Evaluating the Effectiveness of Cybersecurity Tools and Techniques in Predicting Digital Crime: A Comparative Analysis

Introduction

Cybersecurity has become vital today as the dependence and overreliance on digital infrastructure and internet services grew exponentially. Consequently, implementing cybersecurity detection and prevention measures is crucial to safeguard valuable information and resources. Cyber-enabled unlawful behaviour is becoming a problem beyond boundaries and can affect areas of remote jurisdictions; as mentioned by CISA, the Authorities provide guidelines to protect individuals and critical infrastructure in the US, UK and Australia (CISA, 2022). Cybercriminals are using more sophisticated attacks, which has led to the development of new tools. Artificial Intelligence (AI) and Machine Learning are now popular tools among cyber experts to combat evolving threats (Butkar & Waghmare, 2023). Despite the plethora of tools offered to the authorities and the security experts, it would be prudent to evaluate them rather than trust them unquestioningly.

Significance and Contribution of the Current Research in the Discipline

1) Improvement in Prediction and Prevention of Digital Crime. Early and timely detection of cybercrimes is crucial due to their ever-changing nature. Using effective tools can minimise their impact and, hence, their cost. Such an example can be the Cyber Security Modeling Language (CySeMol), which addresses and can effectively

predict multi-faceted threats on industrial control systems known as SCADA networks (Sommestad et al., 2012). Ensuring the safety of the residents of any country holds immense value. It is a crucial aspect that demands attention and prioritization.

2) Cybersecurity Tools Improvement and Development of new ones. Based on the study's findings, incorporating more sophisticated algorithms into intrusion detection systems (IDS) may be necessary as traditional cyber defences, such as firewalls, are currently inadequate (Modi et al., 2013). Finding existing cyber defences' vulnerabilities and weak spots could catalyse further research and development, bringing new technological advancements to light. Moreover, AI-powered cybersecurity systems can be autonomously deployed with minimal human intervention and continuously process extensive data and incidents. This autonomous processing capability is made possible by the underlying algorithms that enable the system to learn and adapt to new threats. AI-based systems can dramatically reduce the workload on human cybersecurity experts and improve overall efficiency by instantly identifying and responding to security threats (Prasad et al., 2020).

3) Strategic Cybersecurity Planning. Assessing the effectiveness of cybersecurity tools and techniques can impact corporate, financial, and national security decision-making. More specifically, Local SMEs are frequent targets, with 72% of breaches by cyber attackers, and have limited funding for cyber security, often working with a fixed budget and no extra funds available (Rees et al., 2011). The research results can determine the investment height in developing appropriate and more efficient

tools. Moreover, at the state level, it can affect the level of national security and the confidentiality, integrity and availability of critical data that each country possesses and affect policies and laws that can come into application (Sabillon et al., 2016)

4) Raising awareness about the potential dangers of cybersecurity threats is crucial in today's digital landscape. Improving the cybersecurity posture of individuals and organizations is imperative to mitigate risks and protect sensitive information. Seeking guidance and assistance from cybersecurity experts and law enforcement agencies can provide the necessary knowledge and support to enhance cybersecurity measures.

Research Question

How effective are various cybersecurity tools and techniques in preventing and predicting digital crime?

Aims and Objectives of the Research Proposal

1. Evaluate the precision and effectiveness but also the shortcomings of these instruments.
2. Analysis of the Predictive Capabilities of Cybersecurity Tools and Techniques
3. To include the often underestimated human factor and user experience as integral parts of the Security policies and components while efficiently implementing the tools and strategies.

Literature Review on the implementation of CS tools in crime prediction

A) Strengths

- High-speed querying of security intelligence data
- Real-time abnormality detection of diverse security data
- Network forensics (the measurement of network performance variables)
- Real-time analytics tools enable continuous monitoring of sensitive data, providing immediate alerts and responses to threats. Being proactive is critical to prevent or minimize the impact of cyberattacks.
- Root Cause Analysis: It is possible to trace back to the origin of any security incident and identify its cause, determine the event's occurrence, the specifics of what took place and how it infiltrated the network

(Mahmood & Afzal, 2013).

B)Weaknesses

- The adaptability of Cyber Threats and AI/ML training. Keeping up with the constantly evolving network information is a challenge in DL and ML model training and deployment. These models require frequent and extensive retraining, emphasizing the need to shift focus towards incremental and lifelong learning for future advancement in this field (Xin et al., 2018).
- Complexity and Resource Requirements. Not all organisations can keep up, as many financial and human resources are required to integrate AI and ML into their cyber defences (Dash et al., 2022).
- AI mechanisms used by Criminals. The incorporation of artificial intelligence in the field of cybersecurity presents a unique challenge as it possesses a dual

nature. Malefactors may exploit its potential to automate attacks, magnifying the severity of security breaches (Dash et al., 2022).

- IDP brings challenges like unbounded patterns, uneven time lags, nonstationarity, high dimensionality, interdependent features, false alarms, class imbalance, insider attacks, uncertainty, and a large number of parameters (Gheyas & Abdallah, 2016).

C) Gaps

The role of humans in security also called the human factor or human firewall, is critical. The intuition and expertise of humans can often surpass even the most sophisticated security algorithms in detecting potential threats.

- User Personality Traits and Cybersecurity Practices. User behaviour is a crucial element of the human factor in cybersecurity. Security defences are often compromised due to user ignorance, carelessness, or reluctance to adhere to security policies (Hadlington, 2017). Even with robust technical defences, human errors or careless actions can lead to significant security breaches. This gap in the literature indicates a need for more Research on effective strategies to improve cybersecurity awareness and practices among users.
- Human-Centric Cybersecurity Solutions. The literature also indicates a gap in Research on human-centric cybersecurity solutions. Cybersecurity systems and policies often prioritise technical measures over designing systems considering human behaviour and psychology. A more effective approach would involve designing user-friendly security interfaces and systems that align with natural human behaviours to ensure compliance and reduce errors

(Furnell, 2005). In organisations, employees often ignore security policies due to a lack of understanding, making security an additional workload and adding stress for critical system users.

- Insider Threats. Insider threats in cybersecurity include intentional and unintentional acts. Research on detecting insider threats focuses on the technical aspect and overlooks comprehending insider motivations and behaviours (Randazzo, 2004).

Methodology of Research

The Methods that will be applied will include two Quantitative and two Qualitative questionnaires (Mixed Method Approach).

Qualitative: Detailed responses about experiences, opinions, and perceptions regarding cybersecurity tools and techniques will be obtained through open-ended questions in the questionnaire. The targeted audience will be cybersecurity experts, IT professionals, and professionals from organisations already implementing cybersecurity measures. Participants can complete the questionnaire online or during a personal interview based on availability and preference.

Quantitative: Closed-ended questions, multiple-choice questions, and ranking scales will be used in this survey, with responses rated on a Likert scale. As part of our research study, we will invite a diverse group of individuals, including IT personnel, cybersecurity experts, and managers, to participate. The selection process will be randomised to ensure a fair representation of the intended

population. We will leverage electronic questionnaire distribution platforms such as SurveyMonkey or Google Forms to facilitate the process. All responses will be automatically logged and saved in a secure database for further analysis. Statistical software tools such as SPSS or R will analyze the data and calculate the mean, median, mode, and standard deviation. This will enable us to understand central tendencies and dispersion better. Descriptive and Inferential Statistics will also be used in Data Analysis.

Ethical Considerations

1) Informed Consent. Obtaining informed consent from all participants is imperative as it is a crucial ethical requirement. Participants should be provided with comprehensive information regarding the Research's aim, methodology, potential ramifications, and their rights as participants (Saunders et al., 2009).

2) Confidentiality and Anonymity of the participants. The preservation of confidentiality and anonymity concerning participant data holds paramount importance, primarily in light of the sensitive nature of cybersecurity information. Hence, security and privacy must be prioritised for the data entrusted to the researcher (Israel & Hay, 2006).

3) Data Protection and Privacy. It is compulsory to adhere to GDPR during research endeavours to avoid penalties. (Situr et al., 2018).

Timeline of Proposed Activities

The Research can be implemented in three Phases

1) Pre-implementation of CyberSecurity tools questionnaire in crime prediction for Qualitative and Quantitative methods.

2) Post-implementation of CyberSecurity tools questionnaire in crime prediction for Qualitative and Quantitative methods.

3) Data Analysis

Integrating qualitative and quantitative methods is necessary to gain a deeper understanding of tool effectiveness. While quantitative data can show measurable changes in performance and security outcomes, qualitative data can provide valuable context and insight into user perception and reasons behind the changes. A strong methodological framework is established by combining pre- and post-implementation questionnaires and performance metrics. This approach enables the evaluation of cybersecurity tools' effectiveness in predicting digital crime and offers valuable insights into user experiences and operational impacts.

Conclusion

Nobody can accurately predict illegal behaviour or fully understand the perpetrators' motives. However, the discussed research proposal can increase the readiness levels in incident reactions. This Research aligns with the changing digital security landscape, which requires a more proactive approach to cybersecurity (Cavelty, 2014). Furthermore, Cybersecurity legal awareness and education can be dramatically increased.

References

Intro

CISA (2022) 2021 Trends Show Increased Globalized Threat of Ransomware. Available from: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-040a [Accessed on 26th November 2023].

Butkar, M.U.D. & Waghmare, M.J., (2023) Crime Risk Forecasting using Cyber Security and Artificial Intelligent.
Computer Integrated Manufacturing Systems, 29(2), pp.43-57.

Contribution

Sommestad, T., Ekstedt, M. and Holm, H., (2012) The cyber security modeling language: A tool for assessing the vulnerability of enterprise system architectures. *IEEE Systems Journal*, 7(3):363-373.

Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A. and Rajarajan, M., (2013) A survey of intrusion detection techniques in cloud.
Journal of network and computer applications, 36(1): pp.42-57.

Prasad, R., Rohokale, V., Prasad, R. and Rohokale, V., (2020) Artificial intelligence and machine learning in cyber security. Cyber Security: The Lifeline of Information and Communication Technology, pp.231-247.
Available from: https://link.springer.com/chapter/10.1007/978-3-030-31703-4_16 [Accessed on 27th November 2023].

Rees, L.P., Deane, J.K., Rakes, T.R. and Baker, W.H., 2011. Decision support for cybersecurity risk planning.
Decision Support Systems, 51(3):pp.493-505.

Available from:
https://www.sciencedirect.com/science/article/pii/S0167923616300239 [Accessed on 27th November 2023].

Sabillon, R., Cavaller, V. and Cano, J. (2016). National cyber security strategies: global trends in cyberspace.
International Journal of Computer Science and Software Engineering, 5(5):67.

Literature Review

Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., Gao, M., Hou, H. and Wang, C. (2018) Machine learning and deep learning methods for cybersecurity.
Ieee access, 6, pp.35365-35381.
Available from: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8359287 [Accessed on 26th Novermber 2023].

Dash, B., Ansari, M.F., Sharma, P. and Ali, A., (2022) Threats and Opportunities with AI-based Cyber Security Intrusion Detection: A Review. *International Journal of Software Engineering & Applications* (IJSEA), 13(5)

Gheyas, I.A. and Abdallah, A.E., (2016) Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis. *Big data analytics*, 1(1):1-29.

Mahmood, T. and Afzal, U. (2013) Security analytics: Big data analytics for cybersecurity: A review of trends, techniques and tools.
In 2013 2nd national conference on Information assurance (ncia) (pp. 129-134). IEEE.

Hadlington, L. (2017) Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon, 3(7).

Furnell, S., 2005. Why users cannot use security. Computers & Security, 24(4):274-279.Available from: https://www.sciencedirect.com/science/article/pii/S0167404805000532 [Accessed on 27th November 2023].

Randazzo, M.R., Keeney, M., Kowalski, E., Cappelli, D. and Moore, A. (2004) Insider threat study: Illicit cyber activity in the banking and finance sector (p. 25). United States Secret Service.

Ethical Considerations

Saunders, M., Lewis, P. & Thornhill, A. (2009) Research methods for business students. Pearson education.

Israel, M. & Hay, I. (2006) Research ethics for social scientists. Sage.

Available from: https://books.google.ae/books?hl=en&lr=&id=4Qtuv0CBuKkC&oi=fnd&pg=PP2&dq=+Israel,+M.,+%26+Hay,+I.+(2006).+Research+Ethics+for+Social+Scientists.+This+text+provides+a+comprehensive+overview+of+the+importance+of+maintaining+confidentiality+and+anonymity+in+research.&ots=U8CqSkrMu8&sig=5OasAIxvuYiz8lkF0c7WvvrPbMo&redir_esc=y#v=onepage&q&f=false [Accessed on 27th Novermber 2023].

Sirur, S., Nurse, J.R. and Webb, H. (2018) Are we there yet? Understanding the challenges faced in complying with the General Data Protection Regulation (GDPR). In Proceedings of the 2nd International Workshop on Multimedia Privacy and Security (pp. 88-95).

Conclusion

Cavelty, M.D., 2014. Cybersecurity in Switzerland. Springer International Publishing.