Volume 3, Issue 3

FEEDFORWARD

MAGAZINE

July - Sept. 2024

IEEE COMPUTER SOCIETY

Santa Clara Valley Chapter

Feedforward is published quarterly by the IEEE Computer Society (CS) of the Santa Clara Valley (SCV). Views and opinions expressed in Feedforward are those of individual authors, contributors and advertisers and they may differ from policies and official statements of IEEE CS SCV Chapter.Although every care is being taken to ensure ethics of publication, Feedforward does not attest to the originality of the respective authors' content.

Editor's Voice

Welcome to the third edition of Volume 3 of FeedForward, the flagship publication of the IEEE Computer Society, Santa Clara Valley chapter. Within these pages, we aim to not only inform but also inspire our readers, offering fresh perspectives and innovative ideas.

As we step into the upcoming quarter with great anticipation, we're thrilled to present an array of technical publications that will kindle your enthusiasm for technology and innovation.

Join us on this exciting voyage where every page unfolds new dimensions of knowledge, fostering a community united by a shared passion for advancement and innovation. Welcome to a world of exploration and enlightenment—your journey awaits within the pages of our magazine.

Content

Acknowledgment

We extend heartfelt thanks to our dedicated reviewers whose expertise and thoughtful feedback have greatly enriched the quality of this publication.

Article Type: Research

Sports Injury Prevention with Generative AI

.Lakshmanan Sethu, *IEEE Senior Member, USA*

Abstract—Traditional injury prevention strategies in sports rely heavily on historical data analysis and biomechanical assessments. However, these methods often lack the ability to proactively predict and address specific injury risks. This paper explores the transformative potential of generative artificial intelligence (AI) in revolutionizing athlete safety through virtual injury simulations (VIS) and personalized training approaches. We present a methodological framework for conducting VIS, encompassing data acquisition, model development, simulation generation, and utilization. Additionally, we showcase the application of AI-driven personalized biomechanical assessments through a dedicated case study. By analyzing individual athlete data, AI can create personalized injury risk profiles, informing the development of customized training programs and preventative measures. This article highlights the immense potential of AI in proactive injury prediction, ultimately fostering a safer and more sustainable future for athletes and the overall sports landscape.

Generative AI has the remarkable ability to create realistic and diverse data sets. In the context of sports, this translates to the potential for generating synthetic training scenarios, Virtual injury simulations & Personalized biomechanical assessments. Let's dive into each topic below.

SYNTHETIC TRAINING SCENARIOS

The ability to accurately predict and mitigate potential injuries can significantly enhance athlete performance and longevity, while also minimizing the risk of setbacks and downtime. Traditional methods of injury prediction often rely on historical data and statistical analysis, but recent advancements in artificial intelligence (AI) offer a promising alternative approach. In particular, the use of Generative AI to create synthetic training scenarios has emerged as a groundbreaking technique for injury prediction and prevention.

Generative AI, a subset of machine learning, enables the creation of realistic and diverse synthetic data that closely mimics real-world scenarios. By leveraging Generative AI, researchers can generate a vast array of training scenarios that encompass a wide range of environmental conditions, athlete characteristics, and movement patterns. These synthetic scenarios serve as invaluable training data for predictive models, allowing researchers to train and fine-tune algorithms to accurately predict injury risk factors.

GANs are a type of neural network architecture that consists of two competing networks: a generator and a discriminator. The generator network tries to generate synthetic data (e.g., images, text, code etc.) that resembles the real data distribution, while the discriminator network tries to distinguish between the real data and the synthetic data generated by the generator. With the help of an adversarial training process, the generator learns to produce increasingly realistic synthetic data.

VAEs are a type of generative model that combines concepts from autoencoders and variational inference. They consist of an encoder network that learns to map input data to a latent space representation, and a decoder network that learns to reconstruct the input data from the latent space representation. VAEs can generate new synthetic data by sampling from the learned latent space distribution and passing the samples through the decoder network.

Recent studies have demonstrated the efficacy of Generative AI in generating synthetic training scenarios for injury prediction across various sports and physical activities. Researchers have developed sophisticated Generative Adversarial Networks (GANs) and Variational Autoencoders (VAEs) capable of generating high-fidelity synthetic data that closely resembles real-world training environments.

In one study, researchers utilized GANs to generate synthetic soccer training scenarios, including player interactions, ball trajectories, and environmental factors such as weather conditions and playing surfaces. By training predictive models on this synthetic data,

researchers were able to accurately predict injury risk factors such as player collisions, overexertion, and environmental hazards.

Similarly, in the field of strength training and weightlifting, researchers have employed VAEs to generate synthetic weightlifting scenarios, incorporating factors such as barbell trajectories, lifter biomechanics, and equipment variations. By training predictive models on this synthetic data, researchers achieved impressive accuracy in predicting potential injury risks such as muscle strain, joint stress, and lifting technique errors.

VIRTUAL INJURY SIMULATIONS

The traditional methods for preventing sports injuries are often reactive, relying on analyzing past data and implementing preventative measures after an injury occurs. However, generative artificial intelligence (AI) offers a transformative approach through virtual injury simulations (VIS). This paper outlines a methodological framework for conducting VIS and presents a case study illustrating its potential applications for athlete safety.

Methodological Framework

The framework for conducting VIS involves five key stages:

Data Acquisition and Preprocessing: Gather relevant data (injury databases, athlete biomechanics, training data) and ensure ethical considerations and data anonymization. Preprocess data for AI model training.

Motion capture systems like Vicon and Qualisys provide kinematic data through athlete movements. Injury databases from organizations offer historical injury records and patterns. Biomechanical modeling tools such as OpenSim can be used to accurate musculoskeletal models informed by medical imaging data from resources like the Visible Human Project. Computational fluid dynamics (CFD) software -ANSYS Fluent can simulate interactions between athletes and playing surfaces. Qualitative feedback from athlete interviews and collaborations with medical experts from societies ensure realistic simulations and effective prevention strategies.

Generative AI Model Development: Choose a suitable model (e.g., GANs, VAEs) based on desired simulation characteristics. Train the model using preprocessed data and refine it through hyperparameter adjustments and expert feedback.

Virtual Injury Simulation: Generation Define the desired injury type, sport, and athlete characteristics. Generate realistic simulations (visual representations and biomechanical data) using the trained model. Validate simulations against real-world data and expert feedback.

Utilizing Virtual Injury Simulations: Analyze simulations to identify common risk factors and develop targeted prevention strategies. Integrate findings into personalized training programs and athlete education for safer training and competition.

Continuous Improvement and Monitoring: Regularly monitor model performance, incorporate new data and advancements, and ensure ethical and responsible implementation through ongoing review and adjustments.

Case Study: ACL-Anterior Cruciate Ligament (ACL) Injury Prevention in Football

This case study demonstrates the application of VIS for preventing Anterior Cruciate Ligament (ACL) injuries in American football.

Data Acquisition In the data acquisition stage, data is captured from the following sources such as historical ACL injury data from professional football leagues,kinematic data of athletes performing football-specific movements (motion capture) and training data on exercise routines, intensity, and recovery.

Kinematic data forms another important part of the study. Professional athletes are observed through motion capture technology while performing football-specific movements such as cutting, jumping, and landing – movements commonly associated with ACL injuries.Through deep analysis of kinematic data, potential flaws or high-risk movement patterns can be identified This biomechanical analysis is crucial to know the underlying causes and developing targeted preventive measures.

Motion capture systems use multiple high-speed cameras to track reflective markers on an athlete's body. This shows detailed 3D kinematic data on joint angles, velocities, and accelerations during movements. Inertial measurement units (IMUs) with accelerometers and gyroscopes can be worn by athletes to measure linear and angular motions. High-speed video analysis, though less accurate, offers a more accessible option for extracting kinematic information. Force plates and pressure mats capture ground reaction forces and center of pressure during high-impact movements, complementing kinematic data. Electromyography (EMG) sensors measure muscle activity to identify imbalances or inefficiencies . Proper

calibration, marker placement, and data processing techniques are essential for accurate kinematic data collection in realistic training .

Model Development The 3D Variational Autoencoder (VAE) is chosen to generate realistic biomechanical simulations of knee movements.and the model is trained on the acquired data to learn the relationships between specific movements and increased ACL injury risk.

Simulation Generation The model is used to generate virtual simulations of high-risk maneuvers commonly associated with ACL injuries, such as landing from jumps or pivoting maneuvers. and the simulations are validated by comparing them with real-world ACL injury biomechanics data and feedback from sports medicine professionals.

Utilization The first step is to analyze simulations that reveal specific movement patterns associated with a higher risk of ACL injury. and on these findings, personalized training programs are developed for athletes identified as high-risk. These programs incorporate the neuromuscular training exercises to improve balance and landing mechanics and plyometric training modifications to reduce stress on the ACL, individualized movement pattern corrections.

Continuous Improvement The model is continuously monitored and updated with new injury data and advancements in biomechanics research.The effectiveness of the training program is evaluated through tracking injury rates and athlete feedback, leading to further refinement.

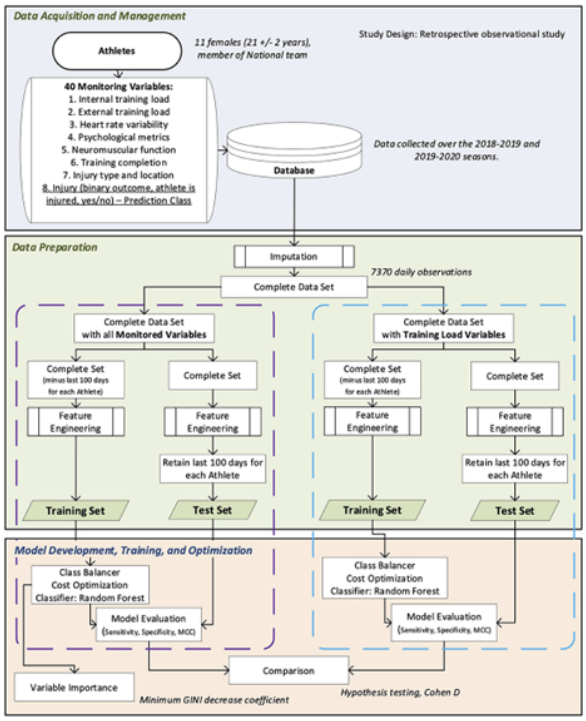

FIGURE 1. From Data acquisition and Management for sports injury prevention

PERSONALIZED TRAINING PROGRAM

Based on the risk profile and AI predictions, a customized training program is developed: Strengthening the wrist flexors helps counterbalance the extensors, promoting overall wrist stability and preventing excessive strain on one muscle group.The coach utilizes motion capture data to adjust the backhand stroke mechanics, minimizing wrist stress during the swing.The wearable sensor data is monitored during training to adjust intensity and rest periods based on real-time fatigue levels.

By continuously monitoring progress and incorporating feedback from the athlete and coach, the training program can be further refined for optimal performance and injury prevention.

Personalized assessments powered by generative AI can offer several benefits Proactive injury prevention - Identifying risks allows for early intervention and implementation of preventative measures before an injury occurs. Improved training efficiency-Personalized programs cater to individual needs and weaknesses, leading to more efficient training and faster progress. It can empower athletes by understanding their individual risk profiles and training adaptations empowers athletes to take an active role in their safety and performance improvement.

This case study exemplifies how personalized biomechanical assessments with generative AI can contribute to athlete safety and performance optimization. By integrating this approach into training routines, athletes, coaches, and medical professionals can work together to create a safer and more successful sporting experience.

While traditional injury prevention methods often missed those key data points, this analysis might reveal specific deficiencies in movement mechanics, such as muscle imbalances or inefficient landing techniques, contributing to injury risk.Generative AI can predict how athletes might respond to different training programs, allowing for personalized adjustments to optimize training efficiency and minimize injury risk.

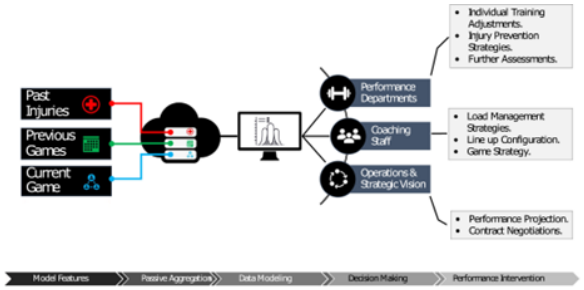

FIGURE 2. Biomedical assessments with Generative AI

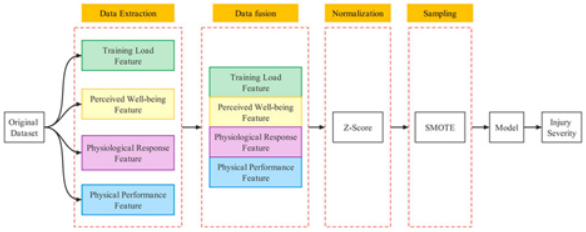

FIGURE 3. Personalize Training assessments with Generative AI

Case Study: Personalized Training for Tennis Players

This case study demonstrates how personalized biomechanical assessments with AI can be implemented in practice.

Data Acquisition In this phase, motion capture data is collected while the athlete performs forehands and backhands.Wearable sensor data is obtained during training sessions to monitor wrist strain and fatigue levels.Medical history also reveals a previous wrist sprain.

AI Analysis and Risk Profile:Analyzing the data with a VAE model identifies potential overuse in the athlete's wrist extensor muscles during backhand strokes.The model predicts an increased risk of repetitive strain injury (RSI) in the wrist due to the identified biomechanical inefficiency.

CHALLENGES AND CONSIDERATIONS

Firstly, data availability remains a crucial hurdle. Training reliable AI models necessitates access to large, diverse, and accurate datasets. This involves integrating various data sources, such as training data, medical records, and biomechanical information. However, this process faces both logistical and ethical considerations, necessitating careful navigation to ensure data privacy and responsible sourcing.

Secondly, the interpretability of AI models poses a significant challenge. Understanding the reasoning behind an AI model's predictions is critical for ensuring its effectiveness and building trust in its outputs. Unfortunately, achieving transparency and interpretability in these models remains a challenging task.

Finally, integrating AI into athlete training and injury prevention raises several ethical concerns. Data privacy considerations are paramount, as are potential biases that might be embedded within the model during development. Additionally, ensuring that technology complements rather than replaces human expertise is crucial for responsible and ethical implementation.

