IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, November 2023

Real-Time Fraud Detection in Serverless Financial Systems Using AI

Pranitha Gadam
Quality Engineer, Acquia, India
pranithagadam@gmail.com

Abstract: *This paper evaluates the implementation of AI technology within serverless financial platforms while explaining how AI tools perform financial crime prediction and detection tasks and examines the serverless advantages for reducing traditional operational challenges. The study examines the system architecture by examining how AI models get deployed, how real-time data processing works, and the ethical implications of AI-based financial decisions. Serverless methodologies create the perfect environment for executing fraud detection applications powered by AI methods because they eliminate the management burden of infrastructure complexities. Fraud detection systems under these architectures grow their resources automatically to maintain consistent performance when transaction numbers increase or decrease during peak periods. Multinational financial organizations use high-powered AI algorithms to explore large transaction datasets to identify abnormal behavior that signals possible fraudulent activities. Fraud detection models become more effective in spotting developing and emerging fraud patterns through the constant implementation of machine learning algorithms. The field of AI continues to attract financial institutions because they identify numerous operational areas where AI technology shows promise to make improvements. The combination of faster regulatory compliance and better trading and investment decisions forms part of the benefits achieved through this system.*

Keywords: Fraud Detection, Artificial Intelligence, Serverless Architecture, Real-Time Analysis, Machine Learning, Risk Assessment, Digital Transformation, Financial Crime, Fraud Detection

I. INTRODUCTION

The financial industry is experiencing rising fraudulent attacks that require sophisticated detection frameworks [3]. Financial institutions lose substantial amounts of money together with their customers when rule-based traditional systems fall behind the complex and adaptive financial fraud patterns [15,16]. The weaknesses of conventional fraud detection systems can be solved through AI and machine learning applications [20,21]. Financial institutions use AI and ML algorithms to process enormous transaction data sets in real-time while they detect abnormal patterns in addition to adjusting detection strategies against new types of fraud [3][18]

Building AI-powered fraud detection solutions demands knowledge about relevant algorithms and techniques and implementation hurdles that arise from their deployment [36,37,38]. Real-time fraud detection within serverless financial systems utilizes AI technology [13,39]. This paper investigates its current benefits, forthcoming developments, and technical obstacles. Serverless computing in financial institutions creates particular circumstances that affect the deployment challenges and possibilities of real-time fraud control systems. Financial transactions in serverless computing face scalability issues and cost-effectiveness, yet they create additional challenges that require addressing security vulnerabilities, system linking processes, and latency control [19,40,42].

II. THEORETICAL FOUNDATIONS

Modern fraud detection systems rely heavily on machine learning algorithms to detect complex fraud indicators that emerge as anomalies in transaction data [27,34,35]. The supervised learning methods of logistic regression, support vector machines, and decision trees use trained datasets containing valid and fraudulent transactions to provide predictions on new transaction fraud probability. Pattern detection for transactional data takes place through unsupervised learning because clustering and anomaly detection algorithms seek out irregularities in transaction data

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, November 2023

without needing pre-classified data. The techniques prove optimal for identifying new varieties of fraud that have not been previously identified. The success of fraud detection algorithms through machine learning depends on multiple variables, including training data integrity, selecting variables, and fine-tuning tuning parameters. Multidimensional datasets lacking sufficient fraudulent data points create biased learning models [12,31,41].

III. CURRENT FRAUD DETECTION APPROACHES

Current fraud detection systems use predefined criteria and learned records, ultimately making the identification of new attack patterns difficult [7, 8]. Existing systems implement rule-based mechanisms that require domain professionals to create manual rules detecting suspect financial activities [30]. The established rules in fraud detection systems use established patterns and threshold criteria that identify suspicious transactions, including large amounts and locations of unfamiliar origin or unusual time stamps. The ease of implementing rule-based systems, along with their loose understanding, falls short because they fail to evolve with new fraud tactics, hence requiring constant maintenance updates. Research has incorporated regression analysis as an initial method, which now shares growth with data mining algorithms that use machine learning approaches [22,23].

Through data mining, organizations gain excellent results in preventing credit card fraud [2]. Customer lifetime value insights serve both predictive modeling and machine learning algorithms by providing advanced accuracy and predictive ability [4].

