentication systems also bring ethical and privacy concerns that must be addressed contemporaneously as these systems develop. As organizations develop biometric systems such as fingerprints or facial recognition, they record and process sensitive personal information about users. Information that could be replicated or modified could be used to establish an individual's identity for malicious or unwanted purposes. Although current biometric systems are only based on geometric features of the face or iris, deep learning algorithms can also reconstruct images from predicted features. Possible re-identification and reconstruction attacks of biometric cryptosystems based on irreversible transformations of the biometrics may happen, resulting in privacy and security breaches. Various defenses, such as prototyping biometric cryptosystems where the transformation is not feasible from the security or mathematical theorem point of view, or using strategies such as destroying the features after the template matching, may be used to avoid the effective use of adversarial samples. There is a panel of experts concerned about how the massive personal data gathered in digitized societies is collected, managed, and protected as biobanks. The movement towards biobanks intended for biomedical research can raise several ethical and privacy issues surrounding consent,

ownership, responsibility, access, and commercialization of samples and data. At a general level, there is speculation about possible and potential abuses of biobanks, but the details concerning the uses of and problems surrounding data banking are less clear. As biometric systems are entrusted with unprecedented and possibly highly sensitive information on individuals, careful consideration of the ethical and social implications of such systems should take place, and forward-looking realistic solutions should be adopted through an international collaboration involving researchers, industry, governments, and civil society.

6.2. Advancements in Biometric Technologies

Recent advancements in biometric technologies are driving the evolution of intelligent biometric authentication. During the last decade, organizations amassed huge biometric and ambient data, which led to noise, drift, drift state, outlier, missing, and uncorrelated data leading to high false acceptances. Big data analytics have the potential to mitigate many of the challenges the biometric community is facing today. Artificial Intelligence (AI) can learn and interpret enormous volumes of biometric and ambient data of individuals giving insights on the behavior and biometric traits when fused can be used as countermeasures to mitigate an adversarial condition like spoofing. AI-driven biometrics with big data analytics can put forth reliable information about an individual in digital payment use cases and can constantly monitor biometric and ambient data for any divergence from learned information, creating autopilot with strong security control and fraud mitigation. The biometric sample data of an individual acquired today can independently put forth his/her unique behavioral attribute - a combination of language model, speech, vocal tract, rhythm, diction, tonality, noise robustness, behavioral COP1, etc, The ambient behavioral modality data of an individual can independently market the image of, his/her ambient - daily accumulating shifting pattern, sound acoustics, topological pattern, news and advertisement, demography, geographical location. An event-based approach with a fusion of Indian multiple-layer speech biometric and ambient behavioral patterns driven after extensive profiling of an individual can be put forth as a strong authentication during MID and transactions both with ambient and biometric sensing. AI-based machine learning can discover new usage making the biometric more future-proof.

7. Conclusion

This proposal demonstrates the innovative use of big data as a fraud mitigation solution in real-time digital payments. Due to the wide-ranging growth of online and smartphone payment systems, fraudulent transactions have greatly increased in each industry sector. The proposal contains the use and implementation methods of big data to mitigate fraud while making an online transaction, with real-time analysis on the machine by huge datasets collected across the industry. It simplifies the issue and helps customers regain fraudulently lost amounts within one minute of detection, integrating AI-driven biometric authentication into the already existing ID password or OTP-based transaction systems. So, fraudsters cannot bypass this biometric authentication without the transaction user's biometric identity. It also helps to identify transaction frauds in physical stores as it contains two fraud detection algorithms to check for invisible transaction frauds and money recovery based on a person's biometrics. Overall, it helps create more secure and trustworthy digital payment systems

across the industry.

