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

SSH325: Ethics in AI

Detecting White Collar Crime: Ethical Challenges and Technical Solutions

1. Discuss the general nature and aim of your technical project.
Crimes with a financial motivation that are committed by people, businesses, and governments are termed White-Collar Crimes (WCC). Crimes such as fraud, embezzlement and money laundering lead to millions in losses. The persecution of such crimes is often a lengthy endeavor, with sophisticated fraudulent activities often being hard to detect and linked back to the perpetrator. We believe AI and its applications have potential in the detection and prevention of these crimes, AI has proven itself to be massively relevant to the field of finance and has had vast applications, such as Algorithm-Based Trading and Robo-advisors, to name a few. In Algorithm-Based High-frequency-Trading (HFT), stock trends are analysed with reference to vast sources of past data using machine learning (ML) and neural networks to predict future trends. "The benefits of AI in HFT include their ability to examine large data sets from many sources in a split second and carry out real HFT that can profit from market anomalies and price disparities." [1].

Other applications of Artificial Intelligence in finance include Robo advisors, which are AI-based software decision-making systems that can manage client portfolios with minute-by-minute updates. "Due to a new generation of clients with the technical know-how of digital technologies who prefer to have active and ongoing control over their investments, robo-advisors have replaced traditional financial services in the wealth management industry" [2].

Artificial intelligence can help in the detection and prevention of white-collar crimes (WCC) through various techniques such as NLP, predictive analysis, and network analysis, among others. AI has the potential to make the detection, prediction and analysis of WCC much easier and faster; in theory, this will lead to much safer financial systems.

Applications of AI in the detection of WCC include but are not limited to:

Anomaly detection: ML systems will eventually learn how you interact and trade. Monitoring your financial transactions to detect any behaviours which might seem out of the ordinary.

Network Analysis: A person's interactions within a financial system may form a network, and AI may detect any suspicious activities, Key players in financial fraud schemes and complex networks can be unravelled with the use of AI.

Natural Language Processing (NLP): large volumes of text data like chat logs, statements and even telephone conversations can have NLP applied to them, to weed out any suspicious persons who might be using language and phrases related to fraudulent activity.

The above techniques may be applied individually or in combination on vast volumes of financial transactions, text data and conversations to achieve desirable results. Limitations such as data quality, biases present in the data, and the inherent opacity of such AI systems have plagued the applicability of these techniques and AI systems. Lastly, we need to consider major ethical considerations of autonomy privacy and transparency among others

2. Discuss the ethical issues that may arise in connection with your project.

Palantir is a data analytics company that had gotten into ethical hot water following their predictive policing systems which often targeted over-policed communities of colour due to previous biases in data [3].

Palantir is expanding into the financial fraud detection sector, and it must do so with care about the ethical considerations they make, since the techniques that are employed for white-collar crime detection give rise to a lot of ethical issues that need to be dealt with.

The techniques that are currently being used in big data analytics involve things such as surveillance algorithms and predictive models, which maintain figures such as risk scores and features such as geographic mapping, temporal models etc.[4], to determine potentially risky individuals.

They also use non-traditional methods of sourcing information such as system access logs, building access data and most importantly, social media information to cross-reference ongoing investigations. These lead to many ethical concerns, such as privacy issues, profiling issues and risks to data security.

Privacy issues emerge when personal information is relied upon heavily to identify financial crimes. Users are not informed that their information is being collected and analysed for investigative purposes, which violates their right to privacy. 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. To find people who might be a risk, predictive models and risk scores can be utilised, although it's likely that these techniques are biased and profile particular people or groups. This has and can result in unjust targeting of certain populations, exacerbating existing societal inequalities and undermining the fairness and impartiality of the criminal justice system.

It's possible that Palantir's algorithms were biased against particular groups, producing unfair results. Police organizations have been deploying Palantir's technology for data-driven policing, which has been found to be pushing racist bias in their predictive outcomes and helping push the very strong systemic bias towards people belonging to certain races [5]. Companies such as Palantir are constantly focusing on increasing their datasets in order to improve their "accuracy" but increasing the amount of data doesn't help eliminate bias, and therefore, the confidence ratings are not indicative of the true nature of the outcomes.

Another major ethical concern is data security, or safeguarding private financial information from unwanted access. Using big data analytics techniques necessitates the gathering and storage of copious volumes of private data. This increases the danger of data breaches and cyberattacks, which can expose financial and personal information and result in identity theft or other financial fraud.

One example of a large-scale data breach that had significant consequences for the general public is the Equifax data breach in 2017. Equifax, a major credit reporting agency, experienced a cyberattack that resulted in the theft of the personal information of approximately 143 million people, including names, addresses, social security numbers, birth dates, and other sensitive data. [6]

3. If possible, discuss the theoretical nuances of these ethical issues drawing from readings you have completed during the course.