THE FUTURE OF AI-POWERED INJURY PREVENTION

While generative AI for injury prediction remains in its early stages, the possibilities are exciting. Combining this technology with existing research in AI and sports science has the potential to revolutionize athlete safety. However, addressing the challenges and ethical considerations are crucial for responsible development and implementation. As research continues and collaborations between researchers, medical professionals, and athletes grow, we can expect AI to play an increasingly significant role in safeguarding athletes on the field and ensuring their well-being.

CONCLUSION

The power of artificial intelligence (AI)plays an important role in the future of athlete safety in sports and is poised for a significant transformation. It involves analyzing individual athlete data, AI can proactively predict potential injuries, enabling timely interventions that mitigate risk. Furthermore, personalized training programs tailored through AI insights can optimize performance while minimizing injury susceptibility. Immersing athletes in AI-powered virtual simulations of risky maneuvers serves a dual purpose: refining safe technique and identifying individual vulnerabilities. Additionally, real-time monitoring with AI facilitates dynamic adjustments to training plans and prompt identification of potential issues, further safeguarding athlete well-being. While challenges remain in data privacy and model interpretability, responsible development of AI holds the potential to create a safer and more sustainable future for athletes, propelling the world of sports to new heights of performance and well-being.

REFERENCES

1. https://www.frontiersin.org/files/Articles/896828/fspor-04-896828-HTML/image_m/fspor-04-896828-g001.jpg
2. Van Eetvelde, H., Mendonça, L.D., Ley, C. et al. Machine learning methods in sport injury prediction and prevention: a systematic review. J EXP ORTOP 8, 27 (2021).https://doi.org/10.1186/s40634-021-00346-x
3. Meeuwisse, Willem H MD, PhD; Tyreman, Hugh BSc; Hagel, Brent PhD; Emery, Carolyn BScPT, PhD. A Dynamic Model of Etiology in Sport Injury: The Recursive Nature of Risk and Causation. Clinical Journal of Sport Medicine 17(3):p 215-219, May 2007. | DOI: 10.1097/JSM.0b013e3180592a48
4. Emmanuel Adetiba, Veronica C. Iweanya, Segun I. Popoola, Joy N. Adetiba & Carlo Menon | Wei Meng (Reviewing Editor) (2017) Automated detection of heart defects in athletes based on electrocardiography and artificial neural network, Cogent Engineering, 4:1, DOI: 10.1080/23311916.2017.1411220
5. Carey, D. L., Ong, K., Whiteley, R., Crossley, K. M., Crow, J. and Morris, M. E.. "Predictive Modelling of Training Loads and Injury in Australian Football" International Journal of Computer Science in Sport, vol.17, no.1, 2018, pp.49-66. https://doi.org/10.2478/ijcss-2018-0002
6. Carolyn A. Emery, Kati Pasanen,“Current trends in sport injury prevention,”Best Practice & Research Clinical Rheumatology,Volume 33, Issue 1,2019,Pages 3-15,ISSN 1521-6942.https://doi.org/10.1016/j.berh.2019.02.009
7. Cohan, Alexander, Schuster, Jake, and Fernandez, Jose. ‘A Deep Learning Approach to Injury Forecasting in NBA Basketball’. 1 Jan. 2021 : 277 – 289.
8. McCullagh, J., and T. Whitfort. "An investigation into the application of Artificial Neural Networks to the prediction of injuries in sport." International Journal of Sport and Health Sciences 7.7 (2013): 356-360.
9. Oliver, Jon L., et al. "Using machine learning to improve our understanding of injury risk and prediction in elite male youth football players." Journal of science and medicine in sport 23.11 (2020): 1044-1048.
10. Tervo, Taru, et al. "The 9+ screening test score does not predict injuries in elite floorball players." Scandinavian Journal of Medicine & Science in Sports 30.7 (2020): 1232-1236.

Lakshmanan Sethu Sankaranarayanan is a Technical account Manager - AI/ML solutions with a large technology firm where he works with enterprise customers to help them succeed on Google Cloud. He is currently focusing on Generative AI/ML & Data Solutions. With more than a decade of experience in the technology industry, Lakshmanan has a passion to transform enterprise organizations with Google Cloud. Prior to Google, He had helped fortune 500 companies to migrate to cloud across North America & Asia & UK regions.

Article Type: Review

How AI is changing the Financial Industry Landscape and its Ethical Consideration

Pankaj Pilaniwala, *University of Arizona, Tucson, AZ, USA*

Abstract—This research paper delves into the profound impact and ethical considerations of Artificial Intelligence (AI) in the financial industry, highlighting the dual nature of AI as a catalyst for innovation and a source of ethical dilemmas. Through a comprehensive analysis, the paper explores how AI is revolutionizing finance by enhancing operational efficiencies, improving risk management, personalizing customer experiences, and facilitating financial inclusion. Concurrently, it addresses the ethical challenges posed by AI, including concerns around data privacy, algorithmic bias, transparency, and the societal implications of widespread AI adoption. The paper presents case studies to illustrate real-world applications and outcomes of AI in finance, followed by a discussion on balancing innovation with ethics and speculations on future trends. The conclusion calls for future research and proposes some directions underscoring the importance of ethical considerations in leveraging AI for the benefit of the industry and society at large, calling for a collaborative approach to navigate the complexities of AI in finance responsibly.

Keywords: *Financial Industry, Artificial Intelligence*

INTRODUCTION

In recent years, Artificial Intelligence (AI) has emerged as a transformative force across several sectors, with the financial industry standing at the forefront of this technological revolution. The integration of AI technologies in finance has not only redefined the operational efficiencies and service delivery models but also introduced complex ethical and regulatory challenges that demand rigorous scrutiny and thoughtful solutions.

There has been a lot of debate around the definition of AI and recently an exhaustive definition has been proposed by Acemoglu and Restrepo [19]. While it's challenging to define exact boundaries, this dynamic and rapidly advancing domain primarily encompasses machine learning, deep learning, NLP (natural language processing) platforms, predictive APIs (application programming interfaces), image recognition, and speech recognition [20], and commerce platforms [66].

The allure of AI in finance [21] is evident through its diverse applications, ranging from automated trading systems [21] to fraud detection algorithms, personalized banking services, and risk management tools. These innovations have significantly enhanced the sector's ability to process vast amounts of data, make predictive analyses, and deliver tailored customer experiences. However, the rapid adoption of AI also raises critical ethical concerns, including issues related to data privacy, algorithmic bias, transparency, and accountability. As per a report AI will grow global GDP by 7% [63] and that aligns with Gartner Trends report of 2023 [64] [Figure 1].

This paper aims to provide a comprehensive overview of the impact of AI in the financial industry, focusing on both its transformative potential and the ethical considerations it necessitates. The paper will explore how AI technologies are reshaping finance, the benefits they bring, and the challenges they pose, especially in terms of ethical use and regulatory compliance. Through a balanced examination of these aspects, the paper seeks to contribute to the ongoing dialogue among researchers, technologists, executives, and policymakers on fostering responsible AI innovation in finance. As per McKinsey [26], AI technology will deliver $1 trillion worth of additional value every year in Fintech.

FIGURE 1. Gartner Trends report of 2023

AI ALGORITHMS USED IN THE FINANCIAL INDUSTRY

AI is used in several use cases in the Financial Industry, such as - AI has impacted the way fund managers perform stock analysis, the marketers reach out to probable customers, or how credit risk is evaluated to the probability of a loan getting defaulted. Everything is now influenced and data is processed by AI algorithms. Several AI algorithms are used by technologists to process data and automate processes while providing customers with an enhanced experience. The AI industry has evolved to master these algorithms that are now shaping the financial industry. The paper will delve into the influence of AI in the Financial Industry in the following sections.

The image [Figure 2] shows different AI algorithms mapped with their use cases in the Financial Industry from Banks to payment processors to Fund Managers to Loan Providers.

Figure 2. shows different AI algorithms used in the financial sector for different use cases. Like SVM is used by portfolio managers to do stock market analysis, Decision Trees are used by several Banks for their loan application decisions. The paper will highlight respective AI algorithms used to achieve use-cases in the sections below.

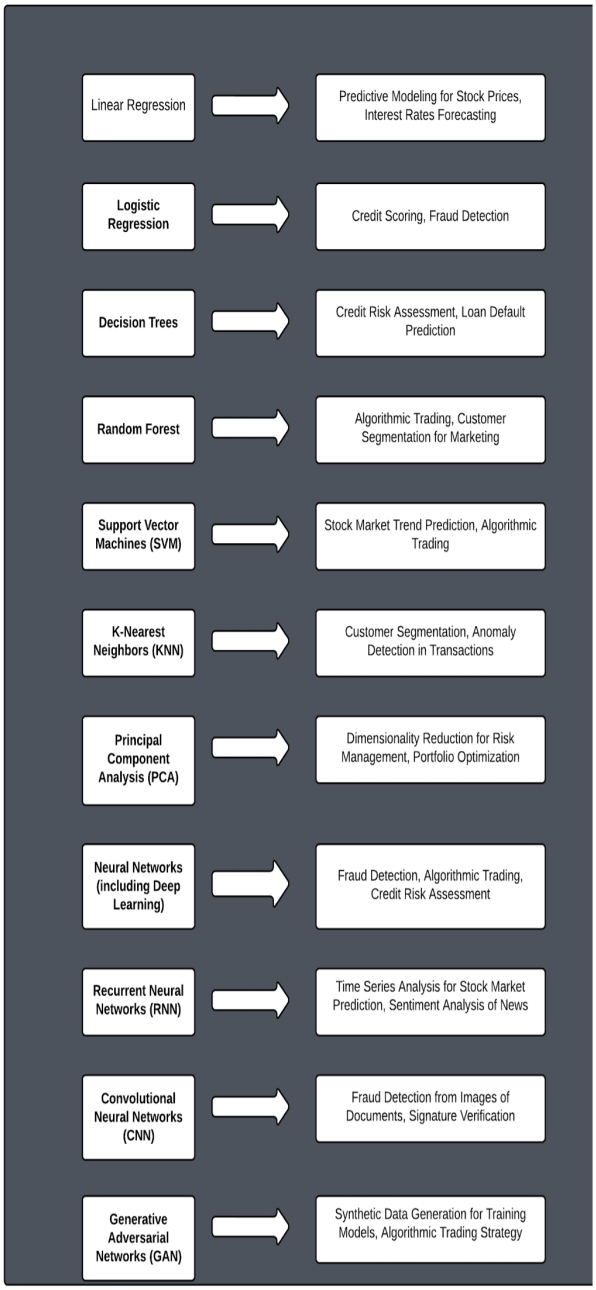

FIGURE 2. AI Algorithms and their use cases

THE IMPACT OF AI IN THE FINANCIAL INDUSTRY

Operational Efficiency

The adoption of AI in the financial industry [29] has led to significant improvements in operational efficiency, reducing costs and increasing speed and accuracy across various processes. For example, JPMorgan Chase's COIN (Contract Intelligence) platform uses machine learning to interpret commercial loan agreements, a task that previously consumed 360,000 hours of work each year by lawyers and loan officers. This AI application not only reduces the processing time from hours to seconds but also minimizes errors in documentation [1] and credit writing [27].

Automated Trading System

Automated trading systems represent another area where AI enhances efficiency. These systems analyze market data at high speeds, execute trades based on pre-defined criteria, and adapt to new information in real-time, optimizing investment strategies far beyond human capabilities. A study by the Wharton University found the positive impact of integrating AI with trading algorithms resulting in higher profits [2]. Some of the common AI algorithms used are SVM, Random Forest, GAN, etc.

Risk-Management & Fraud Detection

AI's ability to predict and manage financial risks has transformed risk management practices [25]. By leveraging vast datasets and advanced algorithms, financial institutions can now identify potential fraud, assess credit risk, and manage market risks with unprecedented precision, even predicting the bankruptcy chances of companies [30][31]. For instance, Mastercard's Decision Intelligence technology applies AI to each transaction, assessing its potential risk and making more accurate fraud decisions to reduce false declines [3].

AI is being used by financial institutions to fight fraud. AI can detect transactions and identify abnormalities, detecting early signs of fraudulence and notify the authorities. Dankse Bank implemented AI to identify Fraud and were able to detect fraud with higher accuracy [73]. Figure 3. Shows several AI algorithms that can be used in Risk Management.

Credit & Lending

Credit scoring models have also evolved with AI, enabling lenders to assess borrowers' creditworthiness more accurately and inclusively. By analyzing non-traditional data points such as rental payment histories and utility bills, AI models can provide credit scores for individuals who were previously "non-scorable," expanding access to financial services. A report by Deloitte highlighted that AI is transforming the financial sector and changing it for the good [4]. Research finds that ML reduces banks' losses on delinquent customers by up to 25 percent [28]. NN, Decision Tree and PCA are commonly used AI algorithms in Credit & Lending.

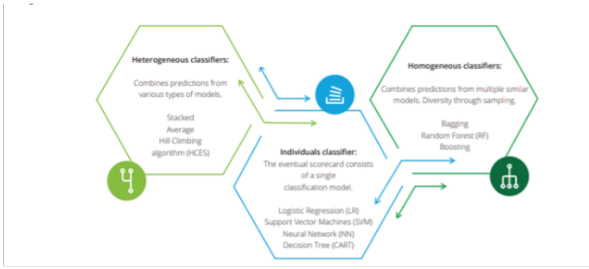

FIGURE 3. Different Algorithms to Consider for Risk
Source: Deloitte AI Credit-Risk Report [65]

Portfolio Management

Researchers have done several studies on utilizing AI/ML algorithm - Hierarchical Risk Parity (HRP) to construct complex portfolio to maximize the gains. As proposed by Depadro [32], it used Graph Theory and ML algorithm to infer the hierarchical relationships between the assets which are then directly utilized for portfolio diversification. Matkovskyy et al. investigated the role of cryptocurrencies in enhancing portfolio return of poorly performing stocks [33].

Robo-advisors represent a significant AI application in investment and wealth management, offering automated, algorithm-driven financial planning services with minimal human intervention. These financial banking apps provide personalized investment management and financial advice based on the user's financial situation and goals, using AI algorithms [24]. Savchenko has described a high-level architecture for Robo-Advisor-based financial solutions [53]. Some of the AI algorithms used are PCA, NN and RNN among several others.

Customer Experience

AI has revolutionized customer experience in the financial industry by providing personalized services and enhancing customer interaction. Chatbots and virtual assistants [34], powered by AI, offer 24/7 customer ser-

vice, handling inquiries, and transactions with speed and accuracy [35]. Bank of America's Erica, a virtual financial assistant, assists over 25 million users by providing account information, financial advice, and facilitating transactions, demonstrating the scalable benefits of AI in customer service. In a recent report [5] released by Bank of America, Erica surpassed 1.5 billion Client Interactions and has helped 37 million Bank's clients. According to a research, Banks are estimated to save $7.3B via chatbots and AI Automation [72]. Gen AI and LLM are used to create these experiences.

