IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Real-Time Fraud Detection In Banking With Generative Artificial Intelligence

Pradeep Kumar Sharma, ServiceNow

Santa Clara, California, USA

Abstract: The increase in digital transactions, cases of banking fraud have also increased. In this scenario, real-time fraud detection methods are essential for financial institutions. Outdated techniques can struggle to keep pace with these continually evolving fraud tactics. One potential solution to this challenge is generative artificial intelligence. Generative AI is a state-of-the-art algorithm-based technology powered by machine learning that imitates human behavior and generates real-world data. You can use this ability to detect banking fraud in real-time. Generative AI can flag suspected activities in real-time, all through its ongoing training on patterns and anomalies within customer transactions. Generative AI can be effective for fraud prevention as it helps identify fraud that occurs not only from ATMs but also from online banking, and multiple channels are available to the target audience. It has opened a wide range of opportunities for banks since real-time detection and prevention of fraudulent activities can be done, resulting in loss prevention and customer asset safety. Generative AI can also be trained for new types of fraud, making it a leading defense against new fraudulent tactics. It allows banks to take proactive measures to prevent fraud instead of reactively fighting it, saving money and time and improving consumer trust. We can protect customers and the financial institution in real-time.

Keywords: Real-Time, Financial Institutions, Online Banking, Trust, Fraud, Customers

I. INTRODUCTION

In finance and banking, real-time fraud detection amounts to detecting and preventing fraudulent activities nowadays. It is a process that utilizes state-of-the-art technology and methods to process large volumes of data quickly to identify and prevent fraudulent transactions. It is especially important in the banking sector because fraud can result in very large monetary losses for banks and their customers. The real-time fraud detection process begins with data collection. Databases such as customer information, transaction history and behavioral patterns need to be collected. A widely used approach in real-time fraud detection [1]. Entails developing a baseline of normal behavior for the firm customer, following which machine learning algorithms can be applied to spot deviations. Let's say a customer suddenly starts making large transactions or purchases in different regions. Predictive analytics is another crucial element in real-time fraud detection. By utilizing historical data to observe patterns and trends that indicate potential fraud. The system can then intelligently flag or block suspicious transactions on the fly based on this analysis, preventing fraud before it takes place. Among the methods banks employ are real-time monitoring systems that observe customer transactions and activity in real-time in addition to these techniques. It helps banks rapidly identify and respond to suspicious behavior, such as attempts to log in multiple times or transactions with new locations [2]. Additional security measures, such as biometric authentication, further enhance real-time fraud

detection in banking, providing an extra layer of protection against identity theft. Remember, the above is just a description of how you do real-time fraud detection in banking, but it is a much broader topic as real-time fraud detection in banking is a very dynamic and continuous process executed using sophisticated technologies and techniques to detect and prevent fraudulent activities in quick time. It is very important to protect both banks and customers by allowing them to make secure and trustworthy transactions. A global concern is real-time fraud detection in banking [3]. Scammers are always coming up with new and clever ways to trick banks and their customers, and banks need help to keep their systems safe. With the rise of online financial transactions, criminals also have more opportunities to commit fraud. Banks have some technical challenges in improving the detection and blocking of fraud in real time. First of all, they must be powered with a very strong and efficient fraud detection system. It needs extensive software that runs with sophisticated algorithms that can examine large quantities of data in real-time. Introducing such a system, though, may be costly and time-consuming, as a lot of active resources are a must, such as a skilled workforce, technology up, maintenance, and so on [4]. A further obstacle banks encounter is verifying their fraud detection systems are effective. False positives and false negatives are consequential for banks. False positives are legitimate transactions that the system marked as fraud, which can cause customer dissatisfaction and can lead to losses for the bank [5]. False negatives happen in those cases where fraudulent transactions are not detected, causing the bank to lose money. That means banks have to balance preventing losses from suspected fraud and erring too much on the side of suspicious designations. Since fraudsters are increasingly using techniques like synthetic identity theft and social engineering to beat the system, real-time fraud detection systems need to be able to sort the signal from the noise. It calls for real-time updates to the system to keep track of the newly devised techniques of fraudsters. This data is often stored across multiple systems and databases, which presents its own set of challenges. A bank can have many systems that are just for specific tasks like customer data, transactions or fraud prevention, which do not talk to each other. It results in a delayed response time in terms of real-time fraudulent activity detection. Thus, real-time fraud detection in the banking domain heavily relies on a range of processes requiring extensive and frequent process investment. As digital banking continues to grow and fraudsters become even more sophisticated, banks must prioritize their fraud detection measures to safeguard themselves and their customers. The main contribution of the research has the following:

- Advancement of Advanced Analytics Techniques: The study of real-time fraud detection in banking has facilitated the advancement of analytics techniques, which take into account the use of machine learning, artificial intelligence, and deep learning to identify fraud in real-time. By analyzing patterns and anomalies that may signal possible fraud based on real-time transaction data, these techniques enhance the accuracy and speed of detection.
- Real-time Monitoring System Implementation: Another significant contribution concerns developing and implementing real-time monitoring systems that continuously track customer behavior and transaction activity to detect suspicious behavior and flag it for further processing.
- Detecting Emerging Fraud Schemes: The research has also helped detect emerging fraud schemes and devise countermeasures against them. Using patterns and historical fraud data, as well as advanced data analysis techniques, researchers can identify patterns and trends that show signals for new types of fraud, enabling banks to take precautionary measures to combat these schemes.

The remaining part of the research has the following chapters. Chapter 2 describes the recent works related to the research. Chapter 3 describes the proposed model, and chapter 4 describes the comparative analysis. Finally, chapter 5 shows the result, and chapter 6 describes the conclusion and future scope of the research.

For this study secondary data has been collected. From the website of KSE the monthly stock prices for the sample firms are obtained from Jan 2010 to Dec 2014. And from the website of SBP the data for the macroeconomic variables are collected for the period of five years. The time series monthly data is collected on stock prices for sample firmsand relative macroeconomic variables for the period of 5 years. The data collection period is ranging from January 2010 to Dec 2014. Monthly prices of KSE -100 Index is taken from yahoo finance.

II. Related Words

Sekar, J. et,al.[7] have discussed real-time fraud prevention in digital banking, which has a cloud powered by artificial intelligence that discovers and prevents fraudulent actions in real time when they occur. It allows banks to fight against fraudulent transactions actively, shielding customers from potential threats in the realm of electronic money transfers. Gautam, A. et,al.[8] have discussed that AI has transformed risk management and fraud detection in the banking sector with advanced algorithms and predictive models that sift through vast amounts of data to detect potential risks and fraudulent activities. It has enhanced the efficiency, accuracy, and speed of detecting and preventing financial crimes, resulting in better protection of banks and their customers. Dahal, S. B. et,al.[9] have discussed how Generative AI can ingest vast and intricate financial data and analyze it in real-time to recognize possible gaps in the market. On another note, to address accurate and fair analysis, some challenges surrounding data quality and bias should also be considered, alongside ethical considerations. All this can transform how we analyze and make decisions in financial markets. Patil, D., et,al.[10] have discussed ChatGPT and other Generative AI Technologies, which are going to be huge across business sectors in the future. With applications in customer service, marketing, data analysis, and product development, these technologies will help automate processes, improve efficiency, and enhance customer experiences. It will be interesting to watch how far we can go this way and the innovative, effective use case that will emerge from this domain with further advancement and research. Kalia, S. et,al.[11] have discussed that generative artificial intelligence is going to reshape the financial industry by automating complex tasks, improving decision-making, and minimizing human error. It can also make possible innovation, and in terms of customer experiences, it can make more personalized recommendations and better detect fraud. It can also be responsible for job displacement and ethical questions. Bello, O. A. et,al.[12] have discussed that the deep learning model is considered in this study for effective cyber financial fraud detection. These techniques are capable of identifying patterns and anomalies through extensive data analysis, which may significantly increase financial security by helping to prevent and detect fraudulent activities.