7.1. Key Findings and Contributions

Various Technologies and Trends of Big Data and AI for Fraud Mitigation in Digital Payments

Digital payment fraud has become a severe threat to financial institutions and individuals' privacy in recent years. Billions of dollars lost due to fraudulent digital transactions compel mandate institutions to focus on implementing better security measures to protect customers. With the advent of Big Data technologies coupled with AI, there is a paradigm shift in designing and implementing fraud prevention systems to support Real-Time Fraud Mitigation on digital transactions. Unlike traditional methods that overly rely on expert-implemented rules, the proposed technology utilizes Big Data-enabled AI processes to extract complex transaction patterns and probabilistic models that support different digital transaction risks dynamically. Ultimately, the setup of advanced biometric systems is based on face, voice, body, and gait patterns/authentication, which provides real benefit to enhancing the security level of digital transactions. Moreover, these biometrics possess unmatched characteristics that cannot be lost or stolen compared to PINs and passwords. All key findings, innovations, and contributions in addressing this research goal based on AI and Big Data-enabled Biometric for Fraud Mitigation on digital payments are summarized and detailed as follows. Digital technologies and trends are being highly adopted globally compared to cash transactions due to their value-addition benefit. Digital payments provide convenience and time-saving solutions for both the entity/merchant and the end customer. However, the adoption of digital payments raises concerns about financial security. Digital payments are susceptible to various genuine requests, which leads digital transactions to vile activities such as money laundering, digital theft, terror funding, etc. Due to this hazardous effect, institutions are overwhelmed by the rapid digital transition of privacy concern requests in digital transactions. Unlike traditional applications for everyday facial verification and identification with limited resources, which almost exclusively depend on expert-designed methods, system designs focus on digital payment transaction analysis to address fraud activities on the same technology with the availability of unlimited computing. There is a current trend of utilizing Big Data and AI technologies and models, which have shown a promising result in addressing fraud detection in financial sectors and credit card transaction security. The Dynamic Adjusting Transaction Risk Model accurately assesses and monitors the risk level of each transaction after analyzing established patterns of past transactions, which adds essential support of an online metric for dynamic analysis of a transaction request's potential risk to existing technologies. In fraud detection and report technologies, multiple detection models of AI and statistical methodology with fraud impact analysis are employed. However, few technologies addressed the issue with a holistic view of Fraud Detection Risks and Frauds Enabling Analysis Models Specific to Digital Payments.

7.2. Implications for Industry and Research

With a huge data volume, especially when enhanced with state-of-the-art AI-driven biometric authentication systems, biometric data will be analyzed together with payment data on the same data platform. Continuous training of ML models with biometric data will

allow a flamboyant attack on spoofed biometrics and existing fraudsters with known biometric signatures. Fast-developing ML model training systems have made this feasible in the democratized era of cloud-based AA architecture and low-cost hardware. At the same time, it raises a large ethical and privacy concern on biometric data collection and storage, e.g. where and how biometric data is collected and stored or with access limitations to the data. Some standards might be necessary to help the unprepared payment platforms tackle this emerging business risk. In parallel, it also leaves some technical issues to solve for the payment platform development, e.g. how to provide transparency and explainability to AI-driven biometric systems. The presented novel approach will pave the way for the generation of new digital payment applications, e.g. a bit like a smart wellness life monitor. Owning and using biometric data, a digital payment system may analyze other life behavior-related data streams that come with digital payment transactions, e.g. customer health state. On the other side, it also gives individuals control of their digital life and money by anonymizing payment data and leaving the behavioral data mining and modeling task to hyper-scale payment platforms. Some preliminary implementation tests on the paid biometric dataset of 150 users have shown the feasibility of biometric-driven payment fraud mitigation. Nonetheless, the generated vast number of physical biometric signal raw data streams has motivated distributed and local data evaluation.