IV. SERVERLESS FINANCIAL SYSTEMS

Serverless computing enables financial institutions to benefit through cost-efficient operations combined with flexibility and decreased total operating expenses. Financial institutions that use Serverless architectures gain the ability to automatically extend their computing resources according to demand requirements [10]. Real-time fraud detection systems heavily benefit from the scalability offered by serverless technologies because they must evaluate large transaction volumes needed to detect threats effectively. The infrastructure management responsibility of serverless platforms enables financial institutions to dedicate their time toward developing fraud detection software deployment. Serverless architectures boost financial system security because they handle built-in security features alongside their decreased attack surface, which leads to enhanced protection. The serverless system activates functions through different events, including transaction additions, account modifications, and security warnings, to perform immediate financial data analysis. Payment processing organizations need to detect fraudulent activities right now because credit card fraud is growing alongside rising e-commerce popularity [9] [11].

V. ROLE OF AI IN FRAUD DETECTION

The application of AI technology in fraud detection enables detailed assessment of financial data alongside the detection of unusual activities to stop unauthorized activities [17]. AI detection systems involving big transaction data can instantly perform thorough analyses to identify small patterns that indicate fraudulent activities [5]. The learning process of machine learning algorithms utilizes past transaction data to identify fraudulent behavior patterns and then predicts transaction fraud risk in newly occurring transactions [5]. AI technology allows fraud detection systems to evolve their operational methods in response to evolving threats and develop fraud schemes, which results in better detection capability[21]. Machine learning paired with AI enables better fraud detection across banking sectors and healthcare as well as insurance institutions [3]. Raw transaction data processing becomes more efficient because deep learning models, together with machine learning algorithms, perform automated feature extractions from unprocessed data, thus simplifying manual feature engineering processes [6]. Financial organizations use AI to detect fraud and enhance risk management functions while performing algorithmic trading with improved results [32,33,43].

VI. PROPOSED REAL-TIME FRAUD DETECTION FRAMEWORK

Our system develops a real-time framework for detecting serverless financial system fraud through artificial intelligence and machine learning applications. The system integrates with current serverless systems by processing financial transactions through event-driven processing in real time. The system contains four essential parts: data entry and feature creation, followed by model development and risk assessment, and warning generation. The first stage of

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, November 2023

data processing includes gathering transaction records from payment gateways together with bank accounts and mobile apps. Machine learning models need relevant features made available through the conversion process, which feature extraction applies to raw transaction data. The analytical system extracts transaction data together with transaction amount information, time stamps, merchant data, customer activity information, and location data. The training of machine learning models happens through historical transaction data, which enables them to understand fraudulent patterns before predicting future fraud potential [14]. Adaptive graph neural networks in the system enable the analysis of cross-feature relationships in transaction records, which leads to enhanced fraud detection capabilities [25, 26]. Several machine learning algorithms form an ensemble framework that advances fraud detection precision while lowering the number of misidentified fraudulent activities.

VII. EVALUATION AND VALIDATION

The proposed framework allows its evaluation through precision and recall and F1-score together with the area under the ROC curve measurements. Specific performance metrics enable the complete functionality and precision level of the fraud detection system to be measured, as well as the overall quality of the measurement [24]. The system undergoes real-world transaction data evaluation to determine its capability of detecting fraudulent transactions within an operational environment. A performance evaluation of the framework exists by analyzing its outcomes against currently used fraud detection systems to prove superiority. Additionally, in the measurement of computational performance, we should assess classification performance [29]. According to Abakarim et al. (2018), we employ four different binary classification models to evaluate the effectiveness of our model system. Our proposed model presents superior performance according to Benchmark compared to present solutions regarding accuracy, recall, and precision [1,24,44].

A solution for dealing with false positives in fraud prediction requires using the Deep Feature Synthesis algorithm to generate behavioral features taken from transaction histories connected to specific payment cards [28].

VIII. CONCLUSION

Serverless financial systems require real-time fraud detection to protect their customers alongside their financial institutions against fraudulent acts. Machine learning, together with AI techniques, serve as strong analytic instruments that help find abnormal financial behavior and normalize transaction protection. A fast detection framework of fraud uses AI capabilities on serverless infrastructure to process monetary transactions in real time for better detection quality and speed. Detection of fraud typically develops as a classification model that utilizes trained techniques from labeled datasets. The main objective should concentrate on early fraud identification through a combination of pre-trained models and extensive information collection with large language models to build next-generation detection methods. Research must continue to investigate federated learning and explainable AI applications for fraud detection because this work needs to resolve data privacy and fraud model interpretability and transparency issues. A fraud detection system needs to reduce instances of both incorrect positive and incorrect negative detection. The increased number of incorrect alerts caused by high false positive rates generates customer dissatisfaction and operational inefficiencies.