III. Proposed Model

A machine learning model proposed for Generative Artificial Intelligence aims to emulate human creativity and imagination at a level beyond that of average human intellectual ability. Primarily trained on diverse examples of creative tasks, it uses a neural network-based model trained on hundreds of examples of everything from images to music and text. The way a GAI model works is as follows: it is trained on a large dataset of text, images, or other content, allowing it to learn the underlying structure of the data.

$$R\left(h,h^{'}\right)=\left\|h-h'\right\|2 \tag{1}$$

$$A_{A,E}=\frac{1}{m}\sum_{i=1}^{m}\left(\frac{1}{2}\left\|h-h_b\right\|^2\right) \tag{2}$$

$$R\left(h,e\left(p\left(h\right)\right)\right) \tag{3}$$

Generative models use various techniques, such as generative adversarial networks and variation auto encoders, to learn to generate new data that is similar to a training set. The model is trained on a wide range of text, allowing it to have a broader understanding of language and the capability to generate outputs that draw on a diverse set of writing styles and ideas. AI applications are tremendously interesting, from assisting artists and designers in the creative process to assisting scientific and research data generation.

$$z = p\left(Z_h + i\right) \tag{4}$$

$$h = e\left(Z'w + i\right) \tag{5}$$

$$AP = \sum_{b=1}^{b} \left(R_i - R_{i-1}\right) P_i \tag{6}$$

$$p\left(h\right) \to x\left(h'\right) \tag{7}$$

Requests for ideas for future applications will also change. Potential applications are vast, and it would be a huge help for designers or artists if we considered all the applications from this perspective. Employing the strength of machine learning could fundamentally change the means by which creativity and innovation are approached.

3. 1. Construction

Planning a review phase involves defining clear review goals and developing a detailed action plan for the review. This is a step that includes steps like defining the scope of the review, forming a review team, and setting a timeline for the completion of the review. Planning also includes devising a review protocol that clearly defines the particular research questions and outlines the inclusion and exclusion criteria to be applied, along with the methods for data collection and analysis. After the planning stage is completed, the review team starts to put the review protocol into practice and conduct the review. This includes concurrently scouring and analyzing data from the literature, reports, and databases. The review team uses well-specified methods to appraise the quality and relevance of the data extracted from the included studies and synthesizes the data to inform the research questions. Once the data have been collected and analyzed, the review team prepares a report summarizing the main findings and conclusions of the review. Fig 1: Shows the construction Model.

