Use of Artificial Intelligence and Machine Learning Techniques for Fraud Detection and Cybersecurity

Raj Shivaji Dhole[1], Aditya Rahul Kutwad[2], Shahfaisal Ijajnabi Gani[3]
PVG's College of Science and Commerce

***Abstract*—This Research Paper delves into the Clarification of Fraud Detection and Cybersecurity with the Help of Artificial Intelligence (AI) and Machine Learning (ML) Techniques, focusing on the Major Economic Frauds implemented by the Big institutions and Multiple Fraudulent Events in the Humankind History as a Data for the Categorization of Frauds and Learning about "How we can use the Modern Technology of Artificial Intelligence for Fraud Detection?" [1]. We are also going to Learn about various Machine Learning Techniques to Detect future possibilities of Fraudulent Behaviour. Frauds can be performed in the Various form and Large Scale for the Profits of Hefty Amounts. Key findings highlight improvements in AI adaptability, strategic decision-making, and Fraud Detection [4][6]. The research identifies gaps in real-time AI adaptability, trust-building in high-stakes environments, and fairness in transactions, aiming to advance AI capabilities in Fraud Detection scenarios [4][6].**

***Index Terms*—Fraud Detection, Cybersecurity, Artificial Intelligence (AI), Machine Learning (ML), Categorization of Frauds, Fraudulent Behaviour, Fraud Detection Techniques.**

I. INTRODUCTION

Artificial Intelligence (AI) and Machine Learning (ML) have revolutionized various industries, including Finance sector. AI refers to the simulation of human intelligence in machines, enabling them to perform tasks that typically require human cognition, such as decision-making, problem solving, and language understanding [1]. ML (Machine Learning), a subset of AI, involves algorithms that learn from data to make predictions or decisions without explicit programming. These technologies have evolved rapidly due to increased computational power, the rapid multiplication of big data, and advancements in algorithmic techniques.

Growing technology allows the rapid growth in AI evolution in the 21st Century. However, different decades of research contributed to the current expeditious AI development. The groundwork was laid by Alan Turin in the mid-20th century by the introduction of the Turing test to evaluate intelligence in machines, and later furnished by John McCarthy to introduce the concept of generality in AI. Though it was later in the century when conceptual theories became tangible implementations, these developments have continued to steer forward. During the 1990s, the world of technology encountered increasing computation power and promising development in data generation and processing systems. As the number and cleverness of cyber-attacks keep increasing rapidly, it's more important than ever to have good ways to detect and prevent them. Recognizing cyber threats quickly and accurately is crucial because they can cause severe damage to individuals and businesses. Artificial Intelligence (AI) offers a range of techniques that significantly enhance fraud detection capabilities. These techniques enable the identification of fraudulent activities with higher accuracy and efficiency compared to traditional methods. Here, we explore some of the key AI techniques employed in fraud detection. Machine Learning (ML) is a subset of AI that focuses on developing algorithms that allow computers to learn from and make predictions based on data. In fraud detection, ML techniques are extensively used to identify patterns and anomalies that indicate fraudulent behavior.

In These Research paper, we are going to analyze and understand the Evolution of Frauds conducted on the Large Scale, Types of Frauds, Preventive Measures for Frauds and Scandals, Economic Disbalance and loss, Use of Modern Technology such as Artificial Intelligence (AI) and Machine Learning (ML) Techniques in the Fraud Detection, Explaining the

Importance of Cybersecurity to avoid the Future scope of getting into Fraudulent Activities.

Some of the most common ways payment fraud occurs are mentioned below. While it is not possible to eliminate these attacks, they can mitigate their risk of impacting the business by taking the right steps.

1. Identity Theft: this type of fraud occurs when fraudsters steal personal and banking information and use the owner's identity to make false purchases and transactions. No new identity is created.

2. *Friendly Fraud*: Another prevalent type of payment fraud occurs after the delivery of service; the customer initiates a false chargeback and denies receiving it. In addition to becoming aware of the service, the amount is refunded back to the customer.

3. *Clean Fraud*: It is the hardest to detect fraud. Fraudsters very carefully analyze business fraud-detection systems and make use of stolen valid payment information.

Machine Learning (ML) Techniques that is Important to Detect the pattern and Accurate Decision-Making Algorithms.

1. ANN - A Multi-Layer Neural Network that works similar to Human thought.
2. Naïve Bayes - A Classification Algorithm that can predict Group Membership.
3. Clustering - Unsupervised Learning Method which involve grouping Identical Instances into the same sets.
4. Decision Tree - A Regression tree and Classification method that is used for Decision Support [6].

And much more.