Personalized Banking Services

AI-driven personalization is transforming how consumers interact with banking services [40], offering customized advice, product recommendations, and financial management tools tailored to individual needs. For example, HSBC partnered with the AI company Personetics to provide its customers with personalized insights and advice through its mobile banking app. This AI-driven service analyzes customers' transaction patterns to offer tailored financial guidance, helping users manage their finances more effectively [6].

Moreover, AI enables personalized financial advice and product recommendations through data analysis, and understanding of individual customer preferences, and financial behaviors [36]. This level of personalization was previously achievable only through high-cost human financial advisors but can now be offered broadly, enhancing customer satisfaction and engagement [38]. Some of the commonly used AI algorithms are KNN and Matrix Factorization.

Access in Emerging Markets

AI is playing a crucial role in expanding access to financial services in emerging markets, where traditional banking infrastructure may be lacking. As per the World Economic Forum Report [7], "For instance, AI-powered mobile banking apps have already made significant strides in reaching rural and remote communities, where traditional banking infrastructure is sparse." As per the latest research, AI along with Bigdata will have a massive ramification on Fintech globally, connecting the unbanked population to the financial system [22]. AI phone agents are used to provide 24x7 service to the users in rural and emerging markets [74]. AI has allowed fintech to reach the emerging market and provide better services while keeping the cost low. Using AI tech like: Language Translation, users can now access app in their language of choice, instant access to virtual assistants have allowed companies to be there whenever the customer needs support, personalized experience via AI has allowed companies to offer the right products to the user group. An app named Wally is helping people in Panama save more and spend responsibly, built for emerging markets using AI, powered by their WallyGPT to support customers [87].

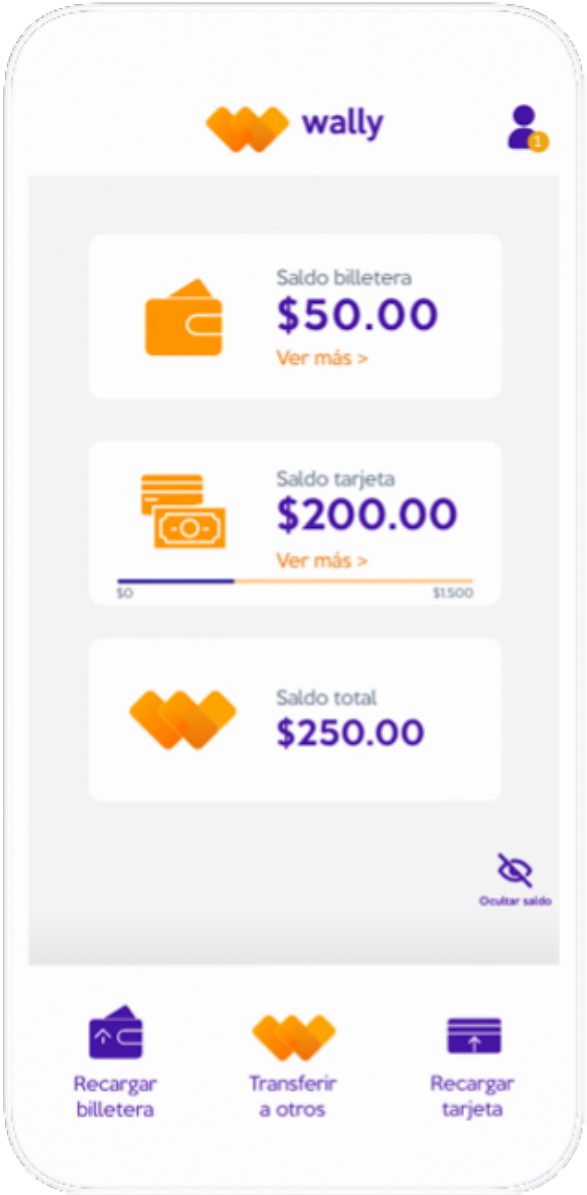

FIGURE 4. Wally App UI

Innovation and New Products

The financial industry has witnessed the introduction of innovative AI-driven products and services [39], from robo-advisors offering automated, algorithm-based investment advice to blockchain-based smart contracts

FIGURE 5. Use Cases of AI

that execute themselves when conditions are met [24]. AI's application in creating new financial products extends to insurance, where companies use AI to assess risks and customize policies in real-time, and in lending, where peer-to-peer platforms use AI to match lenders with borrowers efficiently. These innovations not only provide new opportunities for consumers and businesses but also challenge existing financial institutions to adapt and innovate.

ETHICAL CONSIDERATIONS IN THE USE OF AI IN THE FINANCIAL INDUSTRY

The integration of Artificial Intelligence (AI) into the financial sector [41] has not only revolutionized operational efficiencies and customer experiences but also introduced complex ethical considerations [42]. The ethical deployment of AI in finance raises profound questions regarding data privacy, algorithmic bias, transparency, and the broader societal implications of automated decision-making. As AI continues to evolve, ensuring its ethical use [47] becomes paramount in maintaining trust, fairness, and accountability in the financial sector. Raphael Max et al discuss the same in their paper [8].

Data Privacy and Consent

One of the foundational ethical concerns revolves around data privacy and the consent of individuals whose data is being used. Financial institutions harness vast amounts of personal and financial data to feed into AI systems for various purposes, including credit scoring, fraud detection, and personalized banking services. The ethical question arises: How can we ensure that this data is used responsibly? However, the challenge lies in balancing data utility for AI advancements with individuals' rights to privacy and consent. The integration with AI technology and the need for increasing amounts of user data may raise trust issues among customers and lawmakers [37].

With the current advancement in AI and on device processing, it's not clear what kind of data will the AI capture and process. In a survey, around 80% of users show concern about the data being collected and processed by companies using AI [77]. Most people do banking on their phones, make investments from their phones, talk to their financial advisors on their phones and with AI learning and processing users' data, this is going to create concerns among users. Wells Fargo was fined $1B for selling unnecessary and unconsented products to its customers using AI [86].

Algorithmic Biasness and Discrimination

AI systems are only as unbiased as the data and algorithms that power them. Historical data used in AI models can perpetuate existing biases, leading to discriminatory outcomes [43] in credit lending [44], insurance premiums, and even fraud detection [52]. A study by the AI Now Institute highlighted instances where AI systems in financial services have disadvantaged minority groups, raising concerns over systemic bias [9]. In a recent advancement, JP Morgan has expanded its Gen AI capability to help portfolio managers remove Biasness in decision making [71]. The table below shows the risk level for different AI Algorithms and their risk sources and use cases impacted.

In a study [67] conducted in 2019, it was found that racial discrimination is still a thing in lending. The study highlights that lenders charge Latinx and African-American borrowers higher interest rates, costing them $765M in higher interest charges, every year. AI algorithms also discriminate, but slightly lesser than humans. A similar study showed how African-American applicants were twice as likely to get rejected for a loan as opposed to similar financial-characteristics white applicants [70]. A recent example of biasness is by Apple credit card algorithm that provides lower credit line to female applicants opposed their male counterparts [75]. Another paper studies digital discrimination on Marketplaces like Airbnb, where non-black hosts charge more rentals opposed to the non-white hosts

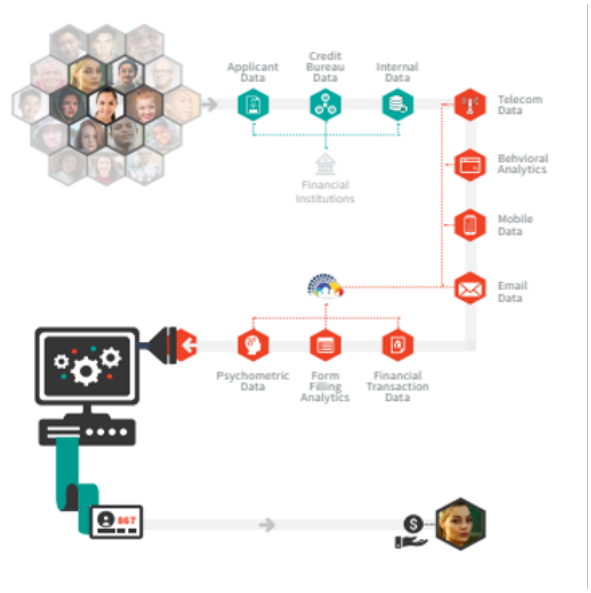

FIGURE 6. AI flow to create a fair Credit Scoring System

[82].

Fairness in AI

The ethical use of AI in finance necessitates a deep examination of fairness [45]: What measures can be implemented to ensure AI systems do not reinforce societal inequities? In the paper by Cynthia Dwork, et al, [48] researchers try to create a framework for fair classification such that similar individuals are treated similarly. Ai can be used to overcome the algorithmic biasness and discrimination, bringing a fairer approach in Financial Decisions. AI brings a unique integration of users' digital as well as financial footprint to create a new model that is not possible in the current method of assigning users with a Credit Score based on their financial history. AI has the potential to utilize data from wide range of sources, creating a more diverse data set for Financial Institutions to become fairer. Figure 6. shows [68] how LenddoEFL [69] utilizes a person's traditional and non-traditional data to create features and arrive at a Credit Score. This is the future of financial services where AI is leveraged to bring in more fairness in the decision process.

Transparency and Accountability

The "black box" nature of certain AI systems, where decision-making processes are opaque, poses significant ethical challenges in terms of transparency and accountability [46]. People, in general are more likely to trust AI, if it cites sources of the produced outcome and it's a great way to be transparent on how AI generated a text or took some decisions [78]. Another example is of a small business owner whose website was knocked off from Google's top results right before holidays, because of updates on Google's algorithm. The owner was left shattered. Google's search results ranking is known to have been using AI to show relevant results to the users and this lack of transparency can lead to users not trusting the system, leading to wider gap and unhappy customers [83].

Societal Impact and the Role of AI

The broader societal implications of AI in finance extend to concerns about job displacement, wealth inequality, and the concentration of power in the hands of a few tech giants. Pikas et al., in their research, have discussed the broader impact of AI on job displacement [60]. Moreover, the deployment of AI can exacerbate wealth inequality by privileging those with access to AI-driven financial tools and services. Facebook, owned by Meta, implemented unfair AI algorithms to block underserved communities to see housing ads [76]. This is not the AI that the society wants. It's widening the gap. The image below shows people in general are more concerned [79] than excited about AI. One way to overcome this is, AI can help the institutions make the financial services more accessible and transparent, thereby having a positive impact on the society.

Maintaining Ethical Balance

The ethical considerations surrounding the use of AI [50] in the financial sector are both profound and multifaceted, requiring a concerted effort from technologists, regulators, and society at large to address. Establishing ethical guidelines and regulatory frameworks that keep pace with AI's evolution is crucial. Initiatives like the OECD Principles on AI offer a foundation for responsible stewardship of trustworthy AI [10]. Several countries have accepted OECD principles as their guiding source to implement AI guidelines, see Figure 8. Philosophically, the ethical use of AI in finance touches upon fundamental questions about the kind of society we wish to build. It challenges researchers and industry to envision a future where technological advancements in AI are harnessed not just for efficiency and profit, but to foster a more equitable, transparent, and inclusive financial ecosystem.

The Challenges of AI Regulation

Regulating AI presents [49] a unique challenge due to the technology's fast-evolving nature and the com-

TABLE 1. AI Features and Their Impact on the Finance Industry

AI Feature	Risk Level	Sources of Risk	Impacted Use Cases	Impact on Finance Industry
Machine Learning	Medium to High	Biased training data, Model complexity, Lack of fairness measures	Credit Scoring, Fraud Detection, Customer Segmentation	Increased risk of biased credit decisions, potential discrimination, and customer targeting
Deep Learning	High	Overfitting, Lack of interpretability, Algorithmic bias	Natural Language Processing, Image Recognition	Difficulty in ensuring fairness, potential misidentification in security applications
NLP Platforms	Medium to High	Sensitive data handling, Privacy regulations, Bias in language models	Sentiment Analysis, Chatbots	Risk of perpetuating biases, potential discrimination
Predictive APIs	Low to Medium	Data quality, API reliability, Lack of fairness measures	Demand Forecasting, Personalized Recommendations	Potential bias in recommendations, fairness concerns in decision-making
Image Recognition	High	Misidentification, Privacy violations, Bias in training data	Facial Recognition, Object Detection	Risk of biased identification, potential privacy breaches
Speech Recognition	Medium	Noisy environments, Speech variability, Bias in training data	Virtual Assistants, Transcription Services	Risk of biased transcription, fairness concerns in voice-based services
Ethical Dilemma	Medium to High	Inherent biases, Lack of transparency, Unintended consequences	All AI applications	Potential ethical violations, trust erosion, regulatory scrutiny

plexity of its applications. Financial regulators must strike a delicate balance between fostering innovation and protecting consumers, involving updating existing regulations to address the nuances of AI and creating new frameworks that anticipate future developments [23].

Researchers have compared and contrasted the Algorithmic Accountability Act of 2022 (US AAA) with the European Artificial Intelligence Act (EU AIA) [51]. Europe is often cited as taking a conservative yet proactive approach to AI regulation [11], particularly concerning data protection and privacy.

CASE STUDIES: AI IN THE FINANCIAL INDUSTRY

Case Study 1: Betterment - Revolutionizing Wealth Management with Robo-Advisors

Overview: Betterment, one of the pioneers in robo-advisory services, uses AI to provide personalized investment advice [53] at a fraction of the cost of traditional financial advisors. The platform uses algorithms to tailor portfolios to individual investors' goals and risk tolerance [12].

Technical: Support Vector Machines, Neural Networks, LLMs, and similar AI algorithms

Impact: Betterment's success showcases how AI can democratize investment advice, making wealth management services accessible to a broader audience.

Product Innovation: Betterment's use of AI extends beyond basic robo-advisory services [54]. It has introduced AI-driven financial planning tools that help users set and achieve personalized financial goals, from saving for retirement to buying a home. These tools analyze user's financial data in real-time, adjusting advice and investment strategies as circumstances change, exemplifying how AI can create dynamic, responsive financial products [13].