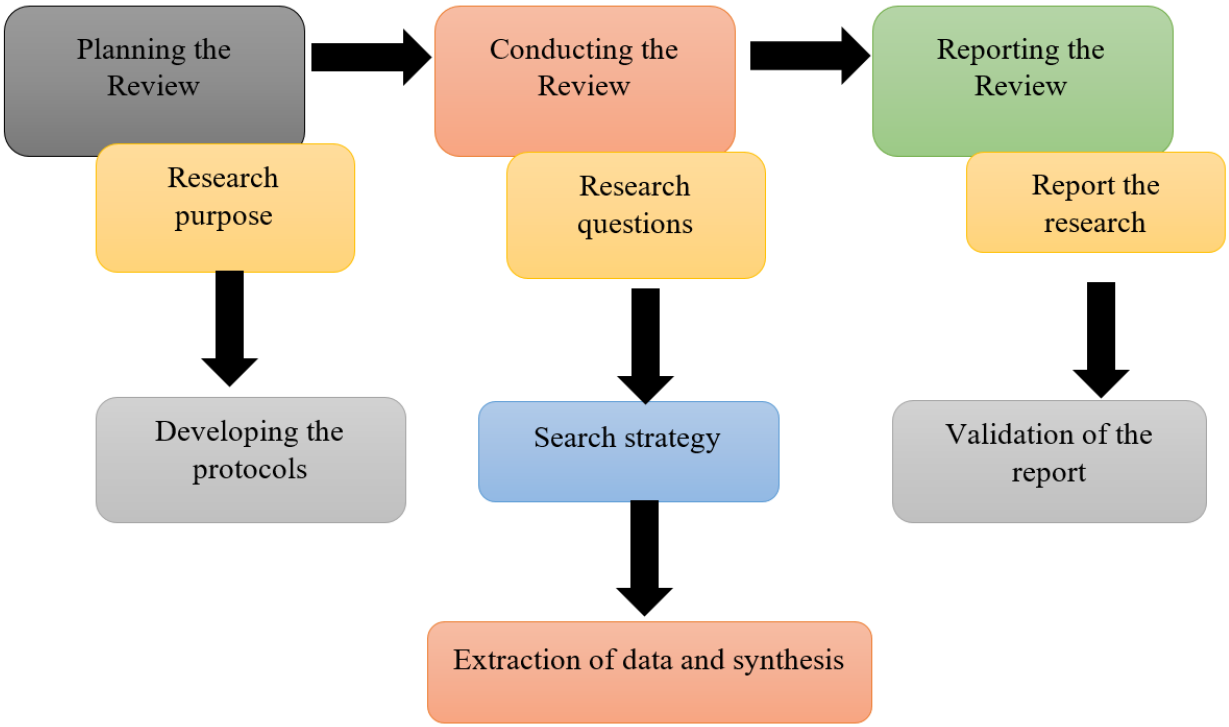

Fig 1: Construction Model

One of these approaches allows you to tell a story as a resolution for a problem or a situation, typically in a written format. However, it can also involve other types of communication, like presentations or infographics. Any action should be transparent, systematic and supported by evidence clearly presented in the report.

$$x\left(h'\right) \to e\left(h\right) = h \tag{8}$$

$$b = \sigma\left(Z_h + b\right) \tag{9}$$

The systematic evaluation of existing evidence on a particular topic that a review was conducted is intended for the purpose of informing decision-making and advancing knowledge in a specific area of research. It might also point to gaps in the existing evidence and possible future research directions. Protocols act like a roadmap for completing the review as they basically outline how the review is conducted systematically and transparently. It typically contains a description of the research question or study design, search strategy, data extraction methods, and data analysis technique.

3. 2. Operating principle

In computer science, the term transaction refers to a certain set of operations performed on a data set. A transaction is a series of operations or work that is performed in one unit. This means that a transaction is an atomic operation that needs to be done either completely or not at all. That is, all actions in a transaction must either be successful or fail.

$$h' = \sigma\left(W'r + b'\right) \tag{10}$$

$$s_{\phi}\left(h/h\right) = m\left(\rho\left(h\right), \omega^2\left(h\right)B\right) \tag{11}$$

A common resource for performing transactions could be a database, file, or any data structure in memory. So simply put, a monitor is a gatekeeper that allows only one thread/process to access a shared resource at a time. It needs to get a lock from the monitor when a thread or process needs to access a shared resource. It guarantees that until the first thread or process releases it, no other thread or process can access the shared resource. This mechanism prevents conflicts, ensuring data integrity. Then, when the thread or process has finished its work, it unlocks and lets other threads/processes use the shared resource. Global counters are data structures that help keep track of the occurrences of events or operations in computer systems. Its content is typically accessed and updated concurrently from multiple threads or processes. Fig 2: Shows the Operating principle Model.

