IBIMA Publishing
Communications of International Proceedings
https://ibimapublishing.com/p-articles/44AI/2024/4421324/
Vol. 2024 (22), Article ID 4421324

Artificial Intelligence and big data: Modern tools for the banking and insurance sectors. Potential risks for local security*

Aleksandra Helena PASIECZNA-DIXIT

Pomeranian School in Starogard Gdański, Starogard Gdański, Poland
ORCID: 0000-0001-6867-3584

Correspondence should be addressed to: Aleksandra Helena PASIECZNA-DIXIT, aleksandra.pasieczna@twojestudia.pl

* Presented at the 44th IBIMA International Conference, 27-28 November 2024 Granada, Spain

Abstract

Artificial intelligence (AI) and big data are increasingly being used in the financial sector with the intention of automating decision-making processes in an optimized manner. Contemporary finance is thus faster and more efficient in various contexts. Despite their widespread use and relative success, AI and big data suffer from multiple issues, which can lead to potential threats to local communities. With the aim of opening discussion about these potential threats, we present various scenarios under which they may be realized. Some of these scenarios were based on actual events reported in news media, while others are gedankenexperiments (thought experiments) designed to highlight these threats. Our examples show that the use of AI and big data within banking and insurance sectors calls for further studies, specifically in local security contexts.

Keywords: Artificial intelligence, Big data, Banking, Insurance, Local Security.

Introduction

The terms Artificial Intelligence (AI) and Machine Learning (ML) usually refer to automated learning techniques deployed to solve certain problems. Financial companies use AI techniques to make decisions about recruitment (Lee and Kim, 2021; Mangal, 2023), insurance pricing (Byrne, 2024), risk management (Aziz and Dowling, 2019), probability of credit repayment (Filiz et al., 2024), among others. This is typically done by translating a given problem into a classification (*Which risk bucket should this asset be assigned to?*) or regression problem (*What is the probability of a payment being missed by this client?*).

AI algorithms can parse big data, a property particularly useful within the financial sector. Big data refers to massive datasets with various data-fields, such as stock prices, meeting minutes, or social media feeds, all of which would be hard to parse through with simpler models. AI models transform these fields into an internal structure, and then extract important features (Kanungsukkasem and Leelanupab, 2019) using this representation. These features are then used to generate an output for decision-making. AI algorithms generally have higher accuracy and adapt to unseen situations and have a larger potential for generating profits. These models also detect new variable interactions saving costs of novelty research.

The focus here is on AI with big data, and the potential risk to local communities within banking and insurance contexts. Use of AI makes community life comfortable, but also brings many potential threats to local security, linked

Cite this Article as: Aleksandra Helena PASIECZNA-DIXIT, Vol. 2024 (22) "Artificial Intelligence and big data: Modern tools for the banking and insurance sectors. Potential risks for local security" Communications of International Proceedings, Vol. 2024 (22), Article ID 4421324, https://doi.org/10.5171/2024.4421324

to the incorporation of technology within our daily lives. Modern solutions used in financial decision-making processes impact communities at regional, national, and international levels. Local communities that are deprived of equal access rights to financial institutions may become marginalized, resulting in the accumulation of socio-economic problems. As the financialization of the economy increases, society becomes increasingly dependent on financial companies, allowing for a "weaponization" of finance (Lin, 2015). The risk of bad actions by foreign agents cannot be ignored, especially in the context of hybrid wars (Shiekh, 2022).

We present different scenarios assuming widespread use of big data and AI within the financial sector, which highlight the risks associated with adoption of modern technology. We also present certain concerns that question what companies and individuals are allowed to do, and where the limit of market freedom, individual freedom and social solidarity lies.

Big data and AI

Big data refers to massive amounts of data obtained from one or more sources (De Mauro et al., 2015). Big data tends to be voluminous, but also diverse in that it may be of different types: numeric (prices), text (minutes of a meeting), images (satellite imagery), audio (speeches) and video (news broadcasts). Data mining algorithms find patterns for further use (Papakyriakou and Barbounakis, 2022), and there has been significant research into mining numeric (Zhang and Cheung, 2014), text (Pejić Bach et al., 2019), image (Zhang, 2021), audio (Moelants et al., 2006), and video (Gul, Bano and Shah, 2021) data.

