Leveraging AI for Preventive Data Security in the Canadian Communications Security Establishment

Roy Luo

Department of Electrical and Computer Engineering

University of Waterloo

r55luo@uwaterloo.ca

***Abstract*— The significance of cybersecurity cannot be overstated when it comes to the functionality, safety, and public trust in government institutions. In this context, the advent of artificial intelligence (AI) emerges as a pivotal asset for bolstering defences against cyber threats. This paper delves into the imperative to integrate anomaly detection and predictive analytics, leveraging Gaussian Mixture models, time series analysis, and predictive functions. The goal is to synergistically enhance the cyber defence mechanisms of the Canadian Securities Establishments (CSE) in response to the ever-evolving landscape of cyber threats.**

***Index Terms* — Anomaly Detection, Predictive Analytics, Summarization, Canadian Securities Establishment, Cyber Security, Machine Learning, Artificial Intelligence, Data Science, Data Engineering, Software Engineering**

I. Introduction

In the digital age, where the battlefield has shifted from physical realms to the network of the internet, the story of the Trojan horse finds a modern parallel. A seemingly harmless domain acts as a contemporary Trojan horse, concealing a threat posed to wreak havoc within a network. Users encounter URLs they believe to be harmless outlets, unknowingly triggering a digital Trojan horse that points to malware. Similar to the citizens of Troy, users innocently interact with deceptive URLs, enabling the malware to infiltrate their systems unnoticed. Once inside, the malware remains dormant until the opportune moment.

This digital Trojan horse, rooted in the association between the URL and the IP address, serves as a metaphor for the contemporary cybersecurity challenges. It underscores the importance of robust defence mechanisms to detect and neutralize such threats before they can unleash their destructive potential.

In 2017, The National Security Agency (NSA) of the United States Department of Defense released intel on a group called "The Shadow Brokers[1]," who had successfully breached the NSA database and stole the NSA's most powerful hacking tools and cybersecurity weapons [2]. This incident underscored the vulnerability of even the most sophisticated cybersecurity organizations. The repercussions were felt globally as these stolen hacking tools were subsequently released into the wild, potentially falling into the hands of malicious actors with the risk of espionage and large-scale cyberattacks [2].

Similarly, closer to home, the Canadian Communications Security Establishment (CSE) faces an ever-growing threat landscape. According to the PwC's Global State of Information Security, "Cyberthreats within Canada have increased by 82% year by year" [3]. As Canada's national cryptologic agency, responsible for foreign signals intelligence and cybersecurity, the CSE plays a critical role in safeguarding the country's digital infrastructure. The escalating frequency of cyber intrusions poses a direct challenge to the CSE's mission, making it imperative to explore and

[1] "The Shadow Brokers" a hacking group that gained prominence in 2016 for leaking classified information and hacking tools that were allegedly obtained from the Equation Group, a highly sophisticated cyber-espionage group widely believed to be associated with the NSA [1].

implement cutting-edge technologies to fortify its defences.

As technology advances, so do the tactics of cyber adversaries, necessitating a proactive and adaptive approach to cybersecurity. The escalating frequency of cyberattacks severely threatens data security, particularly within sensitive sectors such as government security institutions like the CSE. With Acemoglu's essay, “Redesigning AI,” we can dive into the intricate landscape of modern technology and the ethical and responsible usage of AI technologies and machine learning models to face cybersecurity challenges [4]. It becomes imperative to explore innovative solutions that not only detect but proactively mitigate potential data breaches.

In response to this pressing issue, this paper focuses on the proactive applications of AI, specifically anomaly detection and predictive analytics, to fortify the defences of the CSE against potential cyber intrusion and patching system vulnerabilities. While existing literature delves into various aspects of AI-driven data security, a distinctive gap lies in the exploration of applications of preventive AI implementations across government cybersecurity organizations. This begs the question: To what extent can anomaly detection, and predictive analytics, be utilized to proactively detect and mitigate data breaches caused by hacking, thereby enhancing data security within the Canadian Communications Security Establishment?

II. Methodology

To address the research question, a multi-dimensional approach will be adopted.

Literature Review: A comprehensive review of existing literature on AI-driven data security, cyber intrusion prevention, and relevant technologies will help build evidence for a comprehensive argument.

Technology Assessment: Evaluating the capabilities of Anomaly Detection and Predictive Analytics, in the context of CