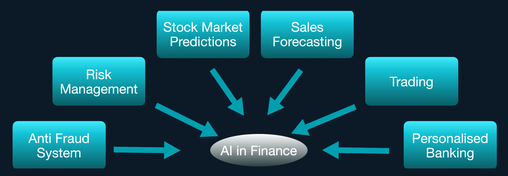
Detecting White-Collar Crime:
Ethical Challenges and Technical Solutions

Agamdeep Singh 2021306 Amolika Bansal 2020424 Pavit Singh 2021178
Parth Barthwal 2021341 Tathagat Pal 2019211

Introduction

- White-collar crimes are non-violent financial crimes perpetrated for personal or corporate gain by people in positions of authority or trust.
- Detecting white-collar crime is crucial to ensure the financial system's integrity and protecting individuals from fraudulent activities.
- AI-based softwares have helped in identifying white-collar crimes [1], however, issues with algorithmic prejudice and privacy infringement have been brought up.
- A case study is presented on ***Palantir*** which was used by law enforcement agencies for **predictive policing** [2].



Use of AI to Detect WCC

- **Anomaly Detection :** AI algorithms have the potential to find irregularities or odd trends in financial data that may be signs of fraud.
- **Natural Language Processing (NLP) :** Large volumes of text data, like emails and financial information, can be analysed using AI-powered NLP to find unusual language that might be a sign of fraud.
- **Predictive Analysis :** Based on past data and patterns, AI can be used to forecast future fraud activities.
- **Network Analysis :** AI detects fraud by analyzing financial networks, identifying connections between individuals and companies.

Ethical Issues

- The techniques employed for white-collar crime detection gives rise to a lot of ethical issues that need to be dealt with. The most significant of these ethical issues include data security, profiling, and privacy issues.
- **Privacy issues** emerge when personal information is relied upon to identify financial crimes. For instance, Palantir's technology was used to collect data on people without getting their permission, which was against their right to privacy.
- **Profiling** arises when certain groups are unfairly treated as a result of profiling based on factors like colour, age, or gender. It's possible that Palantir's algorithms were biassed against particular groups, producing unfair results.
- **Data Security**, i.e. protecting sensitive financial information from unauthorized access is an important ethical concern.

Palantir : A Case Study

- Palantir is a business that offers many industries, including finance, machine learning-based software solutions for data analytics. Concerns have been raised, nevertheless, about how their technology might be used ethically.
- Palantir's potential **bias in algorithms** and misuse of data, including personal information, are significant concerns. As a result, people have been treated unfairly depending on factors like ethnicity or gender.
- The technology was used to **collect data without consent**, potentially on those not suspected of wrongdoing, **violating privacy rights**.
- Palantir's technology was used by law enforcement agencies for predictive policing without adequately addressing these ethical considerations.

How to Address Ethical Dilemmas?

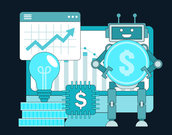
Homomorphic Encryption
Homomorphic encryption allows for computation on encrypted data to be performed in such a way that the results are still encrypted, and only the owner of the secret key can decrypt the results to see the final outcome.

↓

Adopt a Virtue Ethics Approach:
Encourage ethical characteristics like honesty, fairness, and privacy

↓

Embrace the Principle of Beneficence
This will involve placing customers' and stakeholders' needs and interests ahead of the company's own, as well as ensuring that the advantages of its AI technologies are spread fairly. Promote the well being of others.



Conclusion

If there are no foreseeable solutions to ethical concerns in identifying white-collar crime, the project should be abandoned since it would violate individuals' rights and could result in biased outcomes. However, if technological and social/legal/philosophical solutions to ethical difficulties can be adopted, the project can proceed with care.

References

[1] W.A. Stadler, P. Gottschalk, Testing Convenience Theory for White-collar Crime: Perceptions of Potential Offenders and Non-offenders, Deviant Behavior. 43 (2022) 804–820. https://doi.org/10.1080/01639625.2021.1919037.
[2] A. Winston, Palantir has secretly been using New Orleans to test its predictive policing technology, The Verge. (2018). https://www.theverge.com/2018/2/27/17054740/palantir-predictive-policing-tool-new-orleans-nopd.
[3] P. Gottschalk, C. Filstad, R. Glomseth, H. Solli-Sæther, Information management for investigation and prevention of white-collar crime, International Journal of Information Management. 31 (2011) 226–233. https://doi.org/10.1016/j.ijinfomgt.2010.07.002.
[4] B. Narsimha, Dr.C.V. Raghavendran, P. Rajyalakshmi, G. Reddy, M. Bhargavi, P. Naresh, Cyber Defense in the Age of Artificial Intelligence and Machine Learning for Financial Fraud Detection Application, International Journal of Electrical and Electronics Research. 10 (2022) 87–92. https://doi.org/10.37391/ijeer.100206.