UDK 004.4

IMPROVEMENT PAYMENT SYSTEMS USING AI TECHNOLOGY

Oleh Poliarush[1], Svitlana Krepych[2], Iryna Spivak[3]
West Ukrainian National University
[1]phd. student, [2-3] associate professor

I. Problem definition

Traditional payment systems often rely on rule-based algorithms and static methods to detect fraudulent activities. Fraudsters continually evolve their tactics, making it challenging for rule-based systems to keep up with emerging threats. Identity theft, phishing attacks, and account takeovers are common methods employed by fraudsters to exploit vulnerabilities in traditional systems.

II. Goal

Integrating AI into payment systems allows for a dynamic approach to fraud detection and prevention. Machine learning algorithms can analyze historical transaction data, identifying patterns indicative of fraudulent activities. By continuously learning from new data, AI systems adapt and evolve, providing a robust defense against emerging threats. This real-time analysis ensures a proactive response to potential security breaches, safeguarding the integrity of the payment ecosystem.

III. The main part

Traditional fraud detection methods often rely on rule-based systems and manual reviews to identify potentially fraudulent activities. In these systems, predefined rules and thresholds are set based on historical data and known patterns of fraudulent behavior. Automated alerts are triggered when transactions deviate from these established rules, prompting further investigation. Additionally, human analysts play a crucial role in reviewing flagged transactions, manually assessing patterns, and making decisions based on their expertise. While these approaches have been effective to some extent, they can be time-consuming, prone to human error, and struggle to adapt quickly to evolving fraud tactics. As fraudsters become more sophisticated, the limitations of rule-based systems become evident, highlighting the need for more advanced and adaptive technologies, such as artificial intelligence, to bolster fraud detection capabilities.

Commonly most of the systems require complex solutions which could achieve a high level of precision, especially in payment systems. To achieve reliability and accuracy of the prediction we use such AI models like:

- Isolation Forest: Anomaly detection algorithm that excels in isolating and identifying outliers within a dataset. It operates by recursively partitioning the data, randomly selecting features, and creating isolation trees to isolate instances that deviate from the norm. In fraud detection, the Isolation Forest algorithm is particularly effective at detecting unusual patterns associated with fraudulent transactions. By leveraging the concept that anomalies are typically isolated more quickly in random partitions, Isolation Forest offers a scalable and efficient solution for identifying potential fraudulent behavior in financial datasets.
- Logistic Regression: Statistical model commonly used for binary classification tasks by modeling the relationship between input variables and the log-odds of the outcome, logistic regression provides a straightforward and interpretable way to assess the likelihood of fraudulent behavior in financial transactions.
- Autoencoders: Neural network architecture used in unsupervised learning, particularly for dimensionality reduction and feature learning. Consisting of an encoder and decoder, autoencoders aim to reconstruct input data within the network, learning a compact representation of the data in the process. In the context of fraud detection, autoencoders can be employed to capture intricate patterns and anomalies in transaction data, offering a powerful tool for identifying subtle deviations from normal behavior that may indicate fraudulent activity.