Ethical and Regulatory Considerations: The rise of robo-advisors like Betterment raises questions about the fiduciary responsibilities of AI-driven platforms and the adequacy of existing regulatory frameworks to ensure that these technologies act in the best interest

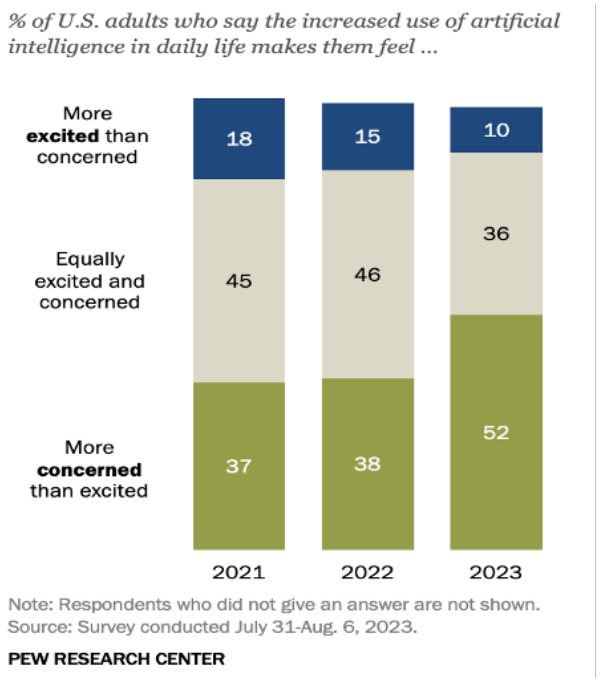

FIGURE 7. Concern about artificial intelligence in daily life far outweighs excitement

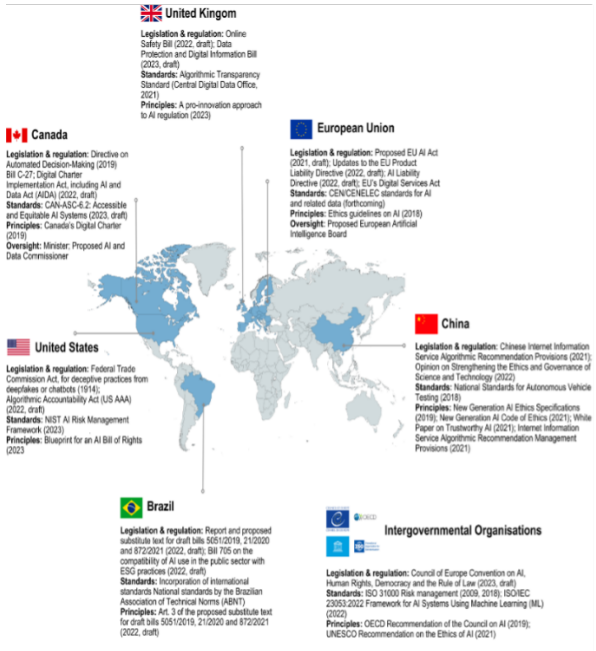

FIGURE 8. Source: OECD Report: https://oecd.ai/en/wonk/national-policies-2

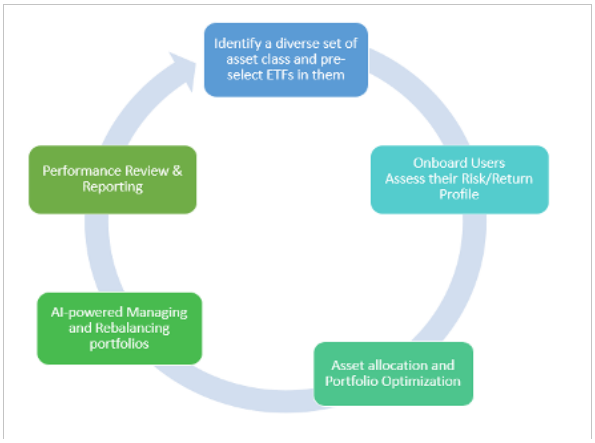

FIGURE 9. Robo-Advisor Process Flow

of consumers.

Case Study 2: Square - AI-Driven Financial Services for Small Businesses

Overview: Square, known for its payment processing solutions, utilizes AI to offer a suite of financial services tailored to small businesses. By analyzing transaction data, Square identifies trends and insights that inform product development, including capital loans and payments fraud detection [14]. Square is using Gen AI and has launched several AI features for businesses [18].

Technical: OpenAI is one of the AI providers but Square has plan to integrate with others like Google Gemini in the future.

Impact: Square's use of AI to offer tailored financial services, notably through Square Capital, has had a profound impact on small businesses. By providing access to capital based on transaction data rather than traditional credit scores, Square enables businesses that might otherwise be ineligible for loans to secure funding. This democratization of financial services supports business growth and economic diversity.

Product Innovation: A standout product is Square Capital, which provides small businesses with access to funding based on their transaction history with Square. This AI-driven approach allows for quick loan approvals without traditional credit checks, democratizing access to capital for small enterprises.

Ethical and Regulatory Considerations: While Square's AI-driven financial products promote inclusivity, they also prompt ethical considerations regarding data privacy and the potential for algorithmic bias. Square addresses these issues by implementing transparent data use policies and developing algorithms

that are fair and unbiased. Compliance with financial regulations ensures that Square's products remain accessible and equitable for all small businesses.

DISCUSSION: NAVIGATING THE FUTURE OF AI IN FINANCE

The integration of Artificial Intelligence (AI) into the financial industry presents a unique conundrum—balancing the relentless pursuit of innovation with the imperative of ethical responsibility. This section explores the ongoing debate surrounding the responsible use of Ethical AI [81] in finance, offering insights into future trends, potential developments, and the evolving landscape of ethical frameworks [17].

Balancing Innovation with Ethics

The financial industry's adoption of AI has undoubtedly led to significant advancements, from operational efficiencies to enhanced customer experiences. However, this rapid innovation brings forth ethical challenges [85] that must be addressed to ensure these technologies benefit society as a whole.

Open Market: With the advancement of AI, regulators must create laws to ensure that the platforms being built on AI technologies don't create platform monopolies. The market shall become more open and transparent for new entrants to come and survive. This will grow the industry and ensure ethical and fair business and technology practices.

Bias and Fairness: AI systems are only as unbiased as the data they are trained on [56]. Historical biases can be inadvertently encoded into AI models, leading to discriminatory outcomes. Financial institutions must prioritize the development of AI systems that are both fair and inclusive [57], employing techniques to identify and correct biases within datasets and algorithms [15]. The industry must develop standards for explainable AI that maintain the effectiveness of these systems while ensuring accountability [58] and fairness [59].

Data Privacy and Security: The ethical use of data is a cornerstone of responsible AI development [55]. Institutions must navigate the delicate balance between leveraging data for AI advancements and respecting individual privacy rights. Adhering to regulations like GDPR in Europe, and developing robust data governance policies, are crucial steps in this direction.

Auditing: Auditing is not a new concept. All the companies go through it for Financial Audit, medical researches go through it and any other form of public services do it. There is a need for AI to also go through third party auditing [84]. This will ensure, the products built don't have the issues discussed above. It involves surveys, A/B Testing, online data scraping, crowdsourced audits [80].

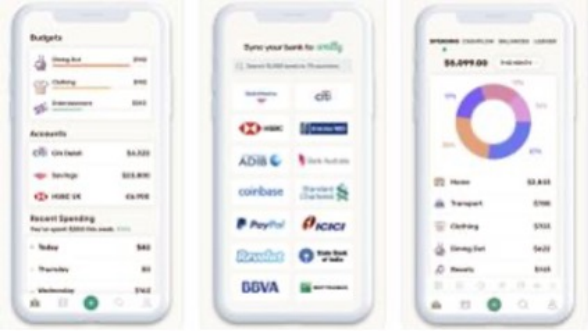

FIGURE 10. GPT-powered Finance App

Collaborative Regulation: A collaborative approach, involving regulators, institutions, and technology providers, is essential to develop flexible, adaptive regulations that encourage innovation while protecting consumers and maintaining financial stability.

Delegen, et al., signify the importance of these dynamics as crucial for policymakers to navigate the complexities of AI-induced job displacement and ensure equitable societal outcomes [61]. The Financial Conduct Authority (FCA) should require that businesses demonstrate and prove that their use of AI leads to the positive outcomes as they claim.

Future Trends and Predictions

Looking ahead, the financial industry can expect several key trends to shape the future of AI in finance:

Advanced Predictive Analytics: The next generation of AI will offer even more sophisticated predictive capabilities, using deep learning and neural networks to anticipate market shifts, consumer behavior [88] as seen in Figure 10, and potential fraud with greater accuracy than ever before [16].

AI and Blockchain Integration: The combination of AI and blockchain technology promises to revolutionize financial transactions, providing unprecedented levels of security, transparency, and efficiency. This integration could lead to the development of new financial products and services, such as smart contracts that automatically execute based on AI-driven insights [62].

Democratization of Financial Services: AI will continue to break down barriers to financial services, offering personalized financial advice, credit, and insurance products to a broader audience. This democratization will help to reduce inequality and promote economic inclusion globally.

CONCLUSION

The exploration of Artificial Intelligence (AI) within the financial industry has unveiled a landscape rich in innovation and fraught with ethical dilemmas. As this research paper has demonstrated, AI's integration into finance has produced significant benefits, however, these advancements come with ethical considerations that demand careful attention with the overarching societal impacts of automation. This paper shall be used to study and research further the integrations of current AI Models. Future studies shall be conducted to study the positive impact of current AI models, their accuracy, and how they can be improved to bring a positive outcome in the Fintech domain. Generative AI will further the integration of AI in Finance impacting the industry in new ways. This opens up the need for scholarly research on how these new AI models are going to change user behavior and what new challenges they pose. AI is a fast-evolving field and continuous research and study of this field is the only way to not only advance the field but also make it more ethical and optimal.

REFERENCES

1. D. C. Weiss, "JPMorgan Chase uses tech to save 360,000 hours of annual work by lawyers and loan officers," Mar. 2, 2017.
2. W. W. Dou, I. Goldstein, and Y. Ji, "AI-Powered Trading, Algorithmic Collusion, and Price Efficiency," Jacobs Levy Equity Management Center for Quantitative Financial Research Paper, Jan. 27, 2024. [Online]. Available: https://dx.doi.org/10.2139/ssrn.4452704
3. CDO Magazine Bureau, "Mastercard Launches Decision Intelligence Pro, New Generative AI Model for Fraud Detection," CDO Magazine, Feb. 06, 2024. [Online]. Available: https://www.cdomagazine.tech/aiml/mastercard-launches-decision-intelligence-pro-new-generative-ai-model-for-fraud-detection
4. Deloitte Report, "Explain Artificial Intelligence for Credit Risk Management." [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/fr/Documents/risk/Publications/deloitte_artificial-intelligence-credit-risk.pdf
5. Bank Of America Report, "BofA's Erica Surpasses 1.5 Billion Client Interactions, Totaling More Than 10 Million Hours of Conversations," Newsroom, July 13, 2023. [Online]. Available: https://newsroom.bankofamerica.com/content/newsroom/press-releases/2023/07/bofa-s-erica-surpasses-1-5-billion-client-interactions--totaling.html
6. Personetics Blog, "HSBC Leverages Smart Analytics to Develop New Tools That Enhance the Personalised Customer Experience," Apr. 25, 2022. [Online]. Available: https://personetics.com/hsbc-leverages-smart-analytics-to-develop-new-tools-that-enhance-the-personalised-customer-experience/
7. World Economic Forum Report, "How Artificial General Intelligence will drive an inclusive financial sector in Latin America," Jan. 11, 2024. [Online]. Available: https://www.weforum.org/agenda/2024/01/ai-is-driving-the-evolution-of-a-more-inclusive-financial-sector-in-latin-america-here-is-how/
8. R. Max, A. Kriebitz, and C. Von Websky, "Ethical Considerations About the Implications of Artificial Intelligence in Finance," Springer, May 13, 2020. doi: 10.1007/978-3-030-00001-1_21-1
9. S. M. West, "Discriminating Systems: Gender, Race, and Power in AI – Report," AI Now Institute, Apr. 1, 2019. [Online]. Available: https://ainowinstitute.org/publication/discriminating-systems-gender-race-and-power-in-ai-2
10. OECD, "OECD AI Principles overview," 2019. [Online]. Available: https://oecd.ai/en/ai-principles
11. EU Official Website, "Ethics guidelines for trustworthy AI," Apr. 8, 2019. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai
12. B. Schmidt and A. Albright, "AI Is Coming for Wealth Management. Here's What That Means," WealthManagement.com, Apr. 24, 2023. [Online]. Available: https://www.wealthmanagement.com/technology/ai-coming-wealth-management-here-s-what-means
13. T. Nagar, "Role of AI in Wealth Management: Its Uses, Trends & Benefits," DevTechnoSys.com, Feb. 26, 2024. [Online]. Available: https://devtechnosys.com/insights/role-of-ai-in-wealth-management/
14. M. Jarrell, "Artificial Intelligence at Square – Two Use-Cases," Emerj.com, Sep. 6, 2021. [Online]. Available: https://emerj.com/ai-sector-overviews/artificial-intelligence-at-square/
15. E. Ferrara, "Fairness and Bias in Artificial Intelligence: A Brief Survey of Sources, Impacts, and Mitigation Strategies," Arxiv. [Online]. Available: https://arxiv.org/ftp/arxiv/papers/2304/2304.07683.pdf
16. M. Goel, P. K. Tomar, L. P. Vinjamuri, G. S. Reddy, M. Al-Taee, and M. B. Alazzam, "Using AI for Predictive Analytics in Financial Management," IEEE, Jul. 24, 2023. doi: https://doi.org/10.1109/ICACITE57410.2023.10182711
17. Ginimachine, "AI Ethics in Finance: Balancing Innovation with Responsibility," Dec. 8, 2023. [Online]. Available: https://ginimachine.com/blog/

ai-ethics-in-finance-balancing-innovation-with-responsibility/#:~:text=Developing%20AI%20with%20Ethical%20Principles,while%20addressing%20ethical%20concerns%20adeptly

