University for the Common Good

SCHOOL OF COMPUTING, ENGINEERING AND BUILT ENVIRONMENT

Department of Computing

MSc Big Data Technologies

MSc Financial Technology

MMI226824

Artificial Intelligence and Machine Learning

Coursework 2 – Written Component

Session 2023/2024, Trimester A

Module Leader: Ji Qi

Name: ***Ronald Wanjohi Gachoka***

"I confirm that the material contained within the submitted coursework is all my own work unless otherwise stated below."

1) How does AI in fraud detection add Value to business and society? *(500 Words)*

In an increasingly digital world protecting businesses and society against fraud is paramount. According to Pickard & Venkataramakrishnan (2023), between 2018 and 2020 the average cost to a business hit by fraud is £16,000 and as technology rapidly evolves so too do the tactics used by fraudsters. AI within fraud detection has been transformative as it enhances efficiency in detection.

One of the main benefits of using AI in fraud detection is their ability to parse through vast amounts of data in real-time and flag transactions that look suspicious and need further investigation (Fraud.com, 2023) much faster and more efficiently than traditional rule-based systems. For instance, credit card fraud, AI systems analyse our typical historical spending behaviour and any sudden spike of purchases/withdrawals e.g. in a different country with our card details is flagged as an anomaly for investigation (Gulati, 2023). This is done by analysing our device information, transactions amongst much more either through supervised learning where past instances of fraud were labelled and the algorithm searches for similar patterns, or unsupervised, where the model will detect anomalies or new patterns that may potentially be fraud.

The main benefit this adds to business is that these systems operate in real-time and can detect possible anomalies instantaneously helping reduce the potential losses or reputational damage that may have occurred. Another value to businesses is the reduction in human resources being spent on false alert detection and routine document evaluations. According to a study conducted by Quest, et al. (2018), the number of false fraud alerts in banks decreased by half due to AI systems despite recording more than 20 times suspicious activity. This not only saves businesses money but also allows them to allocate their resources more efficiently and enhances overall efficiency as seen in the case of Highmark Inc. which saved approximately $245 million (Kaltwasser, 2022) in its efforts fighting fraudulent claims. This savings can also be through reducing the number of analysts who go over financial data and legacy systems as AI models can automate most tasks.

There is a positive cascading effect on society as there is an increased trust in the services as the risks of fraudulent losses reduce drastically and if it does happen there is a higher chance of it being detected quickly and disrupting

potential criminal activity. In addition, AI is being used in various settings aside from banking to improve the safety of individuals and the wider society e.g. by receiving prompts that a potential resource or content is not trustworthy and can be potentially scammed (PwC, 2023). The use of AI can also be used to protect vulnerable citizens such as the elderly or children from scams and financial abuse ensuring their well-being and safety.

In conclusion, the ongoing adoption of AI in fraud detection systems is significantly helping the fight against malicious individuals. Real-time analysis, enhanced accuracy as well as automation not only contribute positively to business but also the society ensuring financial and emotional safety in the services being used. However, AI systems need to be continuously monitored and improved as fraudsters are also using similar AI tools with malicious intent.

2) Discuss the ethical considerations in AI-powered fraud detection. *(500 Words)*

While AI-powered fraud detection systems have greatly increased the operational efficiency in combatting criminal activity, their implementation and explainability have raised numerous ethical questions. As for effective accuracy, AI models need to be trained on large amounts of data, the collection and storage of the data pose significant challenges and risks in data protection. In addition, the main areas of scrutiny of using AI tools are data privacy, data bias and transparency (Charted Banker, 2021).

As models are trained on vast amounts of data, this may also include private and sensitive information. Creators of the AI models need to prioritize data protection and ensure they are in compliance with regulatory laws such as GDPR which has strict rules on data consent and security (Shukla, 2023). In ensuring data protection organizations should employ strong encryption and data anonymization techniques which safeguard private data but also ensure adequate information is available for fraud detection. When it comes to combatting fraud within banks, several countries including the Netherlands and the UK have open-banking regulations that allow banks to share data but the

privacy concerns associated with data sharing have hampered the success of such laws (McNamee, 2022).

Bias in algorithms form a significant challenge, especially in fraud detection. If the training data is biased towards certain groups such as race, age, or gender (Charted Banker, 2021), the AI algorithm can perpetuate these biases and impact the accuracy of its fraud detection system thereby missing fraudulent activity. An instance of this can be if it was trained on skewed income data and disproportionately flagged individuals with lower income for suspicious activity leading to an increase in the false positive rates.