II. FUTURE TRENDS AND DEVELOPMENTS

As AI technologies continue to evolve, the future of fraud prevention holds several promising trends and developments. From advancements in machine learning (ML) and deep learning to the increasing adoption of AI in various sectors, the landscape of fraud prevention is set to undergo Significant Transformations. ML and deep learning technologies are expected to undergo rapid advancements, leading to more sophisticated and accurate fraud detection models. These advancements will enable AI systems to analyze larger datasets, identify complex fraud patterns, and adapt to evolving fraud tactics in real time. AI will increasingly be integrated with emerging technologies such as blockchain and the Internet of Things (IoT) to enhance fraud prevention capabilities. Blockchain can provide a secure and tamper-proof way to store transaction data, while IoT devices can generate real-time data that AI systems can analyze for fraud indicators. While the financial services sector has been a primary adopter of AI-driven fraud prevention, other industries such as healthcare, retail, and telecommunications are expected to increasingly adopt AI technologies for fraud prevention. These industries will leverage AI to detect and prevent fraud in areas such as Credit Card Scams [2], Insurance claims, Retail Transactions, and Telecom billing.

III. CONCLUSION

We have learned about various aspects and perspectives from the different Authors and Research Articles about the Fraud Detection, Cybersecurity and AI and ML Techniques. We have studied about the Machine Learning Techniques and Application of the Techniques. The Observation of the AI-Enhanced Techniques in Frauds mainly in Credit Card Fraud Detection. The Applications of Artificial Intelligence in the Cybersecurity for the Avoidance of Frauds and Scandals. Predicting Fraud in Financial Payment Services through Optimized Hyper-Parameter-Tuned XGBoost Model. Specifications of LightGBM Model. Financial Fraud Detection and Prediction in Listed Companies Using SMOTE (Synthetic Minority Oversampling Technique) and Machine Learning Algorithms.

REFERENCES

[1] Financial Fraud Detection through the Application of Machine Learning (ML) Techniques: a literature review.

[2] Authors: Ludivia Hernandez Aros, Luisa Ximena Bustamante Molano, Fernando Gutierrez-Portela, John Johver Moreno Hernandez & Mario Samuel Rodríguez Barrero. Source: Humanities and Social Science Communities. https://doi.org/10.1057/s41599-024-03606-0

[3] A Systematic Review of AI-Enhanced Techniques in Credit card Fraud Detection. Authors: Ibrahim Y. Hafez, Ahmed Y. Hafez, Ahmed Saleh, Amr A. Abd El-Mageed and Amr A. Abohany. Source: 1. Department of Computer Science and

Engineering, Faculty of Engineering, Egypt-Japan University of Science and Technology, New Borg El-Arab, Alexandria, Egypt.

[4] 2. Faculty of Computers and Information, Kafr El-Sheikh University, Kafrelsheikh, Egypt.https://doi.org/10.1186/s40537-024-01048-8

[5] Artificial Intelligence in Cyber Security.Authors: Md Fazley Rafy (West Virginia University). Source: https://www.researchgate.net/publication/377235308West Virginia University. DOI: 10.13140/RG.2.2.19552.66561

[6] Artificial Intelligence (AI) in Fraud Detection: Revolutionizing Financial Security. Authors: Prabin Adhikari, Prashamsa Hamal and Francis Baidoo Jnr.Lincoln University, California, USA. University of Applied Management, Ghana. Source: International Journal of Science and Research Archive, 2024, 13(01), 1457–1472 https://doi.org/10.30574/ijsra.2024.13.1.1860

[7] Advancing Cybersecurity: a comprehensive review of AI-driven Detection Techniques. Authors: Aya H. Salem, Safaa M. Azzam, O. E. Emam and Amr A. Abohany. Source: 1. Faculty of Computer and Artificial Intelligence, Helwan University, Cairo, Egypt. 2. Faculty of Computer and Information, Kafr El-Sheikh University, Cairo, Egypt. https://doi.org/10.1186/s40537-024-00957-y

[8] Artificial Intelligence (AI) in Fraud Prevention: Exploring Techniques and Applications Challenges and Opportunities. Authors: Oluwabusayo Bello (Illinois State University). Source:https://www.researchgate.net/publication/383264952Illinois State University. DOI: 10.51594/csitrj. v5i6.1252

[9] The Impact of Artificial Intelligence on the Future of Cybersecurity. Authors: Mariam Aldhamer (hebsaif@yahoo.com) Source: Multi-Knowledge Electronic Comprehensive Journal for Education and Science Publications (MECSJ). ISSN:2616-9185

[10] Ai-Based Identity Fraud Detection: a systematic review. Authors: 1. Chuo Jun Zhang School of Computer Science University of Technology Sydney NSW 2007, Australia chuojun.zhang@student.uts.edu.au

[11] 2. Asif Q. Gill School of Computer Science University of Technology Sydney NSW 2007, Australia asif.gill@uts.edu.au

[12] 3. Bo Liu School of Computer Science University of Technology Sydney NSW 2007, Australia bo.liu@uts.edu.au

[13] 4. Memoona Anwar School of Computer Science University of Technology Sydney NSW 2007, Australia memoona.anwar@uts.edu.au Source: School of Computer Science University of Technology Sydney NSW 2007, Australia.