18. Square, "New Generative AI Features from Square Give Powerful Technology to All Businesses," Oct. 18, 2023. [Online]. Available: https://squareup.com/us/en/press/square-ai-tools
19. D. Acemoglu and P. Restrepo, "The wrong kind of AI? Artificial intelligence and the future of labor demand," Cambr J Reg Econ Soc, Cambr Pol Econ Soc, vol. 13, no. 1, pp. 25–35, 2020.
20. A. Martinelli, A. Mina, and M. Moggi, "The enabling technologies of industry 4.0: examining the seeds of the fourth industrial revolution," Ind Corp Chang, 2021. doi: https://doi.org/10.1093/icc/dtaa060
21. M. Cucculelli and M. Recanatini, "Distributed Ledger technology systems in securities post-trading services. Evid Eur Global Syst Banks," Eur J Finance, vol. 28, no. 2, pp. 195–218, 2022. doi: https://doi.org/10.1080/1351847X.2021.1921002
22. J. Jagtiani and J. Kose, "Fintech: the impact on consumers and regulatory responses," J Econ Bus, vol. 100, pp. 1–6, 2018. doi: https://doi.org/10.1016/j.jeconbus.2018.11.002
23. L. D. Wall, "Some financial regulatory implications of artificial intelligence," J Econ Bus, vol. 100, pp. 55–63, 2018. doi: https://doi.org/10.1016/j.jeconbus.2018.05.003
24. J. K. Hentzen, A. O. I. Hoffmann, and R. M. Dolan, "Which consumers are more likely to adopt a retirement app and how does it explain mobile technology-enabled retirement engagement?" Int J Consum Stud, vol. 46, pp. 368–390, 2022. doi: https://doi.org/10.1111/ijcs.12685
25. X. Huang and F. Guo, "A kernel fuzzy twin SVM model for early warning systems of extreme financial risks," Int J Financ Econ, vol. 26, no. 1, pp. 1459–1468, 2021. doi: https://doi.org/10.1002/ijfe.1858
26. S. Biswas, B. Carson, V. Chung, S. Singh, and R. Thomas, "AI-bank of the future: Can banks meet the AI challenge?" McKinsey & Company, Sep. 2020. [Online]. Available: https://www.mckinsey.com/industries/financial-services/our-insights/ai-bank-of-the-future-can-banks-meet-the-ai-challenge
27. S. W. Gates, V. G. Perry, and P. M. Zorn, "Automated Underwriting in Mortgage Lending: Good News for the Underserved?" Housing Policy Debate, vol. 13, no. 2, pp. 369–391, 2002.
28. A. Khandani, K. Adlar, and A. Lo, "Consumer Credit-Risk Models via Machine Learning Algorithms," Journal of Banking & Finance, vol. 34, no. 11, pp. 2767–2787, 2010.
29. M. Jakšič and M. Marinč, "Relationship banking and information technology: the role of artificial intelligence and FinTech," Risk Manag, vol. 21, pp. 1–18, 2019. doi: https://doi.org/10.1057/s41283-018-0039-y
30. M. Hamdi, S. Mestiri, and A. Arbi, "Artificial Intelligence Techniques for Bankruptcy Prediction of Tunisian Companies: An Application of Machine Learning and Deep Learning-Based Models," Journal of Risk and Financial Management, vol. 17, no. 4, pp. 132, 2024. doi: https://doi.org/10.3390/jrfm17040132
31. F. Mai, S. Tian, C. Lee, and L. Ma, "Deep learning models for bankruptcy prediction using textual disclosures," European Journal of Operational Research, vol. 274, no. 2, pp. 743-758, 2019. doi: https://doi.org/10.1016/j.ejor.2018.10.024
32. M. López de Prado, "Building Diversified Portfolios that Outperform Out of Sample," The Journal of Portfolio Management, vol. 42, no. 4, pp. 59–69, 2016. doi: 10.3905/jpm.2016.42.4.059
33. R. Matkovskyy, A. Jalan, M. Dowling, and T. Bouraoui, "From bottom ten to top ten: The role of cryptocurrencies in enhancing portfolio return of poorly performing stocks," Finance Research Letters, vol. 38, pp. 101405, 2021. doi: https://doi.org/10.1016/j.frl.2019.101405
34. D. L. Poole and A. K. Mackworth, "Artificial intelligence: Foundations of computational agents," Cambridge University Press, Cambridge, 2010.
35. V. Gupta, A. Drave, Y. K. Dwivedi, A. M. Baabdullah, and E. Ismagilova, "Achieving superior organizational performance via big data predictive analytics: A dynamic capability view," Industrial Marketing Management, 2019. doi: 10.1016/j.indmarman.2019.11.009
36. M. Evans, "Build A 5-star customer experience with artificial intelligence," Feb. 17, 2019. [Online]. Available: https://www.forbes.com/sites/allbusiness/2019/02/17/customer-experience-artificial-intelligence/#1a30ebd415bd
37. Y. K. Dwivedi, L. Hughes, E. Ismagilova, G. Aarts, C. Coombs, and T. Crick, "Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy," International Journal of Information Management, 2019. doi: 10.1016/j.ijinfomgt.2019.08.002
38. G. Omale, "Improve customer experience with artificial intelligence," 2019. [Online]. Available: https://www.gartner.com/smarterwithgartner/improve-customer-experience-with-artificial-intelligence/
39. A. Atadoga, O. C. Obi, et al., "AI's evolving impact in

US banking: An insightful review," IJSRA, vol. 11, no. 1, pp. 904-922, 2024. doi: 10.30574/ijsra.2024.11.1.0157

40. B. Sugiharto and Harkim, "Artificial Intelligence (AI) Architecture for Integrated Smart Digital Banking System," JPPIPA, vol. 9, no. 10, 2023. doi: 10.29303/jppipa.v9i10.4645
41. E. Almustafa, A. Assaf, and M. Allahham, "Implementation of Artificial Intelligence for Financial Process Innovation of Commercial Banks," 2023. doi: 10.24857/rgsa.v17n9-004
42. R. Hastuti and Syafruddin, "Ethical Considerations in the Age of Artificial Intelligence: Balancing Innovation and Social Values," West Science Social and Humanities Studies, vol. 1, no. 2, pp. 76-87, Aug. 2023.
43. L. Belenguer, "AI bias: exploring discriminatory algorithmic decision-making models and the application of possible machine-centric solutions adapted from the pharmaceutical industry," AI Ethics, vol. 2, pp. 771–787, 2022. doi: https://doi.org/10.1007/s43681-022-00138-8
44. R. Bartlett, A. Morse, R. Stanton, and N. Wallace, "Consumer-lending discrimination in the FinTech era," J. Financ. Econ., vol. 143, no. 1, pp. 30-56, 2022.
45. R. K. Bellamy et al., "AI fairness 360: an extensible toolkit for detecting, understanding, and mitigating unwanted algorithmic bias," arXiv:1810.01943.
46. R. Binns, "Fairness in machine learning: lessons from political philosophy," In Conference on Fairness, Accountability and Transparency, pp. 149–159. PMLR, 2018.
47. P. Boddington, "Towards a Code of Ethics for Artificial Intelligence," Springer, Cham, 2017.
48. C. Dwork, M. Hardt, T. Pitassi, O. Reingold, and R. Zemel, "Fairness Through Awareness," Arxiv, Nov. 30, 2011. doi: https://doi.org/10.48550/arXiv.1104.3913
49. O. J. Erdélyi and J. Goldsmith, "Regulating artificial intelligence: proposal for a global solution," Preprint, arXiv:2005.11072, 2020.
50. T. Hagendorff, "The ethics of AI ethics: an evaluation of guidelines," Mind Mach., vol. 30, no. 1, pp. 99–120, 2020.
51. J. Mökander, P. Juneja, D. S. Watson et al., "The US Algorithmic Accountability Act of 2022 vs. The EU Artificial Intelligence Act: what can they learn from each other?" Minds & Machines, vol. 32, pp. 751–758, 2022. doi: https://doi.org/10.1007/s11023-022-09612-y
52. D. Danks and A. J. London, "Algorithmic bias in autonomous systems," IJCAI International Joint Conference on Artificial Intelligence, pp. 4691–4697, 2017. doi: https://doi.org/10.24963/ijcai.2017/654
53. S. Savchenko and V. Kobets, "Development of Robo-Advisor System for Personalized Investment and Insurance Portfolio Generation," In: O. Ignatenko et al., Eds., ICTERI 2021 Workshops. ICTERI 2021. Communications in Computer and Information Science, vol. 1635, Springer, Cham, 2022. doi: https://doi.org/10.1007/978-3-031-14841-5_14
54. K. Waliszewski and A. Warchlewska, "Financial technologies in personal financial planning: robo-advice vs. human-advice," Ruch Prawniczy, Ekonomiczny i Socjologiczny, vol. 4, pp. 303–317, 2020. [Online]. Available: https://doi.org/10.14746/rpeis.2020.82.4.22
55. M. Kearns and A. Roth, *The Ethical Algorithm: The Science of Socially Aware Algorithm Design*. Oxford University Press, Oxford, 2019.
56. D. McDuff, R. Cheng, and A. Kapoor, "Identifying bias in AI using simulation," arXiv:1810.00471, 2018.
57. N. Mehrabi, F. Morstatter, N. Saxena, K. Lerman, and A. Galstyan, "A survey on bias and fairness in machine learning," ACM Comput. Surv., vol. 54, no. 6, pp. 1–35, 2021.
58. J. Mökander and L. Floridi, "From algorithmic accountability to digital governance," Nature Machine Intelligence, vol. 4, pp. 508–509, 2022. [Online]. Available: https://doi.org/10.1038/s42256-022-00504-5
59. J. Kleinberg, "Inherent Trade-Offs in Algorithmic Fairness," 2018. [Online]. Available: https://doi.org/10.1145/3219617.3219634
60. J. H. Plikas, P. Trakadas, and D. Kenourgios, "Assessing the Ethical Implications of Artificial Intelligence (AI) and Machine Learning (ML) on Job Displacement Through Automation: A Critical Analysis of Their Impact on Society," in *Frontiers of Artificial Intelligence, Ethics, and Multidisciplinary Applications*, FAIEMA 2023, M. Farmanbar, M. Tzamtzi, A. K. Verma, and A. Chakravorty, Eds. Springer, Singapore, 2024. [Online]. Available: https://doi.org/10.1007/978-981-99-9836-4_24
61. M. J. Idrisi, D. Geteye, and P. Shanmugasundaram, "Modeling the Complex Interplay: Dynamics of Job Displacement and Evolution of Artificial Intelligence in a Socio-Economic Landscape," Int J Netw Distrib Comput, 2024. [Online]. Available: https://doi.org/10.1007/s44227-024-00025-0
62. Y. J. An, P. M. S. Choi, and S. H. Huang, "Blockchain, cryptocurrency, and artificial intelligence in finance," in *Fintech with Artificial Intelligence, Big Data, and Blockchain*, P. M. S. Choi and S. H. Huang, Eds.

Springer, Singapore, 2021, pp. 1–34. [Online]. Available: https://doi.org/10.1007/978-981-33-6137-9_1
63. Goldman Sachs, "Generative AI could raise global GDP by 7
64. Gartner, "4 Emerging Technologies You Need to Know About," 2023. [Online]. Available: https://www.gartner.com/en/articles/4-emerging-technologies-you-need-to-know-about
65. Deloitte, "Explain Artificial Intelligence for Credit Risk Management." [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/fr/Documents/risk/Publications/deloitte_artificial-intelligence-credit-risk.pdf
66. P. Pilaniwala, "How AI is changing Commerce Platforms globally," Apr. 2024. [Online]. Available: https://aijourn.com/how-ai-is-changing-commerce-platforms-globally/
67. R. Bartlett, A. Morse, R. Stanton, and N. Wallace, "Consumer-Lending Discrimination in the FinTech Era," National Bureau of Economic Research Working Paper Series, vol. 25943, June 2019. doi: 10.3386/w25943
68. LenddoEFL, "Unlocking Better Decision with alternate data." [Online]. Available: https://static1.squarespace.com/static/59d7c8fc8a02c7612c9b60e3/t/60a1fb41247e7c5dd13bedfe/1621228375951/LenddoEFL_Scoring+Brochure_20201.pdf
69. YData, "How AI assists banks and financial institutions in enhancing financial inclusivity," Nov. 23, 2022. [Online]. Available: https://ydata.ai/resources/the-impact-of-artificial-intelligence-on-financial-inclusion
70. E. Martinez and L. Kirchner, "How We Investigated Racial Disparities in Federal Mortgage Data," Aug. 25, 2021. [Online]. Available: https://themarkup.org/show-your-work/2021/08/25/how-we-investigated-racial-disparities-in-federal-mortgage-data#:~:text=We%20found%20that%20nationwide,the%20same%20financial%20characteristics
71. J. Ma, "JPMorgan will play more 'Moneyball' as the Wall Street giant expands use of an AI tool to help portfolio managers 'correct for bias'," Finance AI, June 2, 2024. [Online]. Available: https://fortune.com/2024/06/02/jpmorgan-generative-artificial-intelligence-moneyball-ai-tool-investment-decisions-jamie-dimon/
72. Juniper Research, "Bank cost savings via chatbots reach $7.3bn by 2023," Feb. 20, 2019. [Online]. Available: https://www.juniperresearch.com/press/bank-cost-savings-via-chatbots-reach-7-3bn-2023#:~:text=A%20new%20study,million%20working%20years
73. AI Case Study, "Danske Bank Fights Fraud with Deep Learning and AI." [Online]. Available: https://assets.teradata.com/resourceCenter/downloads/CaseStudies/CaseStudy_EB9821_Danske_Bank_Fights_Fraud.pdf
74. LiveCaller AI, "AI Phone Agents A Key To Expanding Financial Services In Rural Areas," Feb. 24, 2024. [Online]. Available: https://livecaller.ai/using-ai-phone-agents-to-expand-financial-services-in-rural-areas/
75. W. Knight, "The Apple Card Didn't 'See' Gender—and That's the Problem," Nov. 19, 2019. [Online]. Available: https://www.wired.com/story/the-apple-card-didnt-see-genderand-thats-the-problem/
76. K. Benner, G. Thrush, and M. Isaac, "Facebook Engages in Housing Discrimination With Its Ad Practices, U.S. Says," New York Times, Mar. 28, 2019. [Online]. Available: https://www.nytimes.com/2019/03/28/us/politics/facebook-housing-discrimination.html
77. M. Faverio, "Key findings about Americans and data privacy," Pew Research Center, Oct. 18, 2023. [Online]. Available: https://www.pewresearch.org/short-reads/2023/10/18/key-findings-about-americans-and-data-privacy/
78. A. Tyson and B. Kennedy, "Many Americans think generative AI programs should credit the sources they rely on," Pew Research Center, Mar. 26, 2024. [Online]. Available: https://www.pewresearch.org/short-reads/2024/03/26/many-americans-think-generative-ai-programs-should-credit-the-sources-they-rely-on/
79. A. Tyson and E. Kikuchi, "Growing public concern about the role of artificial intelligence in daily life," Pew Research Center, Aug. 28, 2023. [Online]. Available: https://www.pewresearch.org/short-reads/2023/08/28/growing-public-concern-about-the-role-of-artificial-intelligence-in-daily-life/
80. C. Sandvig, K. Hamilton, K. Karahalios, and C. Langbort, "Auditing Algorithms: Research Methods for Detecting Discrimination on Internet Platforms," 2014. [Online]. Available: https://api.semanticscholar.org/CorpusID:15686114
81. B. D. Mittelstadt, P. Allo, M. Taddeo, S. Wachter, and L. Floridi, "The ethics of algorithms: Mapping the debate," Big Data & Society, vol. 3, no. 2, 2016. [Online]. Available: https://doi.org/10.1177/2053951716679679
82. B. G. Edelman and M. Luca, "Digital Discrimination: The Case of Airbnb.com," Harvard Business School NOM Unit Working Paper No. 14-054, Jan. 10, 2014. [Online]. Available: http://dx.doi.org/10.2139/ssrn.2377353

