Implementing Cyber Security tools and techniques in Crime Prediction LR

Introduction

The rise of online business models has spurred an evolution in criminal activity, necessitating the use of cybersecurity tools as countermeasures. Crime can be classified as conventional or cyber-enabled and premeditated or spontaneous, allowing for targeted prevention and mitigation strategies. Cybersecurity tools like IDS, SIEM, and threat intelligence platforms are crucial for monitoring and analysing data for potential criminal activity (Taddeo & Floridi, 2018).

This literature review aims to assess the efficacy and accuracy of such tools, to identify their strengths and weaknesses, and to explore their ethical and legal implications (Perry et al., 2013). This paper provides valuable insights for improving crime prediction and prevention strategies for researchers, law enforcement, policymakers, and cybersecurity professionals by leveraging the latest research findings.

Objectives and Significance of the LR

- The purpose of this communication is to apprise law enforcement officials, policymakers, and members of the cybersecurity community about the potential benefits of optimising and integrating current tools into existing crime prevention strategies (Maimon & Louderback, 2019).

- It is required to take into account the challenges and constraints associated with the usage of such tools. These could encompass technical, ethical, and practical considerations like data accuracy, privacy concerns, and the potential for bias in predictive modelling (Omand et al., 2012).

Trends in CS tools integration in crime prediction

1) Machine Learning and Predictive Analytics. In crime prediction, machine learning algorithms have been utilised to analyse crime data and anticipate forthcoming criminal patterns. Decision trees, random forests, and support vector machines are among the algorithms trained on crime data from different cities to forecast future crime patterns precisely (Raza & Victor, 2021).

2) Big Data Analytics and Mining. The proliferation of a diverse array of data sources, encompassing surveillance cameras, social media platforms, and Internet of Things (IoT) devices, has engendered a substantial surge in the employment of big data analytics to predict criminal activity (Feng et al., 2019). This has paved the way for law enforcement agencies to identify and respond to potential threats in a more effective manner. The utilisation of these analytics has enabled law enforcement to recognise emerging patterns and trends, thereby enhancing their ability to mitigate and prevent crime.

3) Cyber Threat Intelligence Sharing. Timely and accurate information is crucial for effective crime prediction. To mitigate cybercrime, sharing cyber threat intelligence is

becoming an increasingly important trend within and across law enforcement agencies. In order to establish and maintain a robust and effective security framework, it is imperative to foster a collaborative global effort towards standardising the sharing and structuring of cyber threat intelligence information. Such standardisation will pave the way for developing cutting-edge, knowledge-based strategies that offer substantially higher levels of automation and actionability (Arenas, ND).

4) Integration of CyberSecurity tools in IoT devices. The exponential rise in the usage of Internet of Things (IoT) devices has led to a multitude of opportunities and challenges. In order to mitigate the risks of cybercrime and enhance the ability to forecast criminal behaviour, cybersecurity tools must be integrated into IoT devices (Alterazi et al., 2022).

Strengths and Limitations of CS tools in LR

A) Strengths

- Enhanced Prediction Accuracy. Law enforcement agencies can utilise machine learning algorithms integrated into CyberSecurity tools to quickly and precisely analyse massive datasets, leading to more informed decision-making and efficient resource allocation; an example is the city of Chicago, with 75.6 % accuracy in crime prediction (Safat et al., 2021).
- Real-time Monitoring**.** With the assistance of cybersecurity tools, security analysts can effectively monitor and detect potential cyber threats in real time. This capability allows for swift response to emergent criminal activities while

enabling the development of comprehensive risk assessment models (Javed et al., 2022).

- Extensive data tools aid law enforcement in extracting insights from diverse sources. Upon utilising various data extraction methods, including aggregation, classification, and other techniques, areas with higher crime rates were pinpointed, allowing for efficient allocation of police resources to those regions.
- Interdisciplinary Collaboration. Due to the unexplored nature of emerging Cybercrime, Experts in Cybersecurity, data science, law enforcement and psychology can collaborate to develop innovative solutions (Payne & Hadzhimova, 2020). Interdisciplinary problem-solving can lead to advanced tools and techniques to tackle security threats, creating a more secure environment for everyone.

B) Weaknesses and Limitations

- The breach of privacy and disregard for fundamental human rights such as the presumption of innocence until proven guilty with concrete evidence. Such an example of predictive policing empowered by big data mining was noticed in the US and China with the Palantir company, which provided the data for the police to perform massive arrests (Lindsey, 2018). Another example where integrating cybersecurity tools has circumvented the right to privacy is the Encrochat case when Europol arrested thousands of criminals using an encrypted network (Europol, ND). Though these accomplishments sound astonishing, they create a dangerous precedent in how the data are obtained with non-transparent

procedures in non-ethical ways (Burgess, 2023). As per this essay's author's opinion, Democracy is jeopardised in the name of absolute Security.

- Bias in Predictive Algorithms. Machine learning algorithms used for predicting crime can be susceptible to inheriting biases from historical data, which can lead to discrimination against specific communities. Thus, addressing this ethical issue poses significant challenges that require careful consideration (Lum & Isaac, 2016). Predictive algorithms shape experiences and social ties in various domains of today's lives, and they often are accepted. However, it is crucial to address harmful biases resulting from the simplistic use of predictive algorithms (Fazelpoour & Danks, 2019).
- Data Confidentiality and Security issues. Ensuring the Security of the copious amount of data gathered for crime prediction is a matter of supreme importance. It is crucial to maintain the confidentiality and integrity of the collected data to prevent unauthorised access and potential data breaches. The significance of data security in this regard should be considered and should remain a top priority for all entities involved in the collection and application of said data (Bhatia et al., 2016).
- Lack of Human and Security infrastructure resources. The literature review presents a notable gap in the absence of the human element. Specifically, there is a dire global need for professionals competent in Cybersecurity and possessing technical knowledge to operate the various systems mentioned in the study. This need arises from the need for more talent in Cybersecurity. It is crucial to address this issue as the systems highlighted in the review demand a

skilled workforce to ensure proper functioning and Security. Therefore, it is imperative to foster and support the development of cyber-competent professionals globally to meet the growing demand of the industry (Cobb, 2016). Furthermore, the utilisation of cutting-edge cybersecurity tools and methods may demand substantial financial investments, something that specific law enforcement organisations may not possess.

C) Opportunities

When faced with a challenge, it is essential to recognise the potential opportunities for further development and growth.

1) The integration of Deep Learning in Cybersecurity has shown promising results in the creation of more effective and resilient hybrid models. The advancement of Cybersecurity tools and science has the potential to accurately predict crime rates, as exemplified by the BERT algorithm's superior performance in crime detection (Boukakous & Azizi, 2022). Combining these two domains can lead to a significant improvement in the accuracy and efficiency of crime detection methods. This approach has the potential to revolutionise the field of Cybersecurity and contribute to the development of advanced systems capable of detecting and mitigating cyber threats.

2) International cooperation. It is not uncommon for both criminal and cyber offenders to relocate internationally as a way to avoid their home government's jurisdiction and

prosecution. Implementing cybersecurity tools can present a unique opportunity for collaboration among law enforcement agencies. This type of cooperation permits the exchange of information that can lead to the development of better crime prediction and prevention strategies. Furthermore, it can foster joint operations between agencies (UNDOC, 2020).

3) Ethical and Legal Frameworks. Fortunately, a robust legal and ethical framework has been developed to address the issues surrounding privacy and data confidentiality. This framework is enshrined in the General Data Protection Regulation (GDPR) in Europe, which ensures that crime prediction is carried out responsibly and equitably. By adhering to the principles of the GDPR, organisations can ensure that their use of predictive analytics is conducted transparently and that individuals' rights are respected. Overall, the GDPR framework provides a solid foundation for ensuring that crime prediction is conducted in a manner that is both ethical and compliant with legal requirements (Andrasko et al., 2021).

4) Training and Education. The field of Cybersecurity and its accompanying tools are in a constant state of flux, necessitating the continuous training of law enforcement agencies alongside private sector analysts who are responsible for developing predictive tools aimed at combating criminal activities. Given the dynamic nature of this field, these professionals must remain up-to-date with the latest advancements in Cybersecurity to ensure that their predictive models and strategies remain effective. Failure to do so may result in the loss of valuable data, compromise network security,

and other detrimental outcomes. As such, these professionals must invest in ongoing training and development opportunities to remain competitive and effective in their respective roles.

Research gaps and conclusion

1) Ethical Considerations. Despite the recognition of ethical considerations as vital components of the successful implementation of cybersecurity tools in crime prediction, there exists a significant gap in research and governance in the form of comprehensive ethical frameworks. Such frameworks are critical for ensuring that the implementation of these tools is carried out thoughtfully and responsibly. Currently, there is no controlling or regulating mechanism for applied Ethics in Cybersecurity (Macnish & Van der Ham, 2020).

2) Data Quality. In the realm of crime prediction studies and the application of CS tools, the existence of high-quality data is often considered a prerequisite. However, the need to confront the issue of data quality arises in the face of scenarios where data may be incomplete or manipulated. Further research is essential to address these data quality concerns and to develop practical solutions that can be applied in practice (Ribeiro et al., 2016). The author suggests that AI and machine learning models should support lawmakers and enforcers rather than make decisions. This approach can combine human expertise with AI's capabilities and foster a more effective decision-making process.

3) Standardisation. The current literature reveals a need for more standardised methodologies and evaluation criteria for assessing cybersecurity tools in crime prediction. This void challenges businesses and academic institutions as they seek to evaluate the efficacy of such tools. Research endeavours must focus on developing comprehensive evaluation metrics that can facilitate the assessment of cybersecurity tools in crime prediction. Such metrics can provide clarity and consistency in evaluating the performance of these tools. For example, current monitoring methods use host/network-based monitoring to gather forensic evidence for threat detection; this includes appliances such as Intrusion Detection/Prevention and Data Leak Detection/Prevention System. However, no single method provides a complete view of the insider threat problem (Greitzer & Ferryman, 2013).

4) Human-centric approaches. The indispensability of technology in the field of Cybersecurity is undeniable. However, a significant research gap exists regarding incorporating human-centric approaches in cybersecurity tools for predicting crimes. Despite technology's critical role in the domain, this deficiency must still be adequately addressed (Dunn Cavelty, 2014). Furthermore, the practicality of technological tools is directly correlated with the proficiency of their users, who are, in this context, invariably human. The efficacy of these tools is, therefore, dependent on the ability of users to leverage them effectively and efficiently.

Epilogue

Incorporating cybersecurity tools and techniques into crime prediction significantly benefits public safety and Security. However, it is imperative to address the associated challenges and ethical considerations. By fostering interdisciplinary collaboration and promoting ethical practices, the field of implementing cybersecurity tools in crime prediction can continue to evolve responsibly and effectively, contributing to a safer and more secure society. This literature review has provided a foundation for further research and policy development in this critical area, emphasising the need for a balanced approach that upholds individual rights and societal well-being while harnessing the power of technology for crime prevention and prediction.

References per group

Cybersecurity tools Group

Taddeo, M. and Floridi, L. (2018) Regulate artificial intelligence to avert cyber arms race. Nature 556(7701): 296-298.

Aim and Focus of the LR Group

Perry, W. L., McInnis, B., Price, C. C., Smith, S. C., & Hollywood, J. S. (2013). Predictive policing: The role of crime forecasting in law enforcement operations.

RAND Corporation. Available from: https://www.rand.org/pubs/research_reports/RR233.html. [Accessed 5 November 2023].

Maimon, D. and Louderback, E.R., 2019. Cyber-dependent crimes: An interdisciplinary review. Annual Review of Criminology, 2: 91-216.Available from: https://www.annualreviews.org/doi/full/10.1146/annurev-criminol-032317-092057 [Accessed 5 November 2023].

Omand, D., Bartlett, J., and Miller, C. (2012). 'Introducing social media intelligence (SOCMINT)', Intelligence and National Security, 27(6):801-823.Available from:https://www.tandfonline.com/doi/full/10.1080/02684527.2012.716965?scroll=top&needAccess=true [Accessed 5 November 2023].

Trends Group

Raza, D.M., & Victor, D.B. (2021). Data mining and Region Prediction Based on Crime Using Random Forest. International Conference on Artificial Intelligence and Smart Systems (ICAIS): 980-987, doi: 10.1109/ICAIS50930.2021.9395989.

Feng, M., Zheng, J., Ren, J., Hussain, A., Li, X., Xi, Y. and Liu, Q., (2019) Big data analytics and mining for effective visualization and trends forecasting of crime data. IEEE Access, 7: 106111-106123. Available from: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8768367 [Accessed 5 November 2023].

Arenas, E. (N.D) Cyber Threat Intelligence Information Sharing. School of Engineering and Technology CQUniversity, Australia e. arenas@ cqu. edu. au. Available from: https://www.researchgate.net/profile/Edilson-Arenas-2/publication/320034441_Cyber_Threat_Intelligence_Information_Sharing/links/59c9ed2b0f7e9bbfdc361b55/Cyber-Threat-Intelligence-Information-Sharing.pdf [Accessed 5 November 2023].

Alterazi, H., Kshirsagar, P., Manoharan, H., Selvarajan, S., Alhebaishi, N., Srivastava, G. and Lin, JC. (2022) Prevention of Cyber Security with the Internet of Things Using Particle Swarm Optimization. Sensors (Basel).2022 Aug 16;22(16):6117. doi: 10.3390/s22166117. PMID: 36015878; PMCID: PMC9413110.

Strengths Group

Safat, W., Asghar, S. and Gillani, S.A (2021). Empirical analysis for crime prediction and forecasting using machine learning and deep learning techniques.

IEEE access, 9:70080-70094. Available from: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9424589 [Accessed 5 November 2023].

Javed, A., Lakoju, M., Burnap, P. and Rana, O. (2022) Security analytics for real-time forecasting of cyberattacks. Software: Practice and Experience, 52(3):788-804.

Available from: https://orca.cardiff.ac.uk/id/eprint/129830/1/Security%20Analytics%20for%20real%20time%20forecasting%20of%20cyber%20%20attacks.pdf [Accessed 5 November 2023].

Abdullah, F. (2019). Using big data analytics to predict and reduce cyber crimes. International Journal of Mechanical Engineering and Technology. 10:1540-1546.

Available from: https://www.researchgate.net/publication/331113136_Using_big_data_analytics_to_predict_and_reduce_cyber_crimes [Accessed 6 November 2023].

PAYNE, B.K. and HADZHIDIMOVA, L. (2020). Disciplinary and Interdisciplinary Trends in Cybercrime Research: An Examination. International Journal of Cyber Criminology, 14(1):81-105.Available from: https://www.proquest.com/docview/2404396105?pq-origsite=gscholar&fromopenview=true [Accessed 6 November 2023].

Weaknesses Group

Lindsey, N. (2018) Predictive Policing Raises Important Privacy and Human Rights Concerns.

Available from: https://www.cpomagazine.com/data-privacy/predictive-policing-raises-important-privacy-and-human-rights-concerns/ [Accessed 6 November 2023].

Europol (N.D) Dismantling encrypted criminal EncroChat communications leads to over 6 500 arrests and close to EUR 900 million seized.

Available from: https://www.europol.europa.eu/media-press/newsroom/news/dismantling-encrypted-criminal-encrochat-communications-leads-to-over-6-500-arrests-and-close-to-eur-900-million-seized [Accessed 6 November 2023].

Burgess, M. (2023) Cops Hacked Thousands of Phones. Was It Legal?

Available from:

https://www.wired.com/story/encrochat-phone-police-hacking-encryption-drugs/

[Accessed 6 November 2023].

Lum, K., & Isaac, W. (2016). To predict and serve? Significance, 13(3):14-19. Available from:

https://rss.onlinelibrary.wiley.com/doi/pdf/10.1111/j.1740-9713.2016.00960.x?shared_access_token=IDAY641RsV7xsRV6B1hl04ta6bR2k8jH0KrdpFOxC677Uo2ZpRJGfPu343uxAHkqNhmTYCA7Luw-6h3KOpptkCw153jVJOMXzw25e_4e82JLu75RVoBQza76WyvWFk7BJN2b0K0j-zwfXRgYNqUDbybnAVsHSC6KhR9WXrKYTMY%3D [Accessed 6 November 2023].

Fazelpour, S. & Danks, D., 2021. Algorithmic bias: Senses, sources, solutions. Philosophy Compass, 16(8), p.e12760.

Bhatia, J., Breaux, T.D., Friedberg, L., Hibshi, H. and Smullen, D. (2016) Privacy risk in cybersecurity data sharing. In Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security (pp. 57-64).

Available from: https://dl.acm.org/doi/pdf/10.1145/2994539.2994541 [Accessed 6 November 2023].

Cobb, S. (2016). Mind this Gap: Criminal hacking and the global cybersecurity skills shortage, a critical analysis. In Virus Bulletin Conference (pp. 1-8).Available from: https://www.virusbulletin.com/uploads/pdf/magazine/2016/VB2016-Cobb.pdf [Accessed 6 November 2023].

Opportunities Group

Boukabous, M. and Azizi, M. (2022). Crime prediction using a hybrid sentiment analysis approach based on the bidirectional encoder representations from transformers. Indones. J. Electr. Eng. Comput. Sci, 25(2):1131-1139.

Available from: https://www.researchgate.net/profile/Mohammed-Boukabous/publication/358129186_Crime_prediction_using_a_hybrid_sentiment_analysis_approach_based_on_the_bidirectional_encoder_representations_from_transformers/links/61f17606c5e3103375c17258/Crime-prediction-using-a-hybrid-sentiment-analysis-approach-based-on-the-bidirectional-encoder-representations-from-transformers.pdf

[Accessed 6 November 2023].

UNDOC (2020) Comprehensive Study on Cybercrime. Available from: https://www.unodc.org/unodc/en/organized-crime/comprehensive-study-on-cybercrime.html [Accessed 6 November 2023].

ANDRAŠKO J., MESARČÍK M. and HAMUĽÁK O. (2021) The regulatory intersections between artificial intelligence, data protection and cyber security: challenges and opportunities for the EU legal framework.

AI & Society, 36(2):623-636.Available from:https://www.proquest.com/docview/2553125839?fromopenview=true&pq-origsite=gscholar [Accessed 6 November 2023].

LR GAPS

Macnish, K. & Van der Ham, J. (2020) Ethics in cybersecurity research and practice.Technology in Society.Volume 63,

Available from: https://www.sciencedirect.com/science/article/pii/S0160791X19306840 [Accessed 6 November 2023].

Ribeiro, M.T., Singh, S. and Guestrin, C. (2016). "Why should I trust you?" Explaining the predictions of any classifier.

In Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (pp. 1135-1144).

Greitzer, F.L. & Ferryman, T.A. (2013) Methods and metrics for evaluating analytic insider threat tools. In 2013 IEEE Security and Privacy Workshops (pp. 90-97). IEEE.

Dunn Cavelty, M. (2014) Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. Science and engineering ethics, 20:701-715.