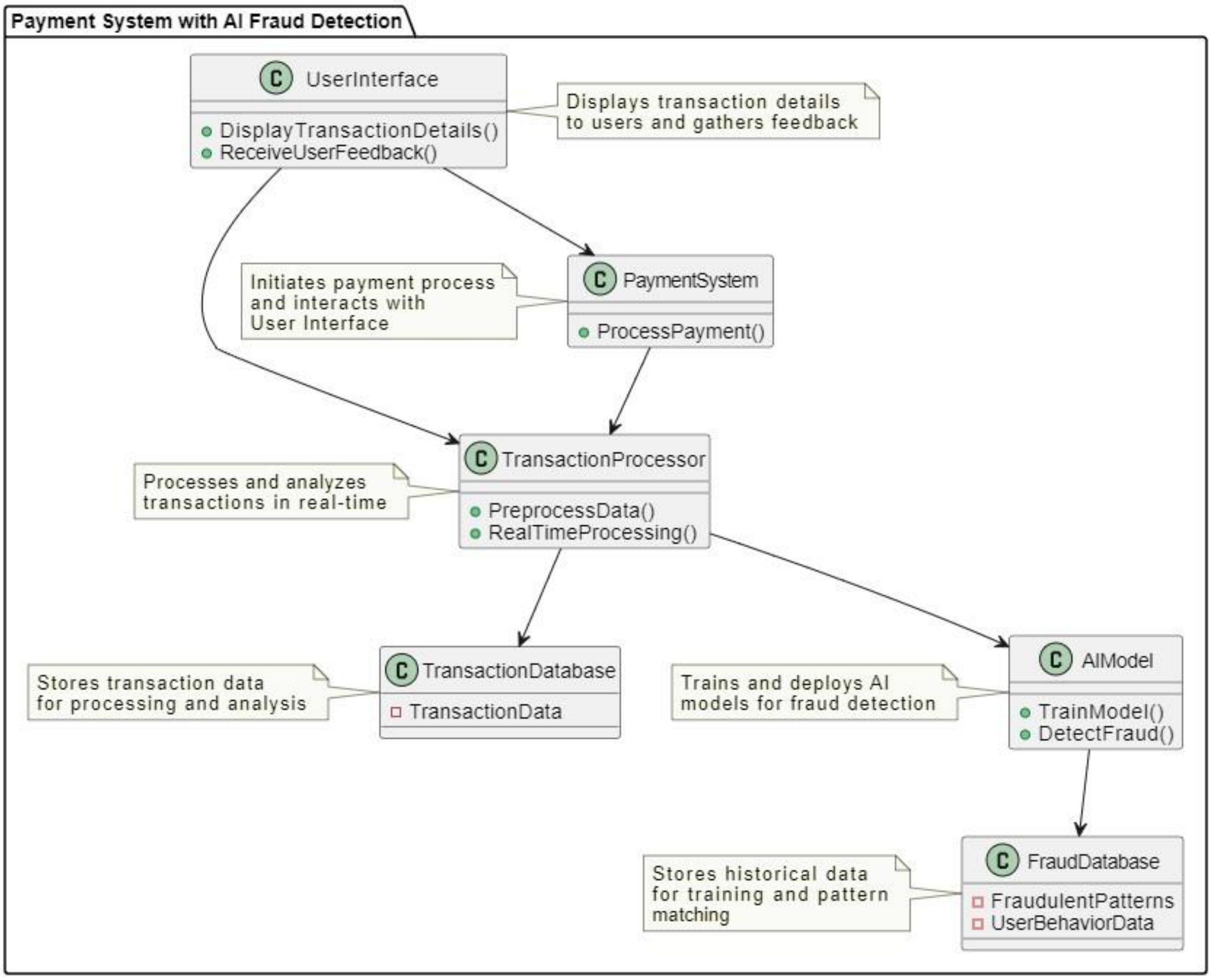

Figure 1 – Calls diagram of Fraud AI usage.

IV. Conclusion

The integration of AI technologies presents a unique opportunity to elevate existing payment systems to new heights. By leveraging the power of machine learning, biometric authentication, predictive analytics, and smart automation, businesses can enhance security, streamline operations, and provide a personalized and efficient payment experience. Embracing these advancements is not just a means of staying competitive; it is a pathway to redefining the future of payment systems. As we continue to innovate, the fusion of AI and payment systems will undoubtedly shape a more secure, efficient, and user-centric financial landscape.

References

1. Sanzharovskyi A. and Yurchyshyn V. “A modified method of detecting fake news based on machine learning algorithms”, Bulletin of the Cherkasy State Technological University, Vol. 2, 2023. – pp.58–70
2. Guven Z.A., “Comparison of BERT models and machine learning methods for sentiment analysis on Turkish Tweets”, in 6th International Conference on Computer Science and Eng.(UBMK), 2021. – pp.98–101
3. S. Krepych, I.Spivak. “Forecasting system of utilities service costs based on neural network”, Advanced Information Systems, Vol.4, No.4, 2020. – pp.102-108
4. S. Krepych, I.Spivak, S,Spivak. “Approach to forecasting of utility costs using neural networks”, in 15th International Conference on Computer Sciences and Information Technologies (CSIT). 2020. – pp.387-391
5. Darouich A., Khoukhi F.and Douzi K. “A dynamic learning content pattern for adaptive learning environment”, in 10th International Conference on Intelligent Systems: Theories and Applications (SITA), 2015. pp.1–6
6. S. Krepych, I.Spivak. “Improvement od SVD algorithm to increase the efficiency of recommendation systems”, Advanced Information Systems, Vol.5, No.4, 2021. – pp.55-59
7. Smith J. and Johnson A. "Advancements in AI for Financial Security." Journal of Technology and Finance, 15(2),2021. pp.45-62.
8. Brown L. and Garcia M. "Biometric Authentication: A Comprehensive Review." International Conference on Cybersecurity and Privacy, Proceedings,2022. – pp.112-125.
9. White S. and Davis R. "Machine Learning Applications in Fraud Detection: A Comparative Analysis." Journal of Financial Technology, 8(4), 2020. – pp.78-93.