To avoid such cases, institutions need to ensure their models are free of potential bias (Charted Banker, 2021). There are various ethical principles in place to ensure AI algorithms are free from bias and are embedded into decision-making such as 'Advanced Analytics and Artificial Intelligence' (Triple-AI) in the UK. Some of the goals of Triple-AI are the ensure that AI models are fair and align with human principles, as well as being transparent (UK Finance; KPMG, 2020).

Lastly, AI systems including fraud detection systems need to be explainable and transparent. Nearly all AI systems are black boxes that make decisions and often lack transparency in how they get to their final decisions. This, therefore, makes it hard for potentially guilty individuals to understand how the decision came about and if they can challenge it (Galhardo-Galhetas, 2023). A new framework for developing AI systems uses Explainable AI which allows users without any computer knowledge to understand how the model came to its final decision (Cher, 2023). This ensures accountability and builds trust in how the model i.e. fraud detection came to its final decision.

In conclusion, the ethical considerations for fraud detection systems are multi-faceted. Data privacy, bias, and transparency are among the main ethical issues faced and their potential impacts to society should be considered carefully to ensure the algorithm is fair and benefits humanity.

References:

Charted Banker, 2021. *The ethics of AI.* [Online]
Available at: https://www.charteredbanker.com/resource_listing//the-ethics-of-ai.html
[Accessed 2023 December 2023].

Cher, S., 2023. Understanding Explainable AI. In: *Deep Learning and XAI Techniques for Anomaly Detection.* Birmingham: Packt Publishing, p. Ch. 2.

Fraud.com, 2023. *Artificial Intelligence – How it's used to detect financial fraud.* [Online]
Available at: https://www.fraud.com/post/artificial-intelligence
[Accessed 30 December 2023].

Galhardo-Galhetas, V., 2023. *Legal and ethical challenges of AI.* [Online]
Available at: https://nevaconsulting.com/legal-and-ethical-challenges-of-ai/
[Accessed 30 December 2023].

Gulati, A., 2023. *How AI Used in Fraud Detection? Benefits, Techniques, Use cases.* [Online]
Available at: https://www.knowledgehut.com/blog/data-science/ai-fraud-detection
[Accessed 4 January 2024].

Kaltwasser, J., 2022. AI for fraud detection. *Managed Healthcare Executive,* 34(4), p. 15.

McNamee, J., 2022. *Data privacy concerns will limit fraud detection technology.* [Online]
Available at: https://www.insiderintelligence.com/content/data-privacy-limit-fraud-detection
[Accessed 30 December 2023].

Pickard, J. & Venkataramakrishnan, S., 2023. *One-fifth of UK businesses hit by fraud, Home Office survey shows.* [Online]
Available at: https://www.ft.com/content/c249a73e-5c84-4135-81ff-8c3563ff71ee
[Accessed 30 December 2023].

PwC, 2023. *https://www.pwc.co.uk/forensic-services/assets/impact-of-ai-on-fraud-and-scams.pdf.* [Online]
Available at: https://www.pwc.co.uk/forensic-services/assets/impact-of-ai-on-fraud-and-scams.pdf
[Accessed 30 December 2023].

Quest, L., Charrie, A. & Roy, S., 2018. *THE RISKS AND BENEFITS OF USING AI TO DETECT CRIME.* [Online]
Available at: https://www.oliverwyman.com/our-expertise/insights/2018/dec/risk-journal-vol-8/rethinking-tactics/the-risks-and-benefits-of-using-ai-to-detect-crime.html
[Accessed 30 December 2023].

Shukla, R., 2023. *Ethical Considerations in AI-Powered Financial Crime Control.* [Online]
Available at: https://www.linkedin.com/pulse/ethical-considerations-ai-powered-financial-crime-control-shukla/
[Accessed 30 December 2023].

UK Finance; KPMG, 2020. *ETHICAL PRINCIPLES FOR ADVANCED ANALYTICS AND ARTIFICIAL INTELLIGENCE IN FINANCIAL SERVICES.* [Online]
Available at: https://www.ukfinance.org.uk/system/files/AAAI-Principles-FINAL.pdf
[Accessed 30 December 2023].