Several researchers have noted that the moral problems with detecting white-collar crime are complicated and multifaceted. Using personal information to spot financial crimes raises questions regarding the right to privacy, making privacy one of the primary issues. According to Grote and Berens (2019), maintaining privacy while using algorithmic decision-making is essential to the healthcare industry. Similarly, Susser, Roessler, and Nissenbaum (2019) contend that even when individuals' consent is obtained, using their personal information for manipulative objectives violates their autonomy.

A further ethical quandary that appears when computers are employed to spot financial crimes is profiling. According to Binns (2017), algorithmic accountability is required to stop the unfair treatment of people based on attributes like race, gender, or age. This is crucial when discussing financial crimes because biased algorithms can produce unjust results.

Data security is also a crucial ethical issue because unauthorized access to private financial data can result in identity theft and financial harm. The importance of data privacy in algorithmic healthcare decision-making, which also extends to financial systems, is emphasized by Grote and Berens (2019). According to Gunkel et al. (2020), data protection is a social and political issue that calls for a group effort.

In conclusion, a comprehensive knowledge of the ethical concerns surrounding white-collar crime detection is necessary and extends beyond technological considerations. Scholars like Binns, Susser, Roessler, Nissenbaum, Grote, and Berens have emphasized the importance of philosophical and social viewpoints in formulating ethical principles and laws that uphold people's rights and advance justice.

4. How do you plan to address the ethical issues that arise as part of your technical project?

Addressing ethical dilemmas in the development of AI requires thoughtful consideration and strategic solutions. One possible solution is to employ homomorphic encryption, which allows computation on encrypted data while keeping the results encrypted until the owner of the secret key decrypts them. Another approach involves adopting a virtue ethics methodology that promotes values like honesty, fairness, and privacy throughout the organization. By fostering a culture of ethical behavior and decision-making, employees are empowered to prioritize the needs and interests of customers and stakeholders over the company's interests, in line with the principle of beneficence. Embracing this principle ensures that the benefits of AI technologies are distributed fairly.

Additionally, businesses could interact with various stakeholders, such as regulators, affected communities, and civil society organizations, to get feedback on the ethical ramifications of their goods and services. This would support the identification and candid discussion of ethical issues. Ultimately, by integrating ethical considerations into AI systems' design and development processes, potential ethical dilemmas can be identified and addressed proactively, promoting integrity and responsible innovation.

In the context of white-collar crimes and financial issues, taking responsibility requires a focus on ethics in design. Development processes must align with ethical principles, and the ethical implications of AI integration and replacement of traditional systems and social structures must be considered. Ethics should be integrated into the design of artificial autonomous systems such as agents and robots. Designers must uphold research integrity as they design, construct, use, and manage artificially intelligent systems. Ultimately, a commitment to ethical design practices is crucial for addressing the ethical dilemmas that arise in the realm of financial technology [7].

The techniques employed for white-collar crime detection give rise to numerous ethical issues that must be dealt with. The most significant 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 due to profiling based on factors like colour, age, or gender. Palantir's algorithms were biased against particular groups, producing unfair results. Data Security, i.e. protecting sensitive financial information from unauthorized access, is a significant ethical concern.

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] Cohen G. Algorithmic Trading and Financial Forecasting Using Advanced Artificial Intelligence Methodologies. *Mathematics*. 2022; 10(18):3302. https://doi.org/10.3390/math10183302

[2] Manchuna Shanmuganathan, Behavioral finance in an era of artificial intelligence: Longitudinal case study of robo-advisors in investment decisions, Journal of Behavioral and Experimental Finance, Volume 27,2020,100297, ISSN 2214-6350, https://doi.org/10.1016/j.jbef.2020.100297. (https://www.sciencedirect.com/science/article/pii/S221463501930214X)

[3] Winston, A. (2018, February 27). *Palantir has secretly been using New Orleans to test its predictive policing technology*. The Verge. Retrieved May 1, 2023, from https://www.theverge.com/2018/2/27/17054740/palantir-predictive-policing-tool-new-orleans-nopd

[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.

[5] 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.

[6] T. S. Bernard, T. Hsu, N. Perlroth, and R. Lieber, “Equifax Says Cyberattack May Have Affected 143 Million in the U.S.,” *The New York Times*, Sep. 07, 2017. Accessed: May 01, 2023. [Online]. Available: https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html

[7] Dignum, V. (2020). Responsibility and Artificial Intelligence. The Oxford Handbook of Ethics of AI, 4698, 215