https://doi.org/10.52131/jcsit.2022.0301.0011

*i*RASD Journal of Computer Science and Information Technology

Volume 3, Number 1, 2022, Pages 01 - 06

Journal Homepage:
https://journals.internationalrasd.org/index.php/jcsit

Silent Saboteurs: Uncovering the Growing Threat of Data Poisoning in Operational AI Pipeline for Cybersecurity

Roy Okonkwo[1], Tawakalitu Omobolanle Abereijo[2], Raheem Babatunde Aguda[3]

[1] North Carolina A&T State University, Department of Information Technology, North Carolina, USA.
Email: riokonkwo@aggies.ncat.edu
[2] North Carolina A&T State University, Department of Computer Systems Technology, North Carolina, USA.
Email: toabereijo@aggies.ncat.edu
[3] Regent University College of Science and Technology, Accra, Ghana. Email: agudaraheem@gmail.com

ARTICLE INFO

Article History:
Received: August 24, 2022
Revised: November 28, 2022
Accepted: December 04, 2022
Available Online: December 10, 2022

Keywords:
Cyber Thefts
Information Technology
Operational Efficiency
Data Mining
Cybersecurity
Machine Learning
Digital Transformation
Protocols

ABSTRACT

The uncovering of the growing threats of data poisoning in operational artificial intelligence pipeline of cyber security refer to changing threats of cybers which is refreshing advancement and significant impact of artificial intelligence that is maintain survival protocol of thefts and training adverbials. Artificial negligence is acting as protective tools and security. Artificial intelligence managing overall information intelligence which is the combination part of cyber security that matters data poisoning in operational pipelines for cybersecurity. The growing threats internal processing in information of technology and define the digitalization. The digital twins of transforming working historical data related to artificial intelligence that matters for operational AI pipeline of cybersecurity. The scope of cybersecurity operation guiding the exploration of both features. Comprehensive analysis of artificial intelligence refers to identification, value management or vulnerability task of assessment and resilience of artificial intelligence which contributes as cyber security. It is related to cyber thefts and privacy concerns of uncovering threats of data poisoning which are growing at multiple positions. Artificial intelligence provides informative data perception and verifying the overall structured data and unstructured data in the systems.

Corresponding Author's Email: riokonkwo@aggies.ncat.edu

1. Introduction

The uncovering of growing threats of data poisoning in operation of artificial intelligence for cybersecurity defines silent saboteurs. The system of artificial intelligence is increasingly addressing issues related to fairness, transparency, and quality procedures. This focus enhances decision-making, reduces workloads, and addresses problems, particularly concerning cyber threats. Data mining involves the growing risk of data poisoning, highlighting the need for a systematic approach to improve financial conditions, operational efficiency, and market adaptability. Information technology is leveraging artificial intelligence to strengthen regulations and prevent the normalization of constant monitoring (Stoddart, 2022). The cyber security thefts meet with various privacy concerns treated by logical features that analysis the data structure. The session of cyber relation between AI that is for transformative in well documentation with application of resources optimization, predictive analysis and data mining while also supportive to solving problems and challenges which implication of information technology and cybersecurity is enhancing societal welfare.

Artificial intelligence is maintaining the silent saboteurs which mention with the growing threats of operational performance match cybersecurity in current situations. The bitter outlets that are refer deep learning and analysis of data behavioral in which make it on formative situational analysis of data management (Ramamoorthi, 2024). The big data analysis is developing sources of cybersecurity and artificial intelligence of infrastructure of information technology The study aims to role Artificial intelligence in identifying risks of cyber security threat analysis the behaviors segments implication of fostering developing the technical analysis in hyperrational efficiency. Artificial intelligence is driving the development in the IT sector, influencing growth in infrastructure through data analysis

.

2. Literature Review

Cyber security focuses on the relation between artificial intelligence, but the influence factors is enclaving the growing data poisoning in operational AI pipeline, it is matter of silent saboteurs. Cybersecurity refers to managing the change with artificial intelligence to advancing discussion about various threats. The detection of threats is behaving the predictive analysis position (Stoddart, 2022). Artificial intelligence focuses on cyberattacks, comparison between data, and validity in sensation of system The development of relation between operational pipelines of artificial intelligence with cybersecurity both managing technical privacy concerns regarding the growing threats of data poisoning.