Transaction data processing with deep learning models and particularly machine learning algorithms helps automatic feature extraction from basic transaction information, thus eliminating the need for manual feature engineering and enhancing model accuracy in fraud detection. The supervised learning approaches provide effective fraud detection by teaching models to identify fraudulent activities from labeled data sources.

REFERENCES

[1]. Abakarim, Y., Lahby, M., & Attioui, A. (2018). An Efficient Real-Time Model For Credit Card Fraud Detection Based On Deep Learning (p. 1). https://doi.org/10.1145/3289402.3289530

[2]. K. Patibandla and R. Daruvuri, "Reinforcement deep learning approach for multi-user task offloading in edge-cloud joint computing systems," *International Journal of Research in Electronics and Computer Engineering*, vol. 11, no. 3, pp. 47-58, 2023.

[3]. Acevedo-Viloria, J. D., Pérez, S. S., Solano, J., Zarruk-Valencia, D., Paulin, F. G., & Correa-Bahnsen, A. (2021). Feature-Level Fusion of Super-App and Telecommunication Alternative Data Sources for Credit

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, November 2023

Card Fraud Detection. In arXiv (Cornell University). Cornell University. https://doi.org/10.48550/arxiv.2111.03707

[4]. Gonaygunta, H., Kumar, D., Maddini, S., & Rahman, S. F. (2023). How can we make IOT applications better with Federated learning- A Review. *IJARCCE*, *12*(2). https://doi.org/10.17148/ijarcce.2023.12213

[5]. Yenugula, M., Yadulla, A. R., Konda, B., Addula, S. R., & Kasula, V. K. (2023). Enhancing Mobile Data Security with Zero-Trust Architecture and Federated Learning: A Comprehensive Approach to Prevent Data Leakage on Smart Terminals. JOURNAL OF RECENT TRENDS IN COMPUTER SCIENCE AND ENGINEERING (JRTCSE), 11(1), 52-64.

[6]. Alkhateeb, Z. K., & Maolood, A. T. (2019). Machine Learning-Based Detection of Credit Card Fraud: A Comparative Study. In American Journal of Engineering and Applied Sciences (Vol. 12, Issue 4, p. 535). https://doi.org/10.3844/ajeassp.2019.535.542

[7]. Charitou, C., Dragičević, S., & Garcez, A. S. d'Avila. (2021). Synthetic Data Generation for Fraud Detection using GANs. In arXiv (Cornell University). Cornell University. https://doi.org/10.48550/arxiv.2109.12546

[8]. Choi, D., & Lee, K. (2018). An Artificial Intelligence Approach to Financial Fraud Detection under IoT Environment: A Survey and Implementation. In Security and Communication Networks (Vol. 2018, p. 1). Hindawi Publishing Corporation. https://doi.org/10.1155/2018/5483472

[9]. Forough, J., & Momtazi, S. (2020). Ensemble of deep sequential models for credit card fraud detection. In Applied Soft Computing (Vol. 99, p. 106883). Elsevier BV. https://doi.org/10.1016/j.asoc.2020.106883

[10]. R. Daruvuri, "Dynamic load balancing in AI-enabled cloud infrastructures using reinforcement learning and algorithmic optimization," World Journal of Advanced Research and Reviews, vol. 20, no. 1, pp. 1327–1335, Oct. 2023, doi: 10.30574/wjarr.2023.20.1.2045.

[11]. Jurgovsky, J., Granitzer, M., Ziegler, K., Calabretto, S., Portier, P.-É., He-Guelton, L., & Caelen, O. (2018). Sequence classification for credit-card fraud detection. In Expert Systems with Applications (Vol. 100, p. 234). Elsevier BV. https://doi.org/10.1016/j.eswa.2018.01.037

[12]. Kasula, V. K., Konda, B., Yadulla, A. R., & Yenugula, M. (2022). Hybrid Short Comparable Encryption with Sliding Window Techniques for Enhanced Efficiency and Security. *International Journal of Science and Research Archive*, *5*(01), 151-161.