83. F. A. Pasquale, "Restoring Transparency to Automated Authority," Journal on Telecommunications and High Technology Law, vol. 9, no. 235, 2011. [Online]. Available: https://ssrn.com/abstract=1762766
84. J. Mökander, "Auditing of AI: Legal, Ethical and Technical Approaches," DISO, vol. 2, p. 49, 2023. [Online]. Available: https://doi.org/10.1007/s44206-023-00074-y
85. A. Jobin, M. Ienca, and E. Vayena, "The global landscape of AI ethics guidelines," Nat Mach Intell, vol. 1, pp. 389–399, 2019. [Online]. Available: https://doi.org/10.1038/s42256-019-0088-2
86. E. Flitter and G. Thrush, "Wells Fargo Said to Be Target of $1 Billion U.S. Fine," The New York Times, Apr. 19, 2018. [Online]. Available: https://www.nytimes.com/2018/04/19/business/wells-fargo-cfpb-penalty.html
87. Wally, [Online]. Available: https://www.wally.tech/
88. R. Clymo, "Wally personal finance review," Techradar, Sep. 29, 2020. [Online]. Available: https://www.techradar.com/reviews/wally-personal-finance

Article Type: Report

Artificial Intelligence in Cybersecurity: LLMs for Securing the Digital World

Swagata Ashwani, *Principle Data Scientist, Boomi Inc., USA*

Shivendra Srivastava, *Software Development Manager, AWS Amazon Inc., USA*

Abstract—This paper thoroughly explores the role of Artificial Intelligence in Cybersecurity, delving into how Artificial Intelligence can alter the way we secure our digital world. LLMs have opened new avenues in bolstering security and enabling companies to ensure that intrusion is detected and defensive measures are activated sooner than what was earlier possible. This paper evaluates the existing methods, and gaps in today's systems that can be mitigated with the help of LLMs and Artificial Intelligence.

Cybersecurity refers to the practice of protecting computer systems, networks, individuals from digital attacks, theft, phishing attacks, and unauthorized access. In the past couple of years the field of machine learning and artificial intelligence has changed the way companies and individuals think about cybersecurity. According to a report from Accenture [2], 74% of CEOs are concerned about their organization's ability to eliminate or reduce the threat of an attack. Cyber crime reports from the Federal Bureau of Investigation indicate that the IC3 [1] (Internet Crime Complaint Center) received 800,944 complaints, a 5% decrease from 2021 but an increase in potential loss from $6.9 billion in 2021 to $10.2 billion in 2022. These are only ransomware incidents that are a threat to the public and to the economy. From 2018 to 2022 IC3 received a total of 3.26 million complaints with an estimated loss of $27.6 billion and out of all the complaints the biggest chunk was for phishing. Cybercrime Magazine predicts that the next 5 years will see an increase of 15% in cybercrime costs reaching 10.5 trillion by 2025. This only emphasizes the need of more cybers security specialists, methods to stop cyber criminals from wreaking havoc in people's lives and the economy.

Traditional Methodologies

Traditionally, companies, security professionals gather information about threats from publicly available sources such as Open-Source Intelligence (OSINT), and leverage Human Intelligence (HUMINT), Technical Intelligence (TECHINT), and SIGINT (Signals Intelligence) Analysts used OSINT to grasp tactics, techniques, and procedures used by adversaries and also understand potential vulnerabilities in systems. HUMINT involves leveraging informants, specialized knowledge individuals who can help gather insider information. Analysts use TECHINT to understand the technological aspects of attacks such as malware behavior, patterns, etc. SIGINT helps analysts intercept communication, and signals to understand the intentions and uncover potential threats to organizations, nations, and people.

Any organization has a culmination of all the above mentioned methodologies that help in intercepting, detecting, and avoiding security threats and ensuring data security, and integrity.

Artificial Intelligence and Machine Learning in Cybersecurity

Machine Learning and Artificial Intelligence play pivotal roles in Cybersecurity. Machine learning provides ways for analysts, organizations, entities to predict the occurrence as well as predict the response. Machine learning algorithms analyze and report system vulnerabilities and also predict possible breach points in an entity's security layer. Artificial Intelligence on the other hand can enable the management of system weaknesses. Machine learning when coupled with AI can enable predictive analysis, regular and automatic categorization of security threats based on past data and also formulate response strategies that enable more robust responses to any security incidents. We will now look at the various aspects in which Machine Learning and Artificial Intelligence have changed the landscape of Cybersecurity.

Threat Intelligence

The integration of Artificial Intelligence (AI) technologies has profoundly transformed threat intelligence. AI, including machine learning and natural language processing, automates and analyzes extensive data, revolutionizing how organizations perceive and respond to cyber threats. Machine learning rapidly processes large datasets, detecting anomalies indicative of potential threats. NLP-based AI enhances contextual understanding of unstructured data, improving threat detection speed. Incorporating AI algorithms into traditional methodologies strengthens the ability to detect and predict evolving threats. AI-driven predictive analytics use historical data to forecast potential threats, empowering swift and informed decision-making. Despite challenges, AI augments human processes, streamlining response workflows and minimizing manual intervention. A key component of robust threat intelligence is the ability to detect, classify and learn from threats quickly.

Threat Detection

In threat hunting, supervised learning techniques have gained prominence for bolstering detection capabilities. This approach entails training a model on labeled data, enabling it to discern patterns and anomalies linked to known threats, thus enhancing threat identification and response effectiveness. This exploration delves into the application of supervised learning in threat detection within the context of threat hunting. Leveraging historical data, supervised learning utilizes labeled examples to train algorithms, allowing the creation of models adept at distinguishing normal and abnormal behavior. Employing methods like classification and regression, algorithms such as Support Vector Machines and Random Forests predict threats based on predefined features, significantly improving detection accuracy and efficiency. These models excel at identifying intricate threat patterns challenging for traditional systems. Furthermore, they expedite response times by swiftly pinpointing potential threats in extensive datasets, while continuous learning enables adaptation to evolving threats.

Furthermore, anomaly detection is crucial for identifying irregular patterns within a system. This is where Unsupervised learning comes into play. Unsupervised learning, free from labeled data, proves effective in discerning anomalies by recognizing significant deviations from norms. Techniques like clustering, autoencoders, and principal component analysis play a vital role in this detection, grouping similar data points, highlighting irregular instances, and aiding in dimensionality reduction. Applied in network security, unsupervised learning identifies suspicious activities, while behavioral analysis spots abnormal user behaviors indicating insider threats. Additionally, system logs benefit from anomaly detection to pinpoint potential malware activities or breaches.

While the above two techniques and others such as Reinforced learning, etc. work for structured data, they do not work well for unstructured data. This is where NLPs come into play. Natural Language Processing (NLP) enables extracting threat intelligence from diverse unstructured data sources, including social media, dark web forums, and incident reports. NLP's contribution involves employing various techniques to parse, comprehend, and categorize unstructured data. Named Entity Recognition (NER) and sentiment analysis stand out as key NLP methods, identifying entities and sentiments within text data. Cybersecurity analysts leverage NLP to efficiently process extensive volumes of text-based data, aiding in the swift identification of potential threats and vulnerabilities within an organization's digital infrastructure. Moreover, NLP-powered algorithms facilitate the extraction of indicators of compromise (IOCs) from unstructured data sources, crucial for identifying potential cyber threats. These IOCs, encompassing IP addresses, malware signatures, and suspicious URLs, play a critical role in proactively fortifying networks against cyberattacks. an organization's overall security.

Challenges of AI based Threat Intelligence and Detection

Models like deep learning neural networks have demonstrated commendable scalability, efficiently handling vast datasets. Architectural advancements, such as distributed computing frameworks like TensorFlow and PyTorch, contribute significantly to enhancing scalability by distributing computations across multiple processors or devices. Additionally, the emergence of cloud computing platforms enables easy access to scalable computational resources, facilitating the deployment of AI models in various applications. The adaptability of AI models is crucial in ensuring their relevance in dynamic environments. However, not every organization/entity has the required resources to invest in AI model training, and tuning for their own use cases. This challenge is at the forefront of easy adoption of AI based threat intelligence models and technologies.

To enable organizations and entities of all sizes to benefit and leverage from AI based threat detection

it is important that local, state, provincial and federal governments fund the creation of models that can be tuned for customer specific use cases. Organizations such as IC3/FBI, MITRE, NIST, CERT or Universities can be at the forefront of such an initiative.

An AI model that learns from the vast dataset of complaints that the IC3 has along with data from OSINT, etc. could be a great asset for organizations and entities to be prepared against any cyberthreats.

SecureBERT

SecureBERT [3] is a domain specific language model for Cybersecurity. This model is capable of capturing text connotations in cybersecurity text (CTI) and therefore successful in automation of critical cybersecurity tasks that would otherwise rely on laborious manual intervention. on data from a decade's worth of resumes, most of which were submitted by men, leading it to favor male candidates. This case serves as a cautionary tale about the potential for AI to perpetuate existing biases if not carefully monitored and corrected.

SecureBERT leverages BERT (Bidirectional Encoder Representations from Transformers). BERT is a transformer based neural network technique used for pre-training. The traditional way of training is to use an ordered sequence of words but BERT can train LLMs on the entire set of words in a sentence or query.

SecureBERT surpasses existing language models in predicting cybersecurity-related masked tokens within texts, showcasing its capacity to comprehend and interpret domain-specific content. To bolster its efficacy while maintaining a broad understanding of language, we implemented tailored techniques such as crafting custom tokenizers and adjusting weights.

SecureBERT employs a potent weight modification approach by introducing slight noise to the initial weights of the pre-trained model. This adjustment proves beneficial when training on a smaller corpus compared to readily available large-scale models, enabling SecureBERT to adeptly fit the cybersecurity context, particularly in grasping homographs and phrases with diverse meanings across domains. By introducing noise, this method displaces the token within a divergent space, facilitating more effective adjustment of embedding weights by the algorithm. As an example SecureBERT is able to accurately predict the result of a virus. Using other language models the result could be that virus causes illness, however SecureBERT predicts accurately that Virus can cause a problem or a crash inline with what is expected from a cybersecurity based LLM. SecureBERT has shown to perform significantly better than existing models like RoBERTa, SciBERT, and SecBERT. SecureBERT has also been uploaded to the Huggingface framework so developers and security engineers can use it to test out how it works.

SecureBERT represents the shift in cybersecurity engineering. Developers can leverage the model and deploy it to monitor threats, tune it with company specific data and then leverage SecureBERT to figure out anomalies that could be leveraged by malicious entities to gain access to the data and cause havoc.

Let's take a look at its use cases and how teams, individuals and governments can use it to strengthen their security in cyberspace.

Phishing Detection: SecureBERT can be used to identify phishing attempts in emails, websites, or other communication channels. By analyzing text content it can help and detect suspicious and/or malicious messages.

Code and Malware Analysis: When applied to code snippets or malware samples, SecureBERT can extract relevant information and identify potential threats. It can also help in understanding the intent and behavior of the code that can provide valuable insights that may be otherwise very tedious to find out.

Intrusion Detection: SecureBERT can assist in detecting unauthorized access attempts or suspicious activities within a network by analyzing network traffic anomalies, and patterns that indicate possible intrusions.

Text Classification: SecureBERT serves as a base model for various downstream tasks, including text classification. Automatic classification into threat levels and attack types are possible without having to write lots of code that would then need to be tested. Named Entity Recognition (NER): SecureBERT can extract entities such as IP addresses, domain names, or software names from unstructured text.

Question Answering (QA): SecureBERT can answer specific questions related to cybersecurity topics. This is very beneficial in organizational settings where SecureBERT could help in conducting training and quizzes and also answering questions for new and existing employees whenever they have questions regarding a possible threat.

Conclusion

The usage of such models to secure organizations is only going to increase. As Generative AI and its usage increases it is important for organizations and individuals to leverage such models to keep their data safe and systems away from any malicious entities.

REFERENCES

1. 2023 INTERNET CRIME REPORT. (2024, March 6). Internet Crime Complaint Center(IC3). Retrieved March 19, 2024, from https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf
2. Accenture's Cyber-Resilient CEO Report. (2023, October 5). Newsroom | Accenture. Retrieved March 19, 2024, from https://newsroom.accenture.com/news/2023/ceos-lack-confidence-in-their-organizations-ability-to-protect-against-cyberattacks-despite-seeing-cybersecurity-as-vital-to-growth-accenture-report-finds
3. SecureBERT: A Domain-Specific Language Model for Cybersecurity. (2022, April 6). arXiv. Retrieved March 19, 2024, from https://arxiv.org/abs/2204.02685

Swagata Ashwani is currently working as a Principal Data Scientist at Boomi. She received her Master's degree in Data Science from Carnegie Mellon University in 2018. She is an avid blogger and writes about state of the art developments in the AI space. She is particularly interested in Natural Language Processing and focuses on researching how to make NLP models work in a practical setting.

Shivendra Srivastava is currently with AWS, Seattle, WA, USA. Author's latest degree received is the M.S. in Computer Science from Georgia Institute of Technology. Author's research interests are cloud computing, machine learning and generative AI. He is a member of the IEEE and the IEEE Computer Society.

Article Type: Research

Methodology for Financial Market Anomalies: Leveraging AI/ML in SnowFlake for Early Crash Detection and Proactive Risk Mitigation

Karthik Rajashekaran, *New York University, USA*

Abstract—Financial markets are susceptible to the anomalies that lead to significant disruptions, including the crashes. Detecting these anomalies early along with implementing proactive mitigation strategies is crucial for maintaining the stability as well as safeguarding investor interests. In this study, we proposed methodology utilizing artificial intelligence (AI) along with machine learning (ML) techniques within Snowflake platform for early crash detection along with proactive mitigation in the financial markets. We utilize credit card fraud detection dataset in order to demonstrate effectiveness of our approach. Our methodology involves preprocessing dataset, selecting appropriate AI/ML models, training as well as evaluating these models, along with leveraging Snowflake for the data processing, storage, as well as analysis. We employed support vector machine (SVM) as well as random forest (RF) algorithms for ML, and convolutional neural networks (CNNs) along with recurrent neural networks (RNNs) for deep learning. Evaluation metrics including accuracy, precision, recall, F1-score, as well as area under ROC curve (AUC-ROC) are used in order to assess performance of proposed models. Our results show that SVM offers promising capabilities for early crash detection along with proactive mitigation in the financial markets, thereby enhancing resilience as well as reducing potential risks.