2.1. An analysis of cyber security effectiveness

The analysis of cybersecurity effectiveness, particularly regarding context-based infrastructure, is influenced by various theoretical aspects of data poisoning. By evaluating the opportunities and effectiveness of cybersecurity, we can better understand its impact on formulating relevant theoretical frameworks. Data poisoning is an increasing concern, especially in relation to the operational efficiency of artificial intelligence. The technology innovation of cyber security makes it highly effective and focuses on developing innovative results which directly helps the information technology and artificial intelligence (Stoddart, 2022). The effectiveness of cybersecurity opens up new opportunities and changes perceptions as it evolves within the structural framework of the current era. The significant impact of artificial intelligence on cybersecurity has been a key topic of discussion among policymakers, particularly regarding issues such as data poisoning in operational AI systems. As information technology continues to advance, the implications of these developments on artificial intelligence are becoming increasingly important.

Cybersecurity thefts leverage information technology to influence data structure and analysis. Machine learning plays a significant role in decision-making and improving computer systems (Ramamoorthi, 2024). It is highly effective in enhancing cybersecurity and privacy features, particularly in relation to data poisoning. Artificial intelligence (AI) and machine learning are managing the cybersecurity threats, which are growing as a silent saboteur. The effectiveness and scope of current developments enhance productivity and simplify decision-making (Mylrea et al., 2021). This includes considering the present advantages and efficacy of cybersecurity, as well as exploring the potential benefits and various aspects of artificial intelligence in information technology.

2.2. Theoretical framework of cybersecurity

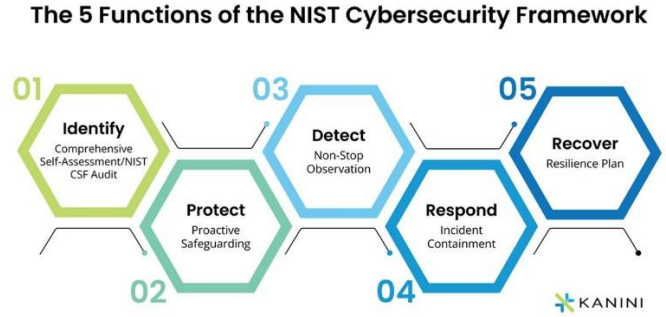

Figure1: Rational Framework of Cyber Security
Source (Mylrea et al., 2021)

The theoretical farmwork of cybersecurity is forcing too deep understanding of growing threats of data poisoning in operational of artificial intelligence pipeline of cybersecurity. It refers to identifying comprehensive self-assessment which is CSF audit and protecting the safeguarding of data merging. It is overall managing the authorities of understanding data margining while cyberattacks and thefts through getting from artificial intelligence. Theis factors maintain the power of build security in informational data management while it can remove the barriers of digital hacking and attacks (Mylrea et al., 2021). The framework of artificial intergenic protecting and proving road maps of artificial intelligence. While it's processing to detect nonstop observation and respond of incidents continents. Cyber security focused on resilience planning against cyber thefts. Multiple businesses can use the framework of cybersecurity based on their rules, follow up situation through the various guidelines and practices.

Through the systematic approach of cybersecurity making by mitigating the cyber risk and protecting from various problems and issues while organization mange the information technology factors and aligning them with artificial intelligence. The major factor of organization is managing operational efficiency and maintaining the data information and secret planning of production (Ramamoorthi, 2024). The framework of cybersecurity in that plays a crucial role which can be established a supportive environment and security posture while meeting with various requirements related to regulation of technology. The version expertise and IT stakeholder among the cybersecurity maintain the solution of cybersecurity partnership and barriers to organization and their department.

2.3. Challenges of growing threats of data poisoning

2.3.1. Privacy concern

The improvement of hacking and cyber-attacks leak the privacy circulation in data poisoning. It takes time to accuracy of artificial intelligence models with volume of data processing while its faithful analysis of internally about the consideration of and collection of data is often needed. The raising of critical trauma between holding the risk of privacy data (Charmet et al., 2022). After improving data comes the halted privacy risk concerns is key challenges that organizations should navigate in the era of artificial intelligence an increase in data comes the heightened risk of privacy breaches This dichotomy between data utility and privacy concerns is a key challenge that governments must navigate in the era of artificial intelligence.

2.3.2. Raw structured data poisoning

The availability of functional results in artificial intelligence (AI) requires the ability to process data values instantly and effectively within cybersecurity systems. This necessitates machines equipped with sufficient memory and processing speed, as they need to identify data threats and highlight the importance of AI development. Currently, many systems still rely on traditional applications, which may not meet current demands. The focus on traditional features often leads to the identification of direct information leaks that are inadequate for modern needs (Charmet et al., 2022). Improving the speed and validity of data mining processes will enhance decision-making efficiency.

2.3.3. Cyber-attacks and threats

The cyber-attacks and threats visualize the challenges of growing threats of data position. The privacy leak is improving distance of fracture which can be harassment of information technology. The mythology of cyber-attacks is coming through the survival parts in the technical issues. Mostly challenges coming through the growing data poisoned problems and issues (Charmet et al., 2022). The organization cerate and faces problems through digital factors which can be manipulated by the concept of growing threats, cyber-attacks, privacy features while processing the work.