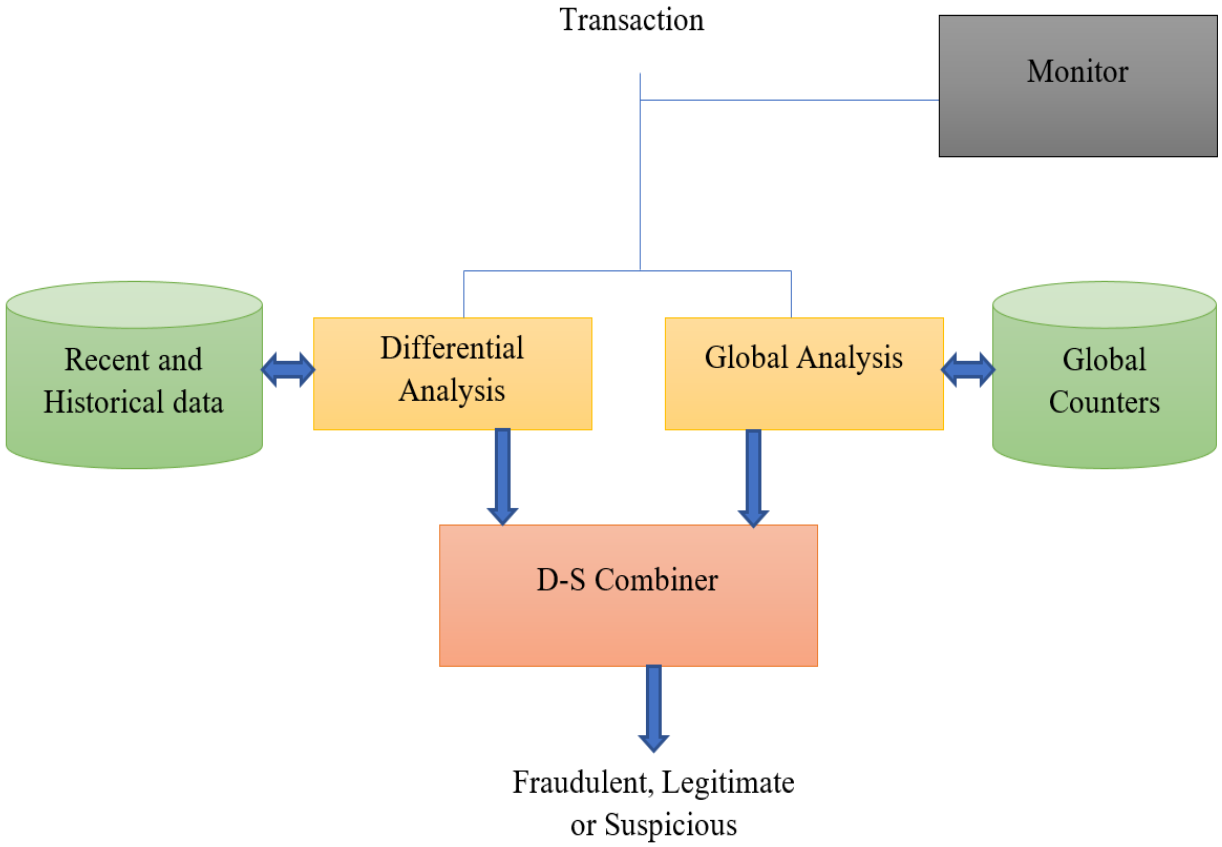

Fig 2: Operating principle Model

In a multi-threaded environment, global counters are usually implemented with atomic operations to be updated correctly. These are widely used in various applications like measuring website traffic, counting errors, load balancing, and providing the services required for site design. The global analysis process involves analyzing data collected from various sources to create a holistic view of the system. The process includes gathering data from multiple parts and analyzing it to detect patterns, trends, and anomalies. Training on global analysis is important for detecting system-wide problems and allowing informed decisions about system design and performance improvements.

$$P_\theta(x) = M(0, B) \tag{12}$$

This allows us to compare differences between data sets, basically subtract one from the other and then surface the differences. Differential analysis is also widely used in performance tuning, troubleshooting and detection of anomalies in system behavior. A data fusion approach that aggregates multiple pieces of evidence or information from different sources into a combined score or decision

IV. Result and Discussion

Beforeyoubegintoformatyourpaper,firstwriteandsavethecontentasaseparatetextfile. 4. 1. Accuracy of Detection: This shows the number of times fraudulent transactions were detected in real-time. It is one of the most essential technical performance metrics, providing insight into how effectively the generative artificial intelligence system can detect fraudulent activities. Fig 3: Shows the computation of Accuracy of Detection.

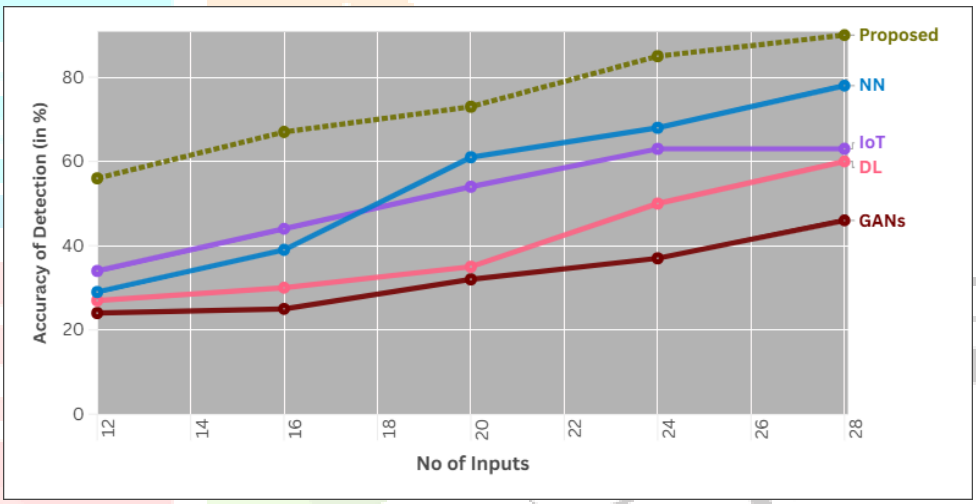

Fig 3: Computation of Accuracy of Detection

To have robustness in real-time fraud detection in banking using generative artificial intelligence, the accuracy of detection is one of the key factors that play a big role in stimulating both customer and financial institution's trust in the security of their monetary transactions.

4. 2. Processing Speed: Real-time fraud detection requires that the system self-processes a vast amount of data in a minuscule time frame to flag potentially fraudulent transactions. Fig 4: Shows the computation of Processing Speed.

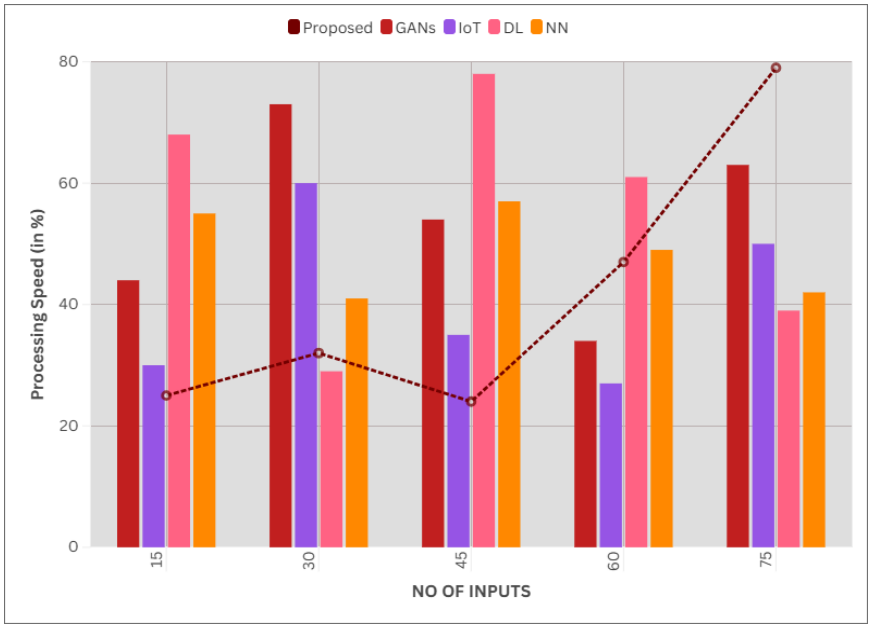

Fig 4: Computation of Processing Speed

One of the most critical technical performance aspects really comes down to processing speed because this is what defines the system's capabilities to detect and analyze fraud in real-time.

4. 3. Scalability: The banking sector's transaction volume continues to grow, and as it grows, the Fraud detection system should be capable of scaling and handling a larger number of transactions without sacrificing accuracy or speed. Fig 5: Shows the computation of Scalability.

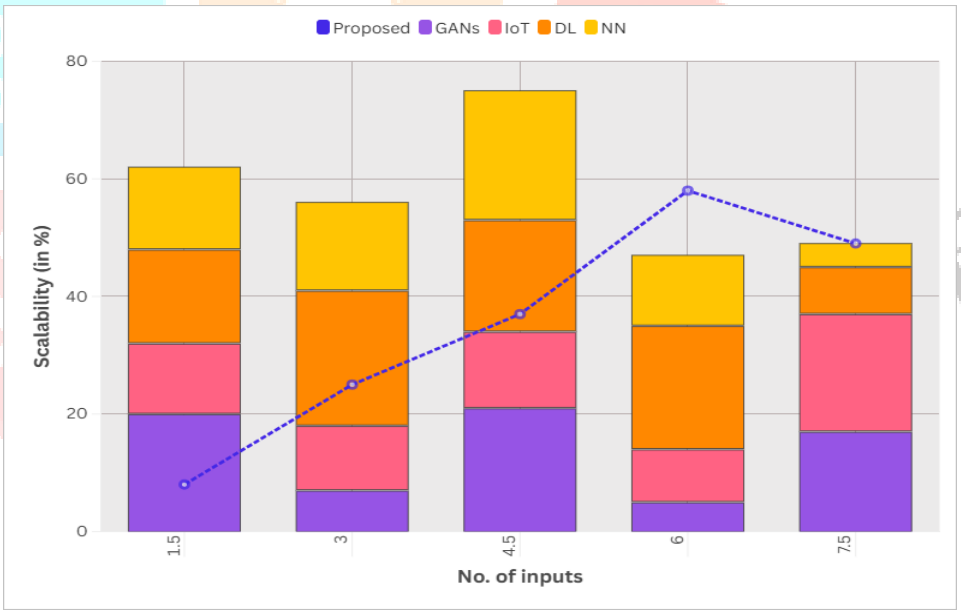

Fig 5: Computation of Scalability

It raises scalability along with other technical performance parameters for real-time fraud detection.

4. 4. False Positive Rate: This is when the system incorrectly identifies a legitimate transaction as fraud. Because of this, a high false positive rate can cause hassle for true customers and increase the burden on fraud analysts. Fig 6: Shows the computation of False Positive Rate.

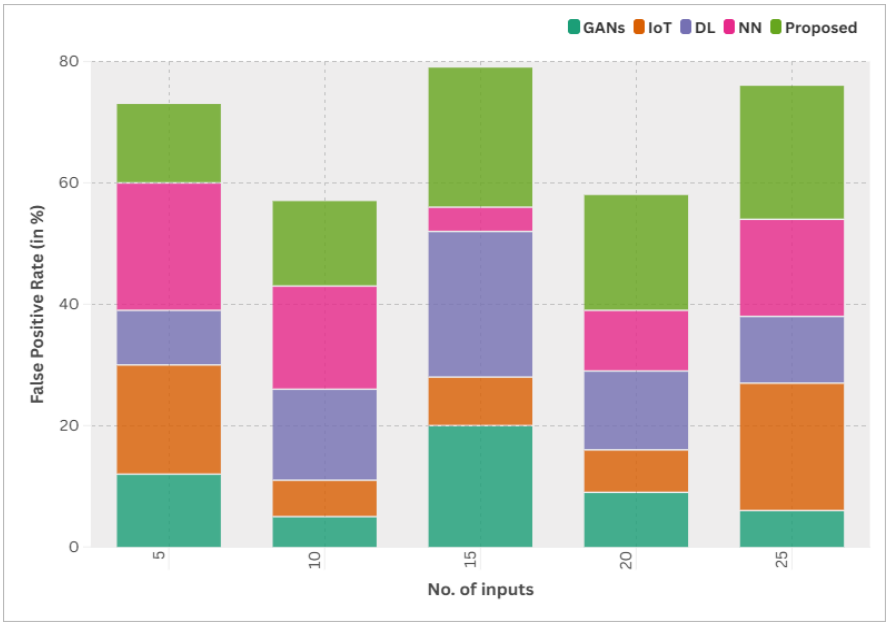

Fig 6: Computation of False Positive Rate

That is why a low false positive rate should be the second most relevant technical performance parameter for real-time fraud detection. This optimized generative talent should be available not just to confirm but repeatedly reduce the false positive space.