THE financial markets are inherently complex as well as dynamic systems, thus susceptible to several anomalies along with fluctuations that lead to significant economic consequences. The cabability to detect as well as mitigate these anomalies early is paramount for safeguarding the market stability along with investor confidence [1]. Traditional methods of the anomaly detection struggle in order to keep pace with speed along with scale of the modern financial markets, necessitating innovative approaches that leverages the advanced technologies. In recent years, integration of the artificial intelligence (AI) along with machine learning (ML) techniques has emerged as promising solution for enhancing the anomaly detection capabilities in financial markets [2]. By utilizing power of the AI as well as ML algorithms, analysts sift through the vast amounts of data, uncover hidden

patterns, along with identifying potential anomalies with greater accuracy as well as efficiency. In addition to this, advent of cloud computing platforms has revolutionized the data management as well as analysis, thus providing scalable infrastructure along with advanced analytics tools for processing the large datasets in real-time. Among these platforms, Snowflake outperforms others due its ability of handling diverse data sources, supporting complex analytics workloads, along with facilitating seamless collaboration among users [3].

In this research paper, we propose methodology for financial market anomaly detection that harnesses capabilities of AI/ML techniques within Snowflake platform. Specifically, we focus on the early crash detection along with proactive mitigation strategies in order to mitigate impact of the market disruptions. While our approach is generalizable to several financial instruments, we have chosen to illustrate its efficacy using credit card fraud detection dataset as proxy for the market anomalies [4]. Through this proposed research, we aim to demonstrate potential of the AI/ML in Snowflake in order to enhance early warning systems present in financial markets, thus enabling stakeholders to take timely as well as informed actions in order to mitigate risks along with preserving market stability. By combining the cutting-edge technology with robust data management practices, we endeavor for contributing

to ongoing efforts in order to build resilient along with adaptive financial systems in increasingly interconnected world. The main key points of our proposed research are given below:

- Innovative Approach: Introducing novel methodology for the financial market anomaly detection utilizing AI/ML techniques within Snowflake platform.
- Early Crash Detection: Focus on early detection of the market anomalies, specifically targeting crashes, in order to enable the proactive mitigation strategies.
- Real-world Application: Demonstrating applicability of proposed methodology by using credit card fraud detection dataset as proxy for the financial market anomalies.

The remainder of research is structured as follows: Section provides overview of the existing research related to credit card fraud detection, thus outlining several methodologies as well as techniques utilized. In Section , we presented our novel approach leveraging AI/ML techniques within Snowflake platform for the early crash detection along with proactive mitigation in the financial markets, with particular focus on the credit card fraud detection. Following this, the Section details experimental setup, thus including data preprocessing techniques as well as model selection, along with presenting results as well as analysis of our proposed ML and DL models. We evaluated performance of these proposed models using the key metrics like accuracy, precision, recall, and F1-score. Finally, Section concludes our research by summarizing key findings, discussing implications of results, along with suggesting potential avenues for the future research in domain of the financial market anomaly detection as well as fraud prevention.

Related Work

Financial markets are regarded as complex systems characterized by the inherent uncertainties, fluctuations, along with occasional anomalies that have significant repercussions on the global economies. The literature on the financial market anomaly detection has witnessed considerable growth as researchers along with practitioners seeking effective strategies in order to identify as well as mitigate these anomalies in timely manner [5].

Traditional approaches for anomaly detection in financial markets relied on the statistical methods as well as expert-driven rules, which were limited in their ability in order to adapt for evolving market dynamics as well as detect subtle anomalies. However, emergence of the AI along with ML techniques has revolutionized anomaly detection by enabling the automated analysis of vast volumes of market data along with uncovering hidden patterns that indicate anomalous behavior [6].

The [7] is related to comprehensive review of several techniques along with approaches used for the credit card fraud detection. It includes wide range of methods like artificial immune systems, genetic algorithms, neural networks, SVM, Bayesian networks, RF, as well as hybrid approaches [8]. The review covers the research papers, conference proceedings, as well as academic thesis from several years as well as locations, thus providing broad overview of evolving landscape of credit card fraud detection models.

Importance of preventing credit card fraud as well as need to research the fraudulent actions in order to reduce occurrence of such incidents is presented in [9]. It emphasized difficulty in detecting the fraud because of imbalance between legitimate as well as fraudulent transactions, along with changing nature of the fraudulent behavior over time. The paper also mentioned usage of automated technology in order to address this issue [10]. Several studies have explored application of AI/ML techniques in the financial market anomaly detection, thus highlighting their effectiveness in identifying the various types of anomalies, including but not limited to sudden price movements, irregular trading patterns, as well as systemic risks [11]. In [12] employed deep learning models for detecting financial fraud as well as market manipulation, thus achieving high accuracy along with robustness in identifying the fraudulent activities. Moreover, integration of the cloud computing platforms, like Snowflake, has further enhanced scalability along with efficiency of the anomaly detection systems by providing the flexible infrastructure for processing as well as analyzing large-scale datasets in the real-time [13]. Snowflake's architecture allows for the seamless integration with AI/ML algorithms, thus enabling analysts to utilize advanced analytics capabilities for detecting the anomalies across diverse financial instruments as well as markets.

Despite these advancements, challenges still remain in developing the robust anomaly detection systems that can adapt to changing market conditions along with evolving threat landscapes [14]. Summary of key findings are illustrated in Table 1. In addition to this, ethical implications of the automated anomaly detection, including privacy concerns as well as potential biases in algorithmic decision-making, warrant careful consideration in design along with deployment of such systems. This study aims to contribute to ongoing

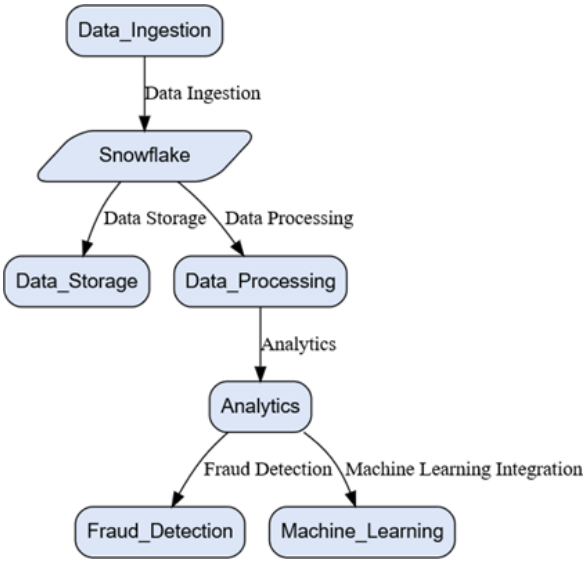

FIGURE 1. Proposed Methodology for Credit Card Fraud Detection

efforts in order to develop resilient along with adaptive financial systems capable of navigating complexities of the modern markets [15].

Proposed Methodology

The proposed methodology for credit card fraud detection is illustrated in Figure 1. The steps adopted to perform the proposed methodology are explained in subsequent sections.

Data Collection and Description

The proposed dataset comprises simulated financial transaction data that span 30-day period, with each and every step representing an hour of the real-world time. Each transaction is further categorized by type, which include CASH-IN, CASH-OUT, DEBIT, PAYMENT, as well as TRANSFER, and is associated with the amount denotin transaction value in local currency. Transaction details includes initiator's as well as recipient's identities, thus denoted by "nameOrig" as well as "nameDest" respectively, as well as their respective account balances before & after transaction. Recipient accounts that starts with "M" are identified as the merchants along with having limited information available. Two crucial flags are present in the proposed datset, "isFraud" and "isFlaggedFraud," that provide insights in fraudulent activity present within the proposed dataset. "isFraud" indicates the transactions conducted by fraudulent agents, thus aiming to exploit the customer accounts, while "isFlaggedFraud" marks those attempts flagged as illegal by business model, involving transactions exceeding the 200,000 units in single transfer. This proposed comprehensive dataset presents opportunity in order to explore patterns of the fraudulent behavior along with developing robust models for fraud detection as well as prevention in the financial transactions.

Data Preprocessing

In preprocessing proposed financial transaction dataset, various steps were undertaken in order to ensure its suitability for analysis along with modeling. Initially, missing values are addressed by dropping rows along with their respective features. Feature engineering was then applied in order to derive new features for capturing relevant information, like calculating difference present between old & new balances to gauge changes present in the account balances. Categorical variables, which includes transaction types along with customer identities, were converted in numerical representations using techniques like one-hot encoding. In addition to this, numerical features underwent normalization to bring them to similar scale, thus enhancing performance of the ML algorithms. Class imbalance in target variable "isFraud" was addressed through synthetic data generation for ensuring balanced representation. Outliers were identified as well as removed using statistical methods like z-scores and interquartile range (IQR), while feature selection techniques like correlation analysis along with feature importance ranking were employed for selecting most informative features for modeling. Finally, proposed dataset was split in training, validation, as well as test sets to accurately evaluate the model performance. These preprocessing steps collectively prepared financial transaction dataset for the effective analysis along with modeling, thus ensuring that it was clean, relevant, as well as conducive for building robust fraud detection models. The statistics of our proposed dataset are illustrated in Table 2.

Utilizing Snowflake for Data Processing, Storage, & Analysis

Utilizing Snowflake for performing data processing, storage, as well as analysis offers various advantages for fraud detection in financial transactions.

Snowflake's cloud-based architecture provides the scalability along with flexibility, thus allowing for seam-

Research Contribution	Key Findings
[5]	Traditional approaches to anomaly detection in financial markets were limited; AI and ML techniques have revolutionized anomaly detection by enabling automated analysis of vast volumes of market data and uncovering hidden patterns.
[6]	Comprehensive review of techniques and approaches for credit card fraud detection, including AI/ML methods such as artificial immune systems, genetic algorithms, neural networks, SVM, Bayesian networks, and RF.
[7]	Importance of preventing credit card fraud and difficulty in detection due to imbalance between legitimate and fraudulent transactions; emphasizes the usage of automated technology to address this issue.
[11]	Exploration of AI/ML techniques for financial market anomaly detection, highlighting their effectiveness in identifying various types of anomalies such as sudden price movements, irregular trading patterns, and systemic risks.
[12]	Utilization of deep learning models for detecting financial fraud and market manipulation, achieving high accuracy and robustness in identifying fraudulent activities.
[13]	Integration of cloud computing platforms like Snowflake has enhanced scalability and efficiency of anomaly detection systems by providing flexible infrastructure for processing and analyzing large-scale datasets in real-time.
[14]	Challenges remain in developing robust anomaly detection systems that can adapt to changing market conditions and evolving threat landscapes; ethical implications of automated anomaly detection, including privacy concerns and potential biases in algorithmic decision-making, warrant careful consideration.

TABLE 1. Summary of Literature on Financial Market Anomaly Detection

less handling of the large volumes of transaction data. With Snowflake's data warehouse capabilities, the financial institutions efficiently store vast amounts of transactional data securely in the centralized repository. Snowflake's data processing features enables fast along with reliable data ingestion, transformation, as well as querying, thus facilitating real-time analysis of the transactional patterns along with anomalies. In addition to this, Snowflake's support for several programming languages along with integration with popular machine learning as well as deep learning frameworks, thus enabling data scientists for developing along with deploying sophisticated fraud detection models directly within Snowflake environment. Additionally, Snowflake's built-in security features, like encryption as well as access controls, ensure integrity along with confidentiality of the sensitive financial data throughout analysis process. By utilizing Snowflake's robust data management as well as analytics capabilities, financial institutions enhance their fraud detection capabilities, identify fraudulent activities more effectively, along with safeguarding their customers' assets against the fraudulent transactions.

Machine and Deep Learning Models Deployment

In model selection phase for the fraud detection, two machine learning models along with two deep learning models were modelled. Random Forest (RF) was chosen as one of ML models. RF is ensemble learning method that constructs the multiple decision trees during the training as well as outputs mode of classes.

$$\mathrm{RF}(x) = \mathrm{mode}\{\mathrm{DT}_1(x), \mathrm{DT}_2(x), \ldots, \mathrm{DT}_n(x)\}$$

Support Vector Machine (SVM) was developed as an- other ML model. SVM is powerful supervised learning algorithm used for the classification tasks, particularly effective in the high-dimensional spaces.

$$\mathrm{SVM}(x) = \mathrm{sign}(w^T x + b)$$

For DL models, Convolutional Neural Network (CNN) as well as Long Short-Term Memory (LSTM) networks were developed. CNNs are adept at automatically learning the hierarchical features from sequential data, thus making them suitable for analyzing the transaction data.

$$y = \mathrm{CNN}(x) = \sigma(W * x + b)$$

LSTM networks, on other hand, excel in capturing the long-range dependencies in sequential data, like temporal patterns in the financial transactions.

$$
\begin{aligned}
i_t &= \sigma(W_i[x_t, h_{t-1}] + b_i) \\
f_t &= \sigma(W_f[x_t, h_{t-1}] + b_f) \\
o_t &= \sigma(W_o[x_t, h_{t-1}] + b_o) \\
c_t &= f_t \odot c_{t-1} + i_t \odot \tanh(W_c[x_t, h_{t-1}] + b_c) \\
h_t &= o_t \odot \tanh(c_t)
\end{aligned}
$$

Evaluation Metrics

Evaluation metrics are essential in order to assess performance of the fraud detection models in financial transactions. The metrics include accuracy, precision, recall, F1-score, confusion matrix, as well as area under Receiver Operating Characteristic (ROC) curve (AUC-ROC). These metrics provide insights in different aspects of model's performance, thus allowing stakeholders to make the informed decisions related to fraud detection strategies.

