AI IN COMBATING FRAUD AND IMPROVING CUSTOMER SERVICE IN UZBEK BANKS

Namozova Maftuna Utkirovna
Tashkent State Economic University 3rd year, group BIA-40
namozova.maftuna2004@gmail.com

Abstract: *This thesis explores the transformative impact of Artificial Intelligence (AI) on fraud detection and customer service within the commerce and service sectors. With the advent of advanced technologies, AI has emerged as a pivotal force, employing machine learning algorithms, natural language processing, and advanced analytics to address the dual challenges of fraud and customer interaction. This study delves into the capabilities of AI to parse extensive datasets, pinpoint anomalies, and customize interactions in real-time, thereby enhancing fraud detection mechanisms and elevating customer service experiences.*

Keywords: *artificial intelligence (AI), fraud detection, customer service, machine learning algorithms, natural language processing, advanced analytics, real-time data analysis, anomaly detection, personalization of interactions, commerce and service sectors, ethical considerations of AI, predictive analytics, behavioral analysis, financial transactions, identity theft, e-commerce security, insurance fraud, credit card fraud, phishing scams, cybersecurity.*

In the modern landscape of commerce and service provision, the twin imperatives of fraud detection and customer service are paramount. Fraud, in its myriad forms, poses a pervasive threat to economic stability and consumer trust, while exemplary customer service stands as a linchpin for brand loyalty and sustainable growth. However, traditional methods for addressing these challenges often fall short in the face of evolving threats and increasing customer expectations.

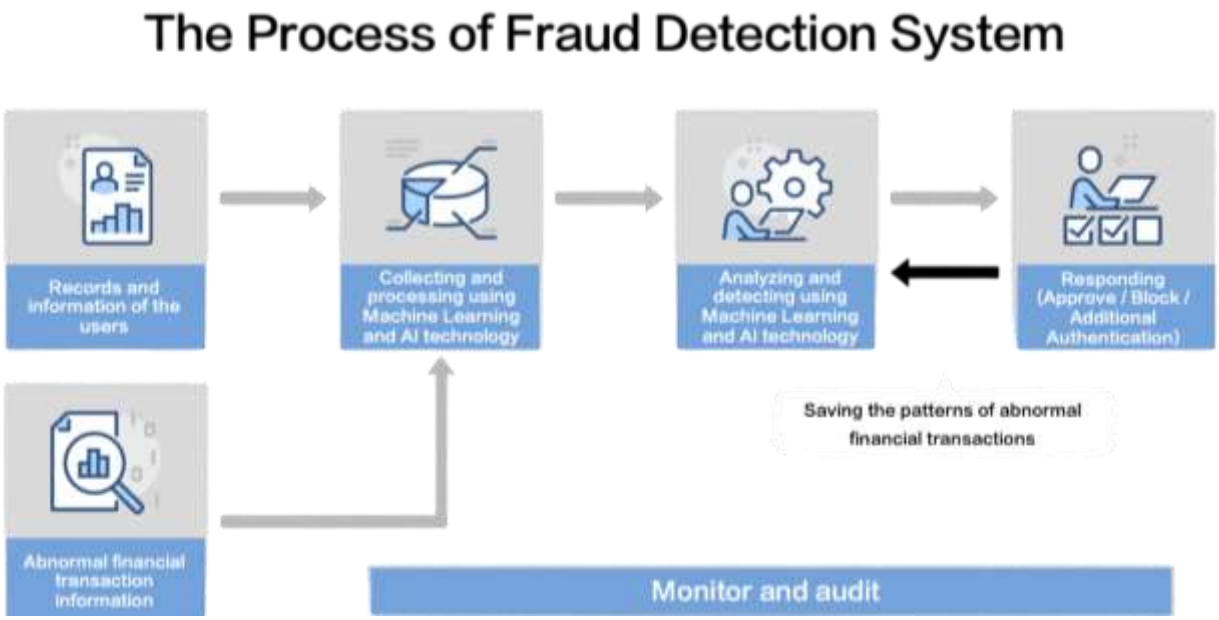
Enter Artificial Intelligence (AI), heralded as a game-changer in the realms of fraud detection and customer service. Leveraging machine learning algorithms, natural language processing, and advanced analytics, AI offers unparalleled capabilities to analyze vast datasets, detect anomalies, and personalize customer interactions in real-time. This thesis examines the intersection of AI, fraud detection, and customer service, exploring its transformative potential, practical applications, and ethical considerations. Through a blend of theoretical analysis and real-world case studies, we aim to elucidate the opportunities and challenges inherent in deploying AI solutions, ultimately contributing to a deeper understanding of AI's role in safeguarding businesses and enhancing customer experiences.