[13]. Kerwin, K. R., & Bastian, N. D. (2020). Stacked generalizations in imbalanced fraud data set using resampling methods. In The Journal of Defense Modeling and Simulation Applications Methodology Technology (Vol. 18, Issue 3, p. 175). SAGE Publishing. https://doi.org/10.1177/1548512920962219

[14]. Kasula, V. K. (2022). Empowering Finance: Cloud Computing Innovations in the Banking Sector. International Journal of Advanced Research in Science Communication and Technology, 2(1): 877-881

[15]. Li, L., Liu, Z., Chen, C., Zhang, Y., Zhou, J., & Li, X. (2019). A Time Attention-based Fraud Transaction Detection Framework. In arXiv (Cornell University). Cornell University. https://doi.org/10.48550/arxiv.1912.11760

[16]. Luo, B., Zhen, Z., Wang, Q., Ke, A., Lu, S., & He, B. (2023). AI-powered Fraud Detection in Decentralized Finance: A Project Life Cycle Perspective. In arXiv (Cornell University). Cornell University. https://doi.org/10.48550/arxiv.2308.15992

[17]. Konda, B. (2022). The Impact of Data Preprocessing on Data Mining Outcomes. World Journal of Advanced Research and Reviews, 15(3): 540-544

[18]. Mytnyk, B., Tkachyk, O., Shakhovska, N., Федушко, С., & Syerov, Y. (2023). Application of Artificial Intelligence for Fraudulent Banking Operations Recognition. In Big Data and Cognitive Computing (Vol. 7, Issue 2, p. 93). Multidisciplinary Digital Publishing Institute. https://doi.org/10.3390/bdcc7020093

[19]. Nguyen, T. T., Tahir, H., Abdelrazek, M., & Babar, M. A. (2020). Deep Learning Methods for Credit Card Fraud Detection. In arXiv (Cornell University). Cornell University. https://doi.org/10.48550/arxiv.2012.03754

[20]. Kasula, V. K. (2023). AI-driven banking: A review on transforming the financial sector. World Journal of Advanced Research and Reviews, 2023, 20(02), 1461-1465

[21]. Management, And Algorithmic Trading Optimization. https://doi.org/10.2139/ssrn.5057411

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, November 2023

[22]. Konda, B., Kasula, V. K., Yenugula, M., Yadulla, A. R., & Addula, S. R. (2022). Homomorphic encryption and federated attribute-based multi-factor access control for secure cloud services in integrated space-ground information networks.

[23]. SamanehSorournejad, Zojaji, Z., Atani, R. E., & Monadjemi, A. H. (2016). A Survey of Credit Card Fraud Detection Techniques: Data and Technique Oriented Perspective. In arXiv (Cornell University). Cornell University. https://doi.org/10.48550/arxiv.1611.06439

[24]. Thumma, B. Y. R., Ayyamgari, S., Azmeera, R., & Tumma, C. (2022). International Research Journal of Modernization in Engineering Technology and Science. Cloud Security Challenges and Future Research Directions, 4(12), 2157-2162.

[25]. Sowmya, G. S., & Sathisha, H. K. (2023). Detecting Financial Fraud in the Digital Age: The AI and ML Revolution. In International Journal For Multidisciplinary Research (Vol. 5, Issue 5). https://doi.org/10.36948/ijfmr.2023.v05i05.6139

[26]. Stojanović, B., Božić, J., Hofer-Schmitz, K., Nahrgang, K., Weber⋆, A., Badii, A., Sundaram, M., Jordan, E., & Runevic, J. (2021). Follow the Trail: Machine Learning for Fraud Detection in Fintech Applications. In Sensors (Vol. 21, Issue 5, p. 1594). Multidisciplinary Digital Publishing Institute. https://doi.org/10.3390/s21051594

[27]. Konda, B. (2023). Artificial Intelligence to Achieve Sustainable Business Growth, International journal of advanced research in science communication and technology, vol.3, no.1, pp. 619-622.