References

1. Pillai, S. E. V. S., Avacharmal, R., Reddy, R. A., Pareek, P. K., & Zanke, P. (2024, April). Transductive–Long Short-Term Memory Network for the Fake News Detection. In 2024 Third International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE) (pp. 1-4). IEEE.
2. Zanke, P., Deep, S., Pamulaparti Venkata, S., & Sontakke, D. Optimizing Worker's Compensation Outcomes Through Technology: A Review and Framework for Implementations.
3. Chintale, P., Deshmukh, H., & Desaboyina, G. Ensuring regulatory compliance for remote financial operations in the COVID-19 ERA.
4. Mahida, A. Secure Data Outsourcing Techniques for Cloud Storage.
5. Purshotam S Yadav. (2024). Optimizing Serverless Architectures for Ultra-Low Latency in Financial Applications. European Journal of Advances in Engineering and Technology. https://doi.org/10.5281/ZENODO.13627245
6. Vaka, D. K. Empowering Food and Beverage Businesses with S/4HANA: Addressing Challenges Effectively. J Artif Intell Mach Learn & Data Sci 2023, 1(2), 376-381.
7. Kommisetty, P. D. N. K., & Nishanth, A. (2024). AI-Driven Enhancements in Cloud Computing: Exploring the Synergies of Machine Learning and Generative AI. In IARJSET (Vol. 9, Issue 10). Tejass Publishers. https://doi.org/10.17148/iarjset.2022.91020
8. Avacharmal, R. (2024). Explainable AI: Bridging the Gap between Machine Learning Models and Human Understanding. Journal of Informatics Education and Research, 4(2).
9. Pamulaparti Venkata, S., & Avacharmal, R. (2023). Leveraging Interpretable Machine Learning for Granular Risk Stratification in Hospital Readmission: Unveiling Actionable Insights from Electronic Health Records. Hong Kong Journal of AI and Medicine, 3(1), 58-84.
10. Chintale, P., Korada, L., WA, L., Mahida, A., Ranjan, P., & Desaboyina, G. RISK MANAGEMENT STRATEGIES FOR CLOUD-NATIVE FINTECH APPLICATIONS DURING THE PANDEMIC.

11. Mahida, A., Chintale, P., & Deshmukh, H. (2024). Enhancing Fraud Detection in Real Time using DataOps on Elastic Platforms.
12. Kommisetty, P. D. N. K., & Abhireddy, N. (2024). Cloud Migration Strategies: Ensuring Seamless Integration and Scalability in Dynamic Business Environments. In International Journal of Engineering and Computer Science (Vol. 13, Issue 04, pp. 26146–26156). Valley International. https://doi.org/10.18535/ijecs/v13i04.4812
13. Yadav, P. S. (2024). Fast and Efficient UserID Lookup in Distributed Authentication: A Probabilistic Approach Using Bloom Filters. In the International Journal of Computing and Engineering (Vol. 6, Issue 2, pp. 1–16). CARI Journals Limited. https://doi.org/10.47941/ijce.2124
14. Vaka, D. K. "Artificial intelligence enabled Demand Sensing: Enhancing Supply Chain Responsiveness.
15. Avacharmal, R., Pamulaparthyvenkata, S., & Gudala, L. (2023). Unveiling the Pandora's Box: A Multifaceted Exploration of Ethical Considerations in Generative AI for Financial Services and Healthcare. Hong Kong Journal of AI and Medicine, 3(1), 84-99.
16. Kommisetty, P. D. N. K., & dileep, V. (2024). Robust Cybersecurity Measures: Strategies for Safeguarding Organizational Assets and Sensitive Information. In IJARCCE (Vol. 13, Issue 8). Tejass Publishers. https://doi.org/10.17148/ijarcce.2024.13832
17. Pamulaparti Venkata, S. (2023). Optimizing Resource Allocation For Value-Based Care (VBC) Implementation: A Multifaceted Approach To Mitigate Staffing And Technological Impediments Towards Delivering High-Quality, Cost-Effective Healthcare. Australian Journal of Machine Learning Research & Applications, 3(2), 304-330.
18. Chintale, P., & Desaboyina, G. (2018). FLUX: AUTOMATING CLUSTER STATE MANAGEMENT AND UPDATES THROUGH GITOPS IN KUBERNETES. International Journal of Innovation Studies, 2(2).
19. Mahida, A. (2024). Integrating Observability with DevOps Practices in Financial Services Technologies: A Study on Enhancing Software Development and Operational Resilience. International Journal of Advanced Computer Science & Applications, 15(7).
20. Yadav, P. S. (2024). Advanced Authentication and Authorization Mechanisms in Apache Kafka: Enhancing Security for High-Volume Data Processing Environments. In Journal of Engineering and Applied Sciences Technology (pp. 1–6). Scientific Research and Community Ltd. https://doi.org/10.47363/jeast/2024(6)e110
21. Vaka, D. K. " Integrated Excellence: PM-EWM Integration Solution for S/4HANA 2020/2021.
22. Kommisetty, P. D. N. K., vijay, A., & bhasker rao, M. (2024). From Big Data to Actionable Insights: The Role of AI in Data Interpretation. In IARJSET (Vol. 11, Issue 8). Tejass Publishers. https://doi.org/10.17148/iarjset.2024.11831
23. Avacharmal, R., Sadhu, A. K. R., & Bojja, S. G. R. (2023). Forging Interdisciplinary Pathways: A Comprehensive Exploration of Cross-Disciplinary Approaches to Bolstering Artificial Intelligence Robustness and Reliability. Journal of AI-Assisted Scientific Discovery, 3(2), 364-370.
24. Pamulaparti Venkata, S., Reddy, S. G., & Singh, S. (2023). Leveraging Technological Advancements to Optimize Healthcare Delivery: A Comprehensive Analysis of Value-Based Care, Patient-Centered Engagement, and Personalized Medicine Strategies. Journal of AI-Assisted Scientific Discovery, 3(2), 371-378.
25. Chintale, P., Khanna, A., Korada, L., Desaboyina, G., & Nerella, H. AI-Enhanced Cybersecurity Measures for Protecting Financial Assets.
26. Kommisetty, P. D. N. K., & Nishanth, A. (2024). AI-Driven Enhancements in Cloud Computing: Exploring the Synergies of Machine Learning and Generative AI. In IARJSET (Vol. 9, Issue 10). Tejass Publishers. https://doi.org/10.17148/iarjset.2022.91020
27. Mahida, A. Explainable Generative Models in FinCrime. J Artif Intell Mach Learn & Data Sci