Given the amount of extractable information, the potential uses are many. For example, emotional states and mental health conditions can be identified from audio and video recordings (Singh and Kumar, 2022). Big data is also used by governments, for example, to keep law and order (Joh, 2014). Collection and use of big data could be legal (through express permission of users) or illegal (without permission), and there is active research in the ethics of these processes (Sipior et al., 2004).

In a broad sense, AI refers to machine-based intelligence that matches humans. Here though, AI implies automatic learning techniques used to solve different problems. Typically, machine-learning (ML) is used to find solutions to a problem by detecting patterns in an automatic manner. Generally, these patterns are detected within large datasets, and so big data and AI tend to be part of one project.

Given the abilities to learn automatically and detect subtle patterns within large datasets, AI is faster and more accurate than humans in statistical inference and problem solving. As AI models tend to be very complex, model interpretability tends to be sacrificed for model accuracy. This raises concerns for its use in sensitive fields (e.g., military and government policy). Nonetheless, AI and big data have already provided many contributions to modern technologies such as facial recognition (Asaithambi, Venkatraman and Venkatraman, 2021), fraud detection (Dai et al., 2016), forensic genetics (Amorim and Pinto, 2018), sports (Bai and Bai, 2021), medical drug discovery (Brown et al., 2018), and finance (Fang and Zhang, 2016).

Potential risks to local security

Political manipulation

A potential misuse of modern technologies to interfere and manipulate the population is best highlighted through the Cambridge Analytica scandal, where Cambridge Analytica was accused of using Facebook data to influence the 2016 US presidential election (Wilson, 2019). The company had mined Facebook users' data with their permissions, from which they profiled political preferences of individuals. Malleable voters were found, targeted, and subtly manipulated.

This shows how big data is relevant to social media, and the risk associated with its misuse. Misuse can even happen within the banking and insurance sectors. Banks and insurance companies continuously use big data to profile their customers. Many financial institutions use "KYC" (know-your-customer) forms to analyze customer profiles. This is sensitive data, and the purpose of its collection is to avoid misuse of banking services. Leakage of this data can have drastic consequences for a bank and its clients. Bad actors sometimes resort to KYC fraud, where customers are scammed into releasing KYC information to scammers instead of banks (Dharmavaram and Mishra, 2023). There is an added risk that banks, or certain employees at the bank, misuse this data with the intention of driving public policy. If a bank decides to manipulate the local populace politically, it can choose to give economic benefits to clients aligned

to their goals. Gradually, society gets split, where an economic disadvantage becomes visible to those not aligned with the bank. This thought experiment aims to highlight the importance and power of banks in society. Banks are aware of this, and generally use data to drive positive change (Perry, 2023).

Local communities are also at risk of market manipulation by financial companies. The risk increases when foreign companies get involved (Chang and Goldman, 2008). By using modern techniques, one can find systemic weak points (Wever et al., 2022). By applying stresses on these weak points, foreign companies can create or amplify systemic collapses that match conventional attacks in terms of recovery costs.

The data generation and collection processes themselves can be manipulated to achieve political influence. This is done to tailor data that privileges one group over another, which can be done at local levels (e.g., data shows higher credit ratings of one group of people), or at international levels. For example, the World Bank is said to have manipulated data under pressure of foreign officials to improve ratings of certain countries (Tirkey, 2021).

In addition to manipulating markets or manipulating datasets, banks can use AI and big data to figure out which sector of a foreign community is sensitive and then dominate investments in that sector. In future, these private or state-controlled banks can use their quasi-monopolistic power to apply political influence and lobby for certain policies.

Bank data leaks and their misuse

As highlighted earlier, client data is collected and stored by multiple financial companies. However, it is not just private enterprises that use this data. For example, Poland uses “Profil Zaufany” (trusted profile) as a way of accessing multiple governmental websites with detailed, confidential information using just the bank account login and password. There is thus a security risk associated with leakage of the data. The sensitive nature of this data implies a potential misuse, resulting in possible criminal targeting of vulnerable subjects (e.g., elderly subjects, patients with mental issues who own property).

An example of data leakage is from February 2022, where the account details of 30 000 Credit Suisse clients were released. This leak revealed that Credit Suisse failed in conducting the due diligence of its clients, since the release focused on the hidden wealth of clients involved in criminal activities (Pegg et al., 2022). While this leak focused on shortcomings on the side of banks, the possibility of the misuse of leaked data persists.

Bad actors tend to look at maximum “impact” or “profit,” and so data breaches happen often in the financial domain. When a breach occurs, banks have a responsibility to notify the impacted clients. As banks have an interest in underplaying these events to protect their public image and project self-confidence, the risk to local security comes from two sources: 1) the actual data leak itself; 2) clients unable to protect themselves due to insufficient information.

One of the many threats of a data leak is monetary loss. Consider the case where credit card information was leaked. Bad actors may simply spend money on online shopping sites. However, in an extreme case, they might use the money to fund groups that attack more banks, or even fund terrorist organizations. Even without economic loss, clients are not fully secure. Many people tend to use one password across different sites, including banks. This information can be used for identity theft on social media with the intention of creating against certain targets, or on professional accounts with the intention of accessing sensitive workplace details. A third threat is that of potential abuse. Since sensitive information is leaked, such as information about undisclosed expenditures, professional activity and financial problems, actors can resort to extortion or blackmail of certain individuals.

Misuse of health data

Health data is collected from diverse sources, such as private or public healthcare accounts. This can be particularly useful to banks and insurance companies to estimate the risk of a loan, and to price insurance policies. However, it is possible to infer health information from indirect means (sometimes even unethical), such as data leaks, publicly available lifestyle data, tracking on browsers, social media, and even instant messengers. For example, companies can buy keyword usage, which can be used with statistical inference methods to classify an individual's mental and physical state. Another example is writing speed, which indicates health condition, since our motor skills are changed by our health (Baker and Rogers, 2010).

Insurance companies use health data to create personalized health coverage schemes for their clients. If unwanted data was leaked, then these insurance companies might misuse the data to create profit for themselves unfairly. For example, ALAB, a clinical laboratory, had a data leak incident in 2023 (Government of Poland, 2023). Insurance

companies can get this data and decide that they have underpriced a certain region based on data analysis. This is unfair since the information was not provided by customers.

In 2023 the My Heritage company restricted access to the information about individual's ethnic group. While the reason for the decision is not clear, we can suspect that it was due to their concern about ethnic group safety and potential misuse of data. Some countries prohibit genetic testing by private companies, raising different objections including potential misuse in the insurance sector. Private insurance companies can misuse genetic data to unfairly charge clients. For example, nowadays, genetic tests provide information about the tendency to suffer from certain illnesses. This is done to provide knowledge to individuals that can be used to control life choices. So, even though clients can control their illnesses, insurance companies might charge these clients unfairly. Furthermore, there tend to be correlations between certain ethnic groups and prevalence of certain genetic disorders. Leakage of genetic profiles might cause insurance companies to unjustly charge a larger premium from a certain group, which causes an economic burden on them.

Finally, the usage of health data raises an ethical question: *if a healthcare-based model gives individuals about potential lifespan with high confidence, should the financial institutions use this information, or should this be fully confidential?*

Biases in big data and AI

Broadly speaking, bias refers to a systematic tendency to give improper importance to a particular phenomenon. Cognitive biases, for example, refer to the biases induced in mental processes, which lead to false inferences and lapses in judgement (Hilbert, 2012). Most of the data collected is not free from human biases. For example, women tend to be granted fewer loans compared to men, even at the same age, health and career level (Montoya et al., 2020). Models using such datasets learn this bias, and they might do so through characteristics correlated to gender, even if the gender of a person is not included directly in a model. The bias reflects the current state of society, and models reinforce the bias, since men will get more economic opportunities than women. Fixing these data biases is cost intensive for banks, since one would need to collect data that rectifies the bias (Srinivasan and Chander, 2021). Collecting alternative data might also be a solution, but it will lead to other privacy-related problems and increased costs of verification.