2.4. The impact of AI on cybersecurity

Artificial intelligence is particularly significant in today's world, where it is integrated with technologies such as cloud computing, machine learning, data analytics, and internet services. Within the realm of information technology, cybersecurity plays a crucial role alongside artificial intelligence, helping to manage the infrastructure of the cyber world. However, cybersecurity also faces distinct risks, including privacy concerns, algorithm vulnerabilities, and internet threats. Using artificial intelligence, cybersecurity can enhance awareness of these risks (Sexton & Campbell, 2022). Cybersecurity necessitates a well-defined plan or strategy within an organization, as it encompasses various aspects, including but not limited to data security, information security, and operational security. The significant shifts brought about by digitalization require organizations to implement methods that assess their current level of cybersecurity awareness and strategy in order to effectively defend against cybercriminal attacks.

3. Research methodology

The research methodology is applying mixed which includes quantitative and qualitative approaches on the topic of uncovering the growing threats of data poisoning in operational artificial intelligence pipeline for cybersecurity which is implication of cyber security analysis which is implication of artificial intelligence while also using data measurement approaches the research design and action of focusing on contribution of analysis of the methodology. The impact of designing research which generalization and performance metric while also using contribution of measurement in the methodology (Sexton & Campbell, 2022). General methodology helps in the outcomes generation and predicts the future forecast resulting through the artificial intelligence integration and threats of cybersecurity which is growing the data poison in business intelligence systems alignment with information technology systems. It identifies digital activity and results from the methodology (Sexton & Campbell, 2022). Research Methodology has quantitative which is focusing survey, various interviews and google forms rather than qualitative analysis is focusing on finding data from second research data, newspapers, case study and older academic journals.

The mixed approach of methodology is determining the mixing of qualitative and quantitative data for analysis the integration of artificial intelligence and focusing of cyber security features that is grow the in threats algorithms of business intelligence systems. Data is sourced from various sampling frames, instruments, and ethical consideration which provides the expected result of outcomes. The Artificial intelligence integration and cybersecurity operational pipeline of data poisons mostly sources the data through the Linkert framework and google forms (Mauro, 2022). Through the primary data making questionnaire that have 25 questions and 50 participates. The secondary data is gathered from the newspaper, academic journals to identify and analysis the research or finding the gaps and problems related with organizational areas in business intelligence systems. Although the data provides specific and accurate Information and considers the ethical environment of business intelligence systems. Through the data source, analysis the various challenges, issues, problems, and advantages and getting best practices and strategies (Mauro, 2022).

4. Discussion and Finding

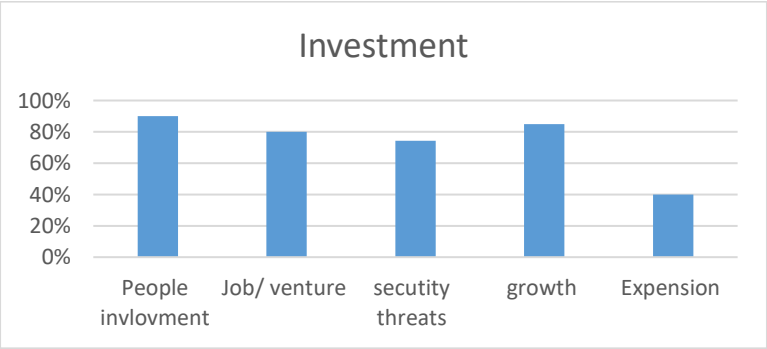

Figure 2: Data Analysis of AI Integration & Cyber Security

The factors of research analysis are briefing the knowledge of uncovering the growing threats of data poising in operational artificial intelligence pipeline for cybersecurity. Analysis the plan through the data approach and find a visual graph and numerical assumption that cybersecurity impaction. The secondary data gathering the information that patent available of artificial intelligence more 170,000 and 90% people is depending on the cyber security and artificial intelligence system in the worldwide. The total venture of cybersecurity and cybersecurity jobs is surrounding the 3.5 billion global level. The information is based on assumption which is implementing artificial intelligence and integration of cybersecurity with meet the data poisoning in the information technology (Mauro, 2022). The use of complex algorithms in AI can pose challenges; these routines are not free, and they often require more time for execution. Consulting AI for guidance tends to increase the time taken to complete routine tasks. However, AI also enhances the effectiveness of cybersecurity, which has important implications for the management of growing data volumes (Hollis & van Benthem, 2021). In the chart it explains the investment of people participation, security threats, growth and expansion which is 90% to expansions show the 40%. while the integration of chart is development of artificial intelligence focusing on the percentage which is growing day by day.

The research is finding the threats of which is implementing the gaps analysis of the cyber security operational people line of artificial intelligence which focused on the research Despite the growing prevalence of AI-driven surveillance in the cyber security features which can b implicate d with data poisoning managing there is a growing notable dearth of research examining its impact on information technology and cyber threats wellbeing (Hollis & van Benthem, 2021). Existing studies have primarily focused on the benefits of artificial intelligence integrating with cyber security such as improved productivity and quality control, while neglecting the potential financial prediction of information costs. In the study specifics gaps is limited understanding of uncovering growth of data poison impacts few studies have investigated the specific effects of AI driven surveillance cyber security, including risk of techniques and decreased Lack of consideration for system of artificial intelligence and data mining process is most research has focused on the particular focus for platforms and stakeholders and users (Hollis & van Benthem, 2021). Insufficient exploration of the contextual factors is impact of AI driven and machine learning inputs in through the mechanical function of cyber information and thefts may vary depending on factors such as work type, platform the polices, and individual worker characteristics which have not been thoroughly examined Methodology limitations often rely on self-reported data or limited samples which may not accurately capture the complexity of gig workers experiences. The Main research suggestion to investigate the of AI driven surveillance on cyber security data poison which is maintain the operational pipe (Aiken et al., 2021). Explore further experiences and perspectives of gig workers regarding surveillance. Examine the contextual factors influencing.

5. Conclusion

The summarizing of silent saboteurs which is uncovering the growing threats of data poisoning in operational artificial intelligence that is determining the features fairness and transparency of AI, which is integrating with cyber security, both factors are implication with social integration. The information technology factor is developing the key area of threats and data poison. Multiple factors of source that can be affected by cyber theft, cyber-attacks and hacking the system to leak privacy and security of organization. It is impacted on top socialization that is focused to greediness of thefts. This focuses on effectiveness of cyber security and integration with artificial intelligence which are making influences of competition in the organization. These strategies help in integration outcomes of business intelligence is defined sourcing of artificial intelligence and machine learning. Which provides fair and well resulting, developing, and aligning with organization information systems.

The integration of artificial intelligence and machine acquiring algorithms in cyber security business intelligence systems also includes their limitations, advantages, challenges, and practices through the analysis plan of implementation. determining the learning factors for AI and cyber security in BI focusing on blurred scope and deep analysis factors which are organizational mentors focusing on business organization and industry

agnostic, theoretical and practical factors are focused on theoretical framework and performance takeaway only. Some diverse types of scope defining the current state and future research direction. The delimitation study provides deep analysis process and focuses on the integration of AI and cyber security in growing data poisons in Business systems, generating profit inside and various challenges implication with cyber security risk and thefts which is interacting with artificial intelligence.

Reference

Aiken, M., Donaldson, S., & Tinnelly, C. (2021). Pathways to Online Hate: Behavioural, Technical, Economic, Legal, Political & Ethical Analysis.

Charmet, F., Tanuwidjaja, H. C., Ayoubi, S., Gimenez, P.-F., Han, Y., Jmila, H.,…Zhang, Z. (2022). Explainable artificial intelligence for cybersecurity: a literature survey. *Annals of Telecommunications*, *77*(11-12), 789-812. https://doi.org/10.1007/s12243-022-00926-7

Hollis, D. B., & van Benthem, T. J. (2021). Threatening Force in Cyberspace. *Temple University Legal Studies Research Paper*(2022-02).

Mauro, A. (2022). *Hacking in the Humanities: Cybersecurity, Speculative Fiction, and Navigating a Digital Future*. Bloomsbury Academic.

Mylrea, M., Nielsen, M., John, J., & Abbaszadeh, M. (2021). Digital Twin Industrial Immune System: AI-driven Cybersecurity for Critical Infrastructures. In W. F. Lawless, R. Mittu, D. A. Sofge, T. Shortell, & T. A. McDermott (Eds.), *Systems Engineering and Artificial Intelligence* (pp. 197-212). Springer International Publishing.

Ramamoorthi, V. (2024). AI-Driven Cloud Resource Optimization Framework for Real-Time Allocation. *Journal of Advanced Computing Systems*, *1*(1), 8-15. https://doi.org/10.69987/JACS.2021.10102

Sexton, M., & Campbell, E. (2022). Cyber War and Cyber Peace.

Stoddart, K. (2022). Cyberwar: Attacking Critical Infrastructure. In *Cyberwarfare* (pp. 147-225). Springer International Publishing.

Appendix