Fraud manifests in various guises across sectors such as banking, insurance, and e-commerce, presenting unique challenges to traditional detection methods. In banking, fraudulent activities encompass identity theft, account takeover, and credit card fraud,

while insurance fraud spans false claims, staged accidents, and premium diversion schemes. E-commerce faces threats from unauthorized transactions, phishing scams, and counterfeit goods. Traditional fraud detection methods often struggle to keep pace with the sophistication and scale of modern fraud schemes, relying on manual reviews, rules-based systems, and historical data analysis, which are prone to inefficiencies, false positives, and lag times.

Enter Artificial Intelligence (AI) as a potent ally in the fight against fraud. AI empowers organizations with predictive analytics, anomaly detection, and behavioral analysis capabilities that augment and enhance traditional fraud detection methods. Machine learning algorithms can sift through vast datasets in real-time, identifying subtle patterns and anomalies indicative of fraudulent activity. Moreover, AI-driven systems continuously adapt and evolve, learning from new data and emerging threats to stay one step ahead of fraudsters. By leveraging AI's advanced capabilities, businesses can fortify their defenses, mitigate financial losses, and safeguard the trust of their stakeholders in an increasingly digital landscape.

One of the biggest features of FDS is that AI technology is applied to realize higher effects in the information collection process, analysis and detection process.



FDS is structured and operated in the following way:

1) Collecting and Processing the Information: The initial phase involves gathering and processing data from the user's financial transaction device. Through refinement and quantitative reduction, the data is prepared for subsequent stages, with machine learning employed for efficient data processing.

2) Analyzing and Detecting: Following data processing, the system proceeds to analyze the information and detect irregular transactions by scrutinizing past financial transaction data and identifying patterns of abnormal activity. Various AI analysis

methods, including deep learning for hybrid detection and identifying data misuse, are utilized in this phase.

3) Responding: Upon detecting abnormal transactions, the system initiates additional authentication procedures for transaction approval or blocking. Furthermore, it accumulates data and notifies both administrators and users about the detected anomalies.

4) Monitoring and Auditing: This phase involves continuous monitoring of the entire Fraud Detection System process to ensure its effectiveness and integrity.

Financial fraud prevention through Fraud Detection Systems (FDS) has seen notable successes, with examples like PayPal leveraging AI to analyze billions of transactions and enhance detection accuracy while reducing false positives. However, challenges arise from varying implementation methods and system inadequacies among different financial institutions. The emergence of cryptocurrency further underscores the need for robust FDS solutions, as seen in Cobit's recent use to prevent phishing attacks, highlighting AI's pivotal role in bolstering security measures.

While AI-driven FDS significantly improves security in electronic transactions, collaboration among financial entities is crucial to combatting evolving fraud techniques effectively. By sharing detected information and methodologies, FDS becomes a potent tool against sophisticated hacking attempts across sectors. Moreover, alongside technological advancements, fostering individual security awareness among transaction participants complements institutional security measures, ultimately reducing the potential for phishing-related losses.

REFERENCES:

1. Fraud Detection System (FDS) with AI Technology | Penta Security https://www.pentasecurity.com/blog/fraud-detection-system-fds-with-ai-technology/

2. Fraud Detection Using AI In Banking – Youverify https://youverify.co/blog/fraud-detection-using-ai-in-banking

3. datadome.co https://datadome.co/learning-center/ai-fraud-detection/

4. Artificial intelligence in fraud detection – Wikipedia https://en.wikipedia.org/wiki/Artificial_intelligence_in_fraud_detection

5. Artificial Intelligence - How it's used to detect financial fraud | Fraud.com https://www.fraud.com/post/artificial-intelligence