2023, 1(2), 205-208.
28. Yadav, P. S. (2023). Enhancing Software Testing with AI: Integrating JUnit and Machine Learning Techniques. North American Journal of Engineering Research, 4(1).
29. Vaka, D. K. (2020). Navigating Uncertainty: The Power of 'Just in Time SAP for Supply Chain Dynamics. Journal of Technological Innovations, 1(2).
30. Avacharmal, R., Gudala, L., & Venkataramanan, S. (2023). Navigating The Labyrinth: A Comprehensive Review Of Emerging Artificial Intelligence Technologies, Ethical Considerations, And Global Governance Models In The Pursuit Of Trustworthy AI. Australian Journal of Machine Learning Research & Applications, 3(2), 331-347.
31. Mandala, V. (2024). Revolutionizing Automotive Supply Chain: Enhancing Inventory Management with AI and Machine Learning. Universal Journal of Computer Sciences and Communications, 10-22.
32. Kommisetty, P. D. N. K. (2022). Leading the Future: Big Data Solutions, Cloud Migration, and AI-Driven Decision-Making in Modern Enterprises. Educational Administration: Theory and Practice, 28(03), 352-364.
33. Perumal, A. P., & Chintale, P. Improving operational efficiency and productivity through the fusion of DevOps and SRE practices in multi-cloud operations.
34. Mahida, A. (2023). Enhancing Observability in Distributed Systems-A Comprehensive Review. Journal of Mathematical & Computer Applications. SRC/JMCA-166. DOI: doi. org/10.47363/JMCA/2023 (2), 135, 2-4.
35. Yadav, P. S. REAL-TIME INSIGHTS IN DISTRIBUTED SYSTEMS: ADVANCED OBSERVABILITY TECHNIQUES FOR CLOUD-NATIVE ENTERPRISE ARCHITECTURES.
36. Dilip Kumar Vaka. (2019). Cloud-Driven Excellence: A Comprehensive Evaluation of SAP S/4HANA ERP. Journal of Scientific and Engineering Research. https://doi.org/10.5281/ZENODO.11219959.
37. Yadav, P. S. (2023). Leveraging Artificial Intelligence and Machine Learning for Anomaly Detection in Financial Investment Regulatory Reporting. European Journal of Advances in Engineering and Technology, 10(12), 67-72.
38. Manavadaria, M. S., Mandala, V., Surabhi, S. N. R. D., Manoharan, S., Gupta, R., & Londhe, P. M. (2024, July). Smart City Traffic Monitoring and Control: Integrating Wireless Sensors with KNN-TCGAN Model. In 2024 International Conference on Data Science and Network Security (ICDSNS) (pp. 1-6). IEEE.