Accuracy (ACC): Accuracy measures proportion of the correctly classified instances out of total number of instances in dataset. It is calculated as follows:

$$\text{ACC} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}}$$

Where:

- TP = True Positives (correctly identified fraud cases)
- TN = True Negatives (correctly identified non-fraud cases)
- FP = False Positives (incorrectly identified as fraud cases)
- FN = False Negatives (incorrectly identified as non-fraud cases)

Precision (PRC): Precision measures proportion of the correctly identified fraud cases out of all the instances classified as fraud. It is calculated as follows:

$$\text{PRC} = \frac{\text{TP}}{\text{TP} + \text{FP}}$$

Recall (REC) or True Positive Rate (TPR): Recall, also known as the True Positive Rate (TPR), measures proportion of the correctly identified fraud cases out of all the actual fraud cases in proposed dataset. It is calculated as follows:

$$\text{REC} = \text{TPR} = \frac{\text{TP}}{\text{TP} + \text{FN}}$$

F1-score: F1-score is harmonic mean of the precision as well as recall. It provides balance between the precision as well as recall. It is useful when class distribution is imbalanced. It is calculated as follows:

$$\text{F1} = 2 \times \frac{\text{PRC} \times \text{REC}}{\text{PRC} + \text{REC}}$$

Area Under the ROC curve (AUC-ROC): ROC curve is graphical representation of true positive rate (TPR) against false positive rate (FPR) at several threshold settings. The AUC-ROC represents area under ROC curve as well as measures model's ability in order to distinguish between the classes. A value close to 1 indicates excellent discrimination ability, while value close to 0.5 represent poor discrimination.

$$\text{AUC-ROC} = \int_0^1 \text{TPR}(\text{FPR})\, d\text{FPR}$$

By utilizing a combination of these evaluation metrics and models, the fraud detection system can effectively identify and mitigate fraudulent activities in financial transactions, thereby safeguarding the integrity of financial systems and protecting stakeholders from financial losses.

Experimental Results

There are several mode of transactions present in our dataset that are depicted in Figure 2. The Figure 2 shows that PAYMENT mode is adopted by most of the users followed by Cash_Out, Transfer, Cash_In and Debit respectively. The boxplot of proposed dataset is illustrated in Figure 3. The Figure 3 illustrates that the outliers are mostly present in Cash_Out mode of transfer followed by Transfer mode.

Histogram of the column "Amount" present in dataset is illustrated in Figure 4 that shows the variation of cash among different users at different timestamps.

The correlation matrix of our proposed dataset is illustrated in Figure 5. The Figure 5 depicts that the amount and step has high impact on fraudulent activities.

The Table 3 presents evaluation metrics for 4 different models employed in proposed study: SVM, RF, CNN, and LSTM. Each model is assessed based on 4 key metrics: ACC, PRC, REC, and F1-Score. ACC reflects overall correctness of model's predictions, thus indicating proportion of the correctly classified instances out of total instances. The highest accuracy of 0.98 is achieved by SVM model, thus showcasing its ability to accurately classify fraudulent transactions. PRC measures model's ability to avoid the false positives by calculating proportion of true positive predictions out of all the positive predictions. Both SVM as

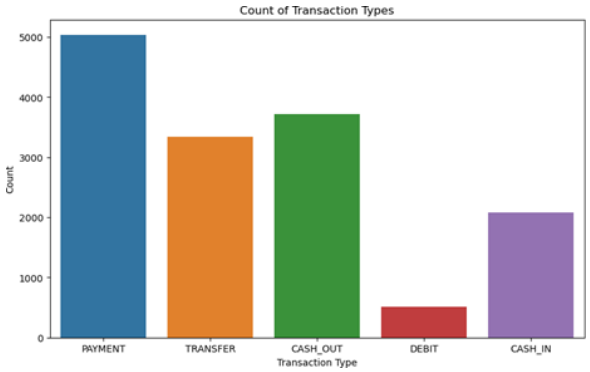

FIGURE 2. Mode of Transactions present in Credit Card Fraud Detection Dataset

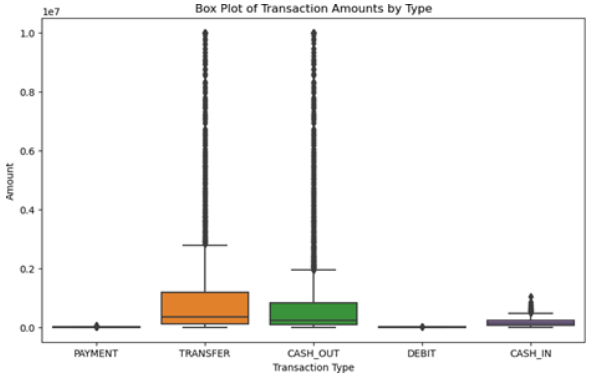

FIGURE 3. BoxPlot of Credit Card Fraud Dataset

well as LSTM exhibit high precision scores of 0.96 & 0.94, respectively, thus indicating their proficiency in minimizing false positives. RCC quantifies model's capability in order to capture all the actual positive instances in the proposed dataset. SVM as well as LSTM achieve recall score of 0.91, thus implying that they effectively identify approximately 1% of fraudulent transactions, thereby minimizing the false negatives. F1 Score, being harmonic mean of precision & recall, provides balanced assessment of model's performance. SVM & LSTM attain highest F1 scores of 0.92 & 0.93, respectively, thus indicating their robustness in achieving balance between precision as well as recall. Overall, Table 3 underscores effectiveness of SVM & LSTM models in detecting the credit card fraud, showcasing their superior performance across the multiple evaluation metrics. These findings contribute valuable insights in case of deploying the efficient fraud detection systems in financial institutions, thereby enhancing security along with mitigating potential risks associated with the fraudulent activities.

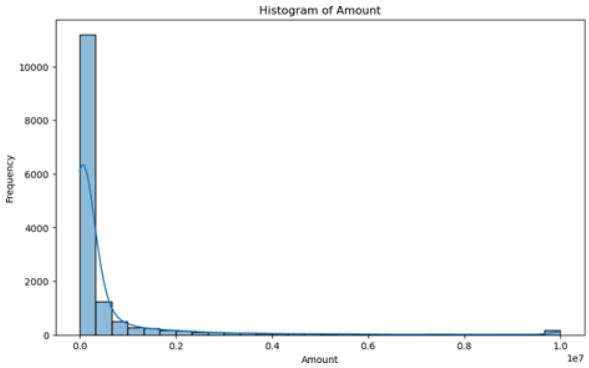

FIGURE 4. Histogram of Amount Column of Proposed Dataset

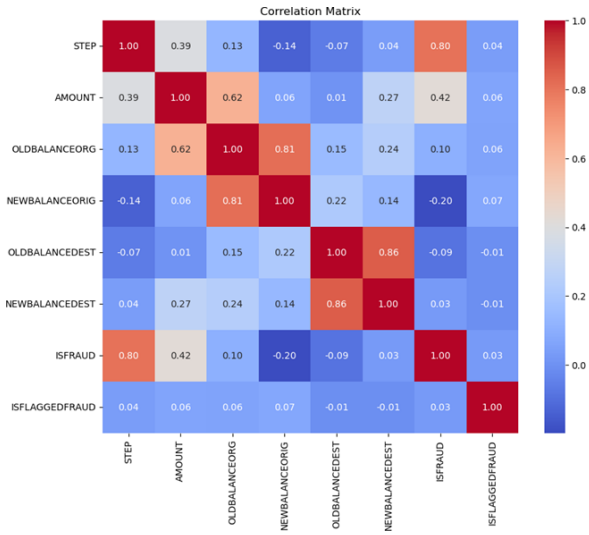

FIGURE 5. Correlation of Credit Card Fraud Dataset

The Table 4 summarizes performance of 4 different models—SVM, RF, LSTM, and CNN in classifying instances of the fraudulent as well as non-fraudulent transactions. Each model's confusion matrix is depicted in Table 4, thus offering insights in classification outcomes. In terms of fraud detection, true positive refers to fraudulent transaction correctly identified, while false negative represents fraudulent transaction incorrectly classified as the non-fraudulent. Conversely, false positive occurs when non-fraudulent transaction is inaccurately classified as the fraudulent, and true negative denotes correctly identified the non-fraudulent transaction. Analyzing Table 4, we observed variations in performance of models across different categories. For example, SVM model exhibits high number of true positives (986) & true negatives (901), indicating

Attribute	Mean	SD	Min.	25% Quartile	75% Quartile	Max.
step	0	1	1	0.0022	0.4992	1
amount	0.1291	0.2582	0	0.0009	0.0502	1
oldbalanceOrg	0.2227	0.4797	0	0.0003	0.0194	1
newbalanceOrig	0.1239	0.4205	0	0	0.0004	1
oldbalanceDest	0.2140	0.6793	0	0	0.0077	1
newbalanceDest	0.3296	1	0	0	0.0215	1
isFraud	0.5000	0.5000	0	0	1	1
isFlaggedFraud	0.0245	0.5000	0	0	0	1

TABLE 2. Dataset Statistics of Credit Card Fraud Detection Dataset

Model	Accuracy	Precision	Recall	F1 Score
SVM	0.98	0.96	0.91	0.92
RF	0.89	0.81	0.88	0.90
CNN	0.88	0.84	0.90	0.87
LSTM	0.94	0.94	0.91	0.93

TABLE 3. Dataset Statistics of Credit Card Fraud Detection Dataset

Model	TP	FN	FP	TN
SVM	986	87	26	901
RF	898	68	114	920
CNN	940	81	72	907
LSTM	878	89	134	899

TABLE 4. Confusion Matrices of Proposed Models

its ability of accurately classifying both fraudulent as well as non-fraudulent transactions. However, it also demonstrates relatively higher false negative count (87), thus suggesting instances where the fraudulent transactions were missed. On other hand, RF model achieves comparable number of the true positives (898) as well as true negatives (920) to SVM, but with slightly higher false negative count (68). Meanwhile, LSTM & CNN models also demonstrate competitive performance, with the LSTM showing higher true positive count (940) & lower false negative count (81), as well as CNN displaying almost similar trend.

Conclusion

In conclusion, the proposed research has delved into efficacy of several machine learning as well as deep learning models for the credit card fraud detection. Through meticulous analysis along with evaluation, we have access performance of SVM, RF, CNN, and LSTM models on credit card fraud detection dataset. The results showcased the notable variations in performance of each and every model across the different evaluation metrics. SVM exhibited exceptional accuracy along with precision, with commendable ability of correctly classifying fraudulent transactions. RF demonstrated the competitive performance, while LSTM as well as CNN showcased promising outcomes, thus underscoring their potential for fraud detection. Ultimately, while each and every model exhibited commendable performance in different aspects, further research along with fine-tuning are necessary in order to enhance their efficacy in the real-world scenarios. By utilizing combination of these models along with evaluation metrics, the financial institutions can develop robust fraud detection systems capable of identifying along with mitigating fraudulent activities in the financial transactions effectively.

REFERENCES

1. K. Yıldız, S. Dedebek, F. Y. Okay, and M. U. S¸ ims¸ek, "Anomaly detection in financial data using deep learning: A comparative analysis," in 2022 Innova- tions in Intelligent Systems and Applications Confer- ence (ASYU). IEEE, 2022, pp. 1–6.
2. A. RB and S. K. KR, "Credit card fraud detection using artificial neural network," Global Transitions Proceedings, vol. 2, no. 1, pp. 35–41, 2021, 1st International Conference on Advances in Information, Computing and Trends in Data Engineering (AICDE-2020).
3. F. Akba, I. T. Medeni, M. S. Guzel, and I. Askerzade, "Manipulator detection in cryptocurrency markets

based on forecasting anomalies," IEEE Access, vol. 9, pp. 108 819–108 831, 2021.
4. W. Yang, R. Wang, and B. Wang, "Detection of anomaly stock price based on time series deep learning models," in 2020 Management Science In- formatization and Economic Innovation Development Conference (MSIEID). IEEE, 2020, pp. 110–114.
5. E. Ileberi, Y. Sun, and Z. Wang, "Performance evaluation of machine learning methods for credit card fraud detection using smote and adaboost," IEEE Access, vol. 9, pp. 165 286–165 294, 2021.
6. R. Bin Sulaiman, V. Schetinin, and P. Sant, "Review of machine learning approach on credit card fraud detection," Human-Centric Intelligent Systems, vol. 2, no. 1, pp. 55–68, 2022. [Online]. Available: https://doi.org/10.1007/s44230-022-00004-0
7. C. V. Priscilla and D. P. Prabha, "Credit card fraud de- tection: A systematic review," in Intelligent Computing Paradigm and Cutting-edge Technologies, L. C. Jain, S.-L. Peng, B. Alhadidi, and S. Pal, Eds. Cham: Springer International Publishing, 2020, pp. 290– 303.
8. J. Forough and S. Momtazi, "Ensemble of deep sequential models for credit card fraud detection," Applied Soft Computing, vol. 99, p. 106883, 2021.
9. Y. Singh, K. Singh, and V. Singh Chauhan, "Fraud detection techniques for credit card transactions," in 2022 3rd International Conference on Intelligent Engineering and Management (ICIEM), 2022, pp. 821–824.
10. M.-S. Cheong, M.-C. Wu, and S.-H. Huang, "Interpretable stock anomaly detection based on spatio-temporal relation networks with genetic algorithm," IEEE Access, vol. 9, pp. 68 302–68 319, 2021.
11. F. K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam, M. Ramzan, and M. Ahmed, "Credit card fraud de- tection using state-of-the-art machine learning and
12. A. Cherif, A. Badhib, H. Ammar, S. Alshehri, M. Kalkatawi, and A. Imine, "Credit card fraud de- tection in the era of disruptive technologies: A sys- tematic review," Journal of King Saud University - Computer and Information Sciences, vol. 35, no. 1, pp. 145–174, 2023.
13. R. Sailusha, V. Gnaneswar, R. Ramesh, and G. R. Rao, "Credit card fraud detection using machine learning," in 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), 2020, pp. 1264–1270.
14. K. Randhawa, C. K. Loo, M. Seera, C. P. Lim, and A. K. Nandi, "Credit card fraud detection using adaboost and majority voting," IEEE Access, vol. 6, pp. 14 277–14 284, 2018.
15. S. Tiwari, H. Ramampiaro, and H. Langseth, "Machine learning in financial market surveillance: A survey," IEEE Access, vol. 9, pp. 159 734–159 754, 2021.

Karthik Rajashekaran is presently employed as a Senior Cloud Data Engineer at Avalara Inc. He earned his Master's degree in Computer Science from New York University in 2015. His broad expertise spans Data Engineering, AI/ML, and cloud computing. He is a dedicated blogger, focusing on the latest advancements in AI/ML, Data Engineering, and Cloud Computing domains. With extensive experience, he holds certifications in Amazon Web Services, Snowflake, Terraform, Apache Airflow, and possesses proficiency in Kubernetes.