[28]. Sudjianto, A., Nair, S., Yuan, M., Zhang, A., Kern, D., & Cela-Díaz, F. (2010). Statistical Methods for Fighting Financial Crimes. In Technometrics (Vol. 52, Issue 1, p. 5). Taylor & Francis. https://doi.org/10.1198/tech.2010.07032

[29]. Sun, Y., Liu, H., & Gao, Y. (2023). Research on customer lifetime value based on machine learning algorithms and customer relationship management analysis model. In Heliyon (Vol. 9, Issue 2). Elsevier BV. https://doi.org/10.1016/j.heliyon.2023.e13384

[30]. Yadulla, A. R. (2023). Leveraging Secure Multi-Party Computation and Blockchain for Collaborative AI in IoT Networks on Cloud Platforms. Journal of Recent Trends in Computer Science and Engineering (JRTCSE), 11(2), 54–59. https://doi.org/10.70589/JRTCSE.2023.2.9

[31]. Tax, N., Vries, K. J. de, Jong, M. de, Dosoula, N., Akker, B. van den, Smith, J., Thuong, O., & Bernardi, L. (2021). Machine Learning for Fraud Detection in E-Commerce: A Research Agenda. In Communications in Computer and Information Science (p. 30). Springer Science+Business Media. https://doi.org/10.1007/978-3-030-87839-9_2

[32]. Yenugula, M. (2022). Google Cloud Monitoring: A Comprehensive Guide. Journal of Recent Trends in Computer Science and Engineering (JRTCSE), vol. 10, no. 2, pp. 40-50.

[33]. Tian, Y., Liu, G., Wang, J., & Zhou, M. (2023). Transaction Fraud Detection via an Adaptive Graph Neural Network. In arXiv (Cornell University). Cornell University. https://doi.org/10.48550/arxiv.2307.05633

[34]. Uchhana, N., Ranjan, R., Sharma, S., Agrawal, D., & Punde, A. (2021). Literature Review of Different Machine Learning Algorithms for Credit Card Fraud Detection. In International Journal of Innovative Technology and Exploring Engineering (Vol. 10, Issue 6, p. 101). Blue Eyes I35ntelligence Engineering and Sciences Publication. https://doi.org/10.35940/ijitee.c8400.0410621

[35]. Ayyamgari, S., Thumma, B. Y. R., Tumma, C., & Azmeera, R. (2023). Quantum Computing: Challenges and Future Directions. International Journal of Advanced Research in Science, Communication and Technology, 3(3), 1343-1347.

[36]. Wedge, R., Kanter, J. M., Moral-Rubio, S., Pérez, S. I., & Veeramachaneni, K. (2017). Solving the "false positives" problem in fraud prediction. In arXiv (Cornell University). Cornell University. https://doi.org/10.48550/arxiv.1710.07709

[37]. Yenugula, M. (2023). Boosting Application Functionality: Integrating Cloud Functions with Google Cloud Services. International Research Journal of Education and Technology, 6(10), 369-375.

[38]. West, J., Bhattacharya, M., & Islam, R. (2015). Intelligent Financial Fraud Detection Practices: An Investigation. In arXiv (Cornell University). Cornell University. https://doi.org/10.48550/arxiv.1510.07165

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, November 2023

[39]. Xiang, S., Zhu, M., Cheng, D., Li, E., Zhao, R., Ouyang, Y., Chen, L., & Zheng, Y. (2023). Semi-supervised Credit Card Fraud Detection via Attribute-Driven Graph Representation. In Proceedings of the AAAI Conference on Artificial Intelligence (Vol. 37, Issue 12, p. 14557). Association for the Advancement of Artificial Intelligence. https://doi.org/10.1609/aaai.v37i12.26702

[40]. Yazıcı, Y. (2020). Approaches to Fraud Detection on Credit Card Transactions using Artificial Intelligence Methods (p. 235). https://doi.org/10.5121/csit.2020.101018

[41]. Yadulla, A. R., Yenugula, M., Kasula, V. K., Konda, B., Addula, S. R., & Rakki, S. B. (2023). A time-aware LSTM model for detecting criminal activities in blockchain transactions. International Journal of Communication and Information Technology, 4(2): 33-39

[42]. Kumar, D. (2022). Factors Relating to the Adoption of IoT for Smart Home. University of the Cumberlands.

[43]. R. Daruvuri, "An improved AI framework for automating data analysis," World Journal of Advanced Research and Reviews, vol. 13, no. 1, pp. 863–866, Jan. 2022, doi: 10.30574/wjarr.2022.13.1.0749.

[44]. Yadulla, A. R. (2022). Building smarter firewalls: Using AI to strengthen network security protocols. Int J Comput Artif Intell, 3(2):109-112.