V. Conclusion

I. Fraud has long afflicted the banking industry, costing banks and their customers dearly. In the past, fraud networks used to identify fraudulent activity through traditional methods were unable to keep pace with the evolving techniques used by fraudsters. But, with further advancements in artificial intelligence, especially in the area of generative AI, a new and faster way to detect fraud is on hand. Thus, this paper presents generative AI for real-time fraud detection in the banking sector. Generative AI relies on complex algorithms that generate realistic data sets that can be exploited to reveal patterns of fraud that may not exist in traditional datasets. It houses another dimension of fraud prevention by targeting a broad spectrum of growing fraud methodologies as well and empowers banks to take preemptive measures. Detecting fraud in real time is essential to avoid monetary loss for both banks and customers. With the ability to review millions of data points instantly, generative AI saves hours in piecing together information and can identify fraudulent events with ease while flagging them for appropriate action. Not only has this ledger eliminated the need for manual fraud detection, but it cut down both time and resources. The use of Generative AI for real-time fraud detection in banking can dramatically enhance the bank's ability to prevent fraud and, thus, reduce financial losses. Fraud techniques constantly evolve, and the application of generative AI can enable banks to stay one step ahead and protect not just their but also their customers' assets

REFERENCES

[1] **[1]** Selvaraj, A., Selvaraj, A., & Venkatachalam, D. (2022). Generative Adversarial Networks (GANs) for Synthetic Financial Data Generation: Enhancing Risk Modeling and Fraud Detection in Banking and Insurance. Journal of Artificial Intelligence Research, 2(1), 230-269.

[2] Rane, N. (2023). Role and challenges of ChatGPT and similar generative artificial intelligence in finance and accounting. Available at SSRN 4603206.

[3] Dixit, S. (2024). Generative AI-Powered Document Processing at Scale with Fraud Detection for Large Financial Organizations. Authorea Preprints.

[4] Renugadevi, R., Shobana, J., Arthi, K., Kalpana, A. V., Satishkumar, D., & Sivaraja, M. (2024). Real-Time Applications of Artificial Intelligence Technology in Daily Operations. In Using Real-Time Data and AI for Thrust Manufacturing (pp. 243-257). IGI Global.

[5] Yusof, S. A. B. M., & Roslan, F. A. B. M. (2023). The Impact of Generative AI in Enhancing Credit Risk Modeling and Decision-Making in Banking Institutions. Emerging Trends in Machine Intelligence and Big Data, 15(10), 40-49.

[6] Patil, D., Rane, N. L., & Rane, J. (2024). Applications of ChatGPT and generative artificial intelligence in transforming the future of various business sectors. The Future Impact of ChatGPT on Several Business Sectors, 1-47.

[7] Sekar, J. (2023). REAL-TIME FRAUD PREVENTION IN DIGITAL BANKING A CLOUD AND AI PERSPECTIVE. Journal of Emerging Technologies and Innovative Research, 10, P562-P570.

[8] Gautam, A. (2023). The evaluating the impact of artificial intelligence on risk management and fraud detection in the banking sector. AI, IoT and the Fourth Industrial Revolution Review, 13(11), 9-18.

[9] Dahal, S. B. (2023). Utilizing Generative AI for Real-Time financial market analysis opportunities and challenges. Advances in Intelligent Information Systems, 8(4), 1-11.

[10] Patil, D., Rane, N. L., & Rane, J. (2024). Future directions for ChatGPT and generative artificial intelligence in various business sectors.

[11] Kalia, S. (2023). Potential Impact of Generative Artificial Intelligence (AI) on the Financial Industry. International Journal on Cybernetics & Informatics (IJCI), 12(12), 37.

[12] Bello, O. A., Folorunso, A., Ogundipe, A., Kazeem, O., Budale, A., Zainab, F., & Ejiofor, O. E. (2022). Enhancing Cyber Financial Fraud Detection Using Deep Learning Techniques: A Study on Neural Networks and Anomaly Detection. International Journal of Network and Communication Research, 7(1), 90-113.