[14] A Survey of Artificial Intelligence in Cybersecurity. Authors: 1. Katanosh Morovat Department of Mathematics and Computer Science Western Carolina University Cullowhee, USA kmorovat@wcu.edu

[15] 2. Brajendra Panda Dept. of Computer Science and Computer Engineering University of Arkansas, Faytteville, USA bpanda@uark.edu Source:2020 International Conference on Computational Science and Computational Intelligence (CSCI). DOI 10.1109/CSCI51800.2020.00026

[16] Artificial Intelligence in Cybersecurity: A Comprehensive Review and Future Direction. Authors: Lizzy Ofusori, Tebogo Bokaba & Siyabonga Mhlongo. Source: ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/uaai20 https://doi.org/10.1080/08839514.2024.2439609

[17] Predicting Fraud in Financial Payment Services through Optimized Hyper-Parameter-Tuned XGBoost Model. Authors: Surjeet Dalal, Bijeta Seth, Magdalena Radulescu, Carmen Secara and Claudia Tolea. Source: https://doi.org/10.3390/math10244679 https://www.mdpi.com/journal/mathematics

[18] Credit Card Fraud Detection Based on Machine Learning. Authors: Yong Fang, Yunyun Zhang and Cheng Huang. Source: 1. College of Cybersecurity, Sichuan University, Chengdu, 610065, China

[19] 2. College of Electronics and Information Engineering, Sichuan University, Chengdu, 610065, China.www.techscience.com/cmc CMC, vol.61, no.1, pp.185-195, 2019

[20] A Machine Learning based Credit Card Fraud Detection using the GA Algorithm for feature selection.

[21] Authors: Emmanuel Ileberi, Yanxia Sun and Zenghui Wang.Source: Department of Electrical & Electronic Engineering Science, University of Johannesburg, Kingsway Ave, 2006 Johannesburg, South Africa. https://doi.org/10.1186/s40537-022-00573-8

[22] Financial Fraud Detection and Prediction in Listed Companies Using SMOTE and Machine Learning Algorithms. Authors: Zhihong Zhao and Tongyuan Bai. Source: School of Applied Science and Civil Engineering, Beijing Institute of Technology, Zhuhai 519085, China.

[23] Faculty of Natural, Mathematical and Engineering Sciences, King's College, London WC2R 2LS, UK. https://doi.org/10.3390/e24081157

[24] An Intelligent Payment Card Fraud Detection System. Authors: Manjeevan Seera, Chee Peng Lim, Ajay Kumar, Lalitha Dhamotharan, Kim Hua Tan. Sources: Annals of Operations Research (2024) 334:445–467 https://doi.org/10.1007/s10479-021-04149-2

[25] Online Payment Fraud: from Anomaly Detection to Risk Management. Authors: Paolo Vanini, Sebastiano Rossi, Ermin Zvizdic and Thomas Domenig. Source: 1. University of Basel, Basel, Switzerland.2. Novartis AG, Basel, Switzerland. 3. swissQuant Group, Zurich, Switzerland. https://doi.org/10.1186/s40854-023-00470-w

[26] Financial Fraud, Scandals, and Regulation: A Conceptual Framework and Literature Review. Authors: Hugo van Driel. Source: ISSN: 0007-6791 (Print) 1743-7938 (Online) Journal homepage: www.tandfonline.com/journals/fbsh20 https://doi.org/10.1080/00076791.2018.1519026

[27] Intelligent Anti-Money Laundering Fraud Control Using Graph-Based Machine Learning Model for the Financial Domain.

[28] Authors: Atif Usman, Naseer Naveed and Saima Munawar. (Department of Computer Science and Information Technology, Virtual University of Pakistan, Pakistan.) https://orcid.org/0000-0002-8130-7957 https://orcid.org/0000-0002-2446-3670 Journal of Cases on Information Technology.

[29] Explainable Artificial Intelligence Applications in Cyber Security: State-of-the-Art in Research. Authors: Zhibo Zhang, Hussam al Hamadi, Ernesto Damiani, Chan Yeob Yeun and Fatma Taher. (Senior Members of IEEE). Source: IEEE Access. DOI: 10.1109/ACCESS.2022.3204051

[30] Machine Learning for Fraud Detection in E-Commerce: A Research Agenda. Authors: Niek Tax, Kees Jan de Vries, Mathijs de Jong, Nikoleta Dosoula, Bram van den Akker, Jon Smith, Olivier Thuong, and Lucas Bernardi. Booking.com, Amsterdam. Source: Booking.com, Amsterdam.