Biases in AI are closely related to biases in datasets since AI models learn from datasets. Even subtle biases are picked up by AI and impact decisions (UN Women – Headquarters, 2024), which may go undetected. Since AI leverages upon millions of examples, it is possible that a bias is picked up, even if that bias is not widespread among humans. An example of this is a potential amplification of name bias, where certain names tend to be preferred over others relevant in several contexts. If a dataset has a mild version of this bias, something not widespread in the community, there is a risk that the AI reinforces the weak bias, making certain people discriminated against.

This is very important in banking and insurance companies. Consider the case of an AI helping insurance agents decide the price of an insurance policy. If the AI was trained on a dataset consisting of predominantly young and middle-aged people, it might learn that people above a certain age will not survive long. The consequence is that it recommends the agent to charge a larger premium from older clients. While age is an important factor, the model might amplify the bias so much that the insurance policy might be unaffordable for older clients. One way to fix this is to include datasets that are more balanced across groups, but subtle biases will always exist (education level, life choices), and will be picked up (Ferrer et al., 2021).

AI models are also prone to overfitting, where models learn the random patterns within smaller datasets, but which are not valid for the larger population. For example, a training dataset for an insurance AI model might show slightly different alcohol preferences across master's and bachelor's students. If the AI model learns indefinitely, it will pick up this insignificant difference, and then amplify it. The AI does not generalize to a larger population and unfairly overprices one group.

In the context of health insurance, some open topics to deal with biases include:

- Should everyone in society pay the same premium (or percentage of their income)? This is done by governments to provide minimal healthcare for all citizens. It is unclear whether private companies should do something in this spirit to reduce data/AI biases. If everyone is charged the same, will people take more care of their health or less?

- People can protest and ask for changes if human agents apply a bias. If there is a bias in the AI model, who is accountable – the data provider, the AI model, the programmers, the programmers' manager, or the entire company?

- Local communities strive to fight discrimination, but subtle biases in AI may accidentally make societies more polarized. Can we envisage regulatory measures to reduce any potential impact of AI-based systems?

Information asymmetry

Insurance companies also protect agricultural and real estate enterprises against unknown dangers. A fair price of an insurance policy can be assumed when clients and companies have equal access to the risk information, and the pricing structure. If they do not have equal access, there is information asymmetry, which can be misused. For example, insurance companies can quickly verify and confirm claims using satellite imagery. Companies can save cost and time by quickly estimating the damage caused by natural disasters without visiting the sites. However, clients tend to be disadvantaged if such data is used in the pricing. For example, insurance companies might charge larger premiums for a region that gets more exposed to hurricanes compared to another. A valid question is whether this excess premium is fair or not. From the insurers' perspective, they provide coverage against a "known" risk, and they get compensated. From the clients' perspective, they may not be aware of it, have no control over the risk factor, and are "punished" for living there.

Another example of information asymmetry lies in access to pollution data. Insurance companies can quickly analyze local pollution data and detect patterns in how the pollution changes over time. This information can be used to economically discriminate against people from a certain region, assuming they have been exposed and may suffer from potential diseases. The consequence of this is that the cost of treating these people is paid for by the public sector.

Even with small excess premia, this type of pricing is a risk to local communities since certain groups will always be favored over others. Information asymmetry might also work against insurance companies. Customers may willfully conceal information that is pertinent to the policy with the intention of getting a lower premium. This forms a threat to local stability since if many clients withhold important information, insurance companies will not be able to sufficiently protect the community against the realization of the concealed risk factor.

Risk of using similar AI models by financial companies

Banks and insurance companies tend to buy or create very similar AI programs to build the risk profiles of certain individuals and companies. This creates a potential amplification of any bias, and inequalities among certain groups tend to increase. As the big institutions discriminate against certain groups, it falls on smaller companies to take on these clients. The risk increases for small companies – the smaller companies tend to take on a particular group of clients that are considered risky by market-dominating companies.

Such potential threats are not without precedent. Indeed, many computational models, even the very simple ones, tend to converge to similar solutions from different sources. This can be due to selective pressure, herd behavior, or talent acquisition from competition. Many problems have few unique "good" solutions, and many machine-learning algorithms may converge to the same points. This can be particularly important when the optimization criteria of models are similar across companies within the industry, which happens to be the case in banks and insurance companies – maximize profits and minimize risk.

Model risk of AI

AI models are models that learn from datasets with the intention of capturing patterns in the real world. They are only approximations to observed phenomena, and not the "truth, and so users are exposed to model risk, the risk of a certain model failing due to data, its construction or its usage (Derman, 1996; Pasieczna, 2021).

Given that all models have some inherent model risk, banks, insurance companies and their clients are all exposed to it. As the world becomes more reliant on technology, with the financial world being driven by algorithms, local communities need to consider the cost of a potential model failure, which can be quite large within the context of banking and insurance.

Misinterpretation of computational models has been associated with financial crashes. For example, consider the financial crisis that followed the collapse of Long-Term Capital Management (LTCM) in 1998. LTCM used a simple model to estimate the portfolio risk, relying on historical data. Multiple studies have shown that had they used a bit more history (even just going back to 10 years), their losses would have been reduced enough to avert the market crash (Rimkus, 2016).

With AI, the threat of model risk realization is much higher due to the difficulty of interpretation. AI is also susceptible to parametrization error, where differences in data or learning parameters give vastly different results. Model risk within complex systems may be undetected for very long periods, and even model risk is factored in, finding the cause of a bias is harder, since it is not clear when a bias is due to the data, insufficient training, excessive training, or the model uncertainty.

Conclusions

AI and big data bring immeasurable benefits related to more efficient analysis of information from various sources. Within the financial system, where it is necessary to analyze information from the distant past as well as current analysis, or integrate data from various data sources, these tools improve the work of analysts and managers. AI and big data can be used for very advanced decision-making processes handling various geographical units and within legal and regulatory frameworks. In this work, we drew attention to the existing and hypothetical threats related to the use of these tools in financial companies.

AI and big data can be exploited by foreign institutions in the context of hybrid wars and political inference. This may be difficult to detect in complex financial systems for humans, and as shown, the damage can be as large as conventional attacks. Misuse of AI and big data may result in a significant increase in the costs of loans and insurance for local communities and may so result in financial discrimination that underprivileges the region. Use of big data carries the risk of many biases, which may also result in discrimination against certain individuals or groups. Detecting and correcting errors might be difficult in a fully automated process.

Potential risks of using AI and big data in financial institutions are not limited to their clients or local communities, but also to these institutions and the financial network as well. This is particularly important as more companies begin to use AI and big data and get more interconnected among themselves and the macroeconomy.

The work highlighted the threats that the use of AI and big data by financial companies bring to local security. To reduce the associated risks, technology providers (AI/big data companies), technology users (financial companies and their clients), regulatory bodies and local community representatives need to have open debates with each other. Every member here has different needs and aims, some of which might be detrimental to others, resulting in a reduction of local security. SWOT analyses might prove useful to weigh the benefits against the risks of using modern tools for banking and insurance within the context of local security.

References

- Amorim, A., and Pinto, N. (2018). Big data in forensic genetics. *Forensic Science International Genetics*, 37, pp.102–105.
- UN Women – Headquarters. (2024). *Artificial Intelligence and gender equality*. [online] Available at: https://www.unwomen.org/en/news-stories/explainer/2024/05/artificial-intelligence-and-gender-equality [Accessed 15 May 2024].
- Asaithambi, S. P., Venkatraman, S., and Venkatraman, R. (2021). Proposed big data architecture for facial recognition using machine learning. *AIMS Electronics and Electrical Engineering*, 5, 68–92.
- Aziz, S. and Dowling, M. (2019). Machine learning and AI for risk management. In: Lynn T., Mooney J.G., Rosati P. and Cummins M., eds., *Disrupting finance: FinTech and strategy in the 21st century*. Cham: Springer International Publishing, pp.33–50.
- Bai, Z. and Bai, X. (2021). Sports Big Data: Management, Analysis, Applications, and Challenges. *Complexity*, [online] 2021, pp.1–11.
- Baker, N.A. and Rogers, J.C. (2010). Association between computer use speed and age, impairments in function, and touch typing training in people with rheumatoid arthritis. *Arthritis Care & Research*, 62(2), pp.242–250.

- Brown, N., Cambruzzi, J., Cox, P. J., Davies, M., Dunbar, J., Plumbley, D., Sellwood, M. A., Sim, A., Williams-Jones, B. I., Zwierzyna, M., and Sheppard D.W. (2018). Chapter Five - Big Data in Drug Discovery. In: Witty D.R., and Cox B., eds., *Progress in Medicinal Chemistry*. Elsevier, 57, pp.277–356.
- Byrne, A. (2024). Pricing Risk: An XAI Analysis of Irish Car Insurance Premiums. *Communications in computer and information science*, pp.315–330.
- Chang, F.K. and Goldman, J. (2008). Meddling in the Markets: Foreign Manipulation. *The US Army War College Quarterly: Parameters*, 38(1), p.43.
- Dai, Y., Yan, J., Tang, X., Zhao, H. and Guo, M. (2016). Online Credit Card Fraud Detection: A Hybrid Framework with Big Data Technologies. *2016 IEEE Trustcom/BigDataSE/ISPA*, pp. 1644–1651.
- De Mauro, A., Greco, M. and Grimaldi, M. (2015). What is big data? A consensual definition and a review of key research topics. *AIP Conference Proceedings*, 1644(1), pp. 97–104.
- Derman, E. (1996). Model risk: What are the assumptions made in using models to value securities and what are the consequent risks? *RISK-LONDON-RISK MAGAZINE LIMITED-9*, pp.34–38.
- Dharmavaram, V. G. and Mishra, O. (2023). KYC Fraud: A New Means to Conduct Financial Fraud--How to Tackle It? In: *Cybersecurity Issues, Challenges, and Solutions in the Business World*. IGI Global, pp. 81–94.
- Fang, B., and Zhang, P. (2016). Big Data in Finance. In: Yu, S., Guo, S., eds., *Big Data Concepts, Theories, and Applications*, pp.391–412.
- Ferrer, X., Van Nuenen, T., Such, J. M., Coté, M., and Criado, N. (2021) 'Bias and Discrimination in AI: A Cross-Disciplinary Perspective', *IEEE Technology and Society Magazine*, 40(2), pp. 72–80.
- Filiz, G., Bodur, T., Yaşlıdağ, N., Sayar, A., and Çakar, T. (2024) 'Predicting Credit Repayment Capacity with Machine Learning Models', in *2024 32nd Signal Processing and Communications Applications Conference (SIU)*, pp. 1–4.
- Government of Poland. (2023). *Hakerzy ujawnili kolejną część danych wykradzionych z ALAB Laboratoria – sprawdź czy Twoje dane zostały upublicznione - Baza wiedzy - Portal Gov.pl*. [online] Available at: https://www.gov.pl/web/baza-wiedzy/hakerzy-ujawnili-kolejna-czesc-danych-wykradzionych-z-alab-laboratoria--sprawdz-czy-twoje-dane-zostaly-upublicznione [Accessed 15 May, 2024].
- Gul, S., Bano, S. and Shah, T., 2021. Exploring data mining: facets and emerging trends. *Digital Library Perspectives*, *37*(4), pp.429-448.
- Hilbert, M. (2012). Toward a synthesis of cognitive biases: How noisy information processing can bias human decision making. *Psychological Bulletin*, 138(2), pp.211–237.
- Joh, E. E. (2014). Policing by numbers: big data and the Fourth Amendment. *Washington Law Review*, [online] 89(1), p.35. Available at: https://digitalcommons.law.uw.edu/wlr/vol89/iss1/3/ [Accessed 15 May 2024].
- Kanungsukkasem, N., and Leelanupab, T. (2019). Financial latent Dirichlet allocation (FinLDA): Feature extraction in text and data mining for financial time series prediction. *IEEE Access*, 7, pp.71645–71664.
- Lee, B. C., and Kim, B. Y. (2021). Development of an AI-based interview system for remote hiring. *International Journal of Advanced Research in Engineering and Technology (IJARET)*, 12, pp.654–663.
- Lin, T. C. (2015). Financial weapons of war. *Minnesota Law Review 205*, 100, p.1377.
- Mangal, A. (2023). An Analytical Review of Contemporary AI-Driven Hiring Strategies in Professional Services. *ESP Journal of Engineering and Technology Advancements*, 3(3), 52–63.
- Moelants, D., Cornelis, O., Leman, M., Gansemans, J., De Caluwe, R., De Tré, G., Matthé, T., and Hallez, A. (2006). Problems and opportunities of applying data-and audio-mining techniques to ethnic music. *Conference on music information retrieval*, pp.334–336.
- Montoya, A. M., Parrado, E., Solís, A., and Undurraga, R. (2020). Bad taste: gender discrimination in the consumer credit market.
- Papakyriakou, D., and Barbounakis, I. S. (2022). Data mining methods: A review. *International Journal of Computer Applications*, 183, pp.5–19.
- Pasieczna, A. H. (2021). Model Risk of VaR and ES Using Monte Carlo: Study on Financial Institutions from Paris and Frankfurt Stock Exchanges. Contemporary Trends and Challenges. In *Finance: Proceedings from the 6th Wroclaw International Conference in Finance*, pp.75–85.
- Pegg, D., Makortoff, K., Chulov, M., Lewis, P., and Harding, L. (2022). Revealed: Credit Suisse leak unmasks criminals, fraudsters and corrupt politicians. The Guardian. Available at:

https://www.theguardian.com/news/2022/feb/20/credit-suisse-secrets-leak-unmasks-criminals-fraudsters-corrupt-politicians [Accessed 15 May 2024].

- Pejić Bach, M., Krstić, Ž., Seljan, S., and Turulja, L. (2019). Text mining for big data analysis in financial sector: A literature review. *Sustainability*, 11, p.1277.
- Perry, J. (2023). *Australian banks act to protect customers from financial abuse*. [online] Australian Banking Association. Available at: https://www.ausbanking.org.au/australian-banks-act-to-protect-customers-from-financial-abuse/ [Accessed 15 May 2024].
- Rimkus, R. (2016). *Long-Term Capital Management - Financial Scandals, Scoundrels & Crises*. [online] Available at: https://www.econcrises.org/2016/04/18/long-term-capital-management/ [Accessed 15 May 2024].
- Shiekh, H. (2022). AI as a Tool of Hybrid Warfare: Challenges and Responses. *Journal of Information Warfare*, 21, pp.36–49.
- Singh, A., and Kumar, D. (2022). Detection of stress, anxiety and depression (SAD) in video surveillance using ResNet-101. *Microprocessors and Microsystems*, 95, p.104681.
- Sipior, J. C., Ward, B. T., and Rongione, N. M. (2004). Ethics of collecting and using consumer internet data. *Information Systems Management*, 21, pp.58–66.
- Srinivasan, R., and Chander, A. (2021). Biases in AI Systems: A Survey for Practitioners. *Queue* 19(2), pp.45–64.
- Tirkey, A. (2021). The World Bank data manipulation controversy: A cause for worry [online] Available at: https://www.orfonline.org/expert-speak/the-world-bank-data-manipulation-controversy [Accessed 15 May 2024].
- Wever, M., Shah, M., and O'Leary, N. (2022). Designing early warning systems for detecting systemic risk: A case study and discussion. *Futures*, 136, p.102882.
- Wilson, R. (2019). Cambridge analytica, Facebook, and Influence Operations: A case study and anticipatory ethical analysis. *European conference on cyber warfare and security*, p.587.
- Zhang, D. (2021). *Fundamentals of image data mining*. Springer International Publishing.
- Zhang, Y., and Cheung, Y.-M. (2014). Discretizing numerical attributes in decision tree for big data analysis. *2014 IEEE International Conference on Data Mining Workshop*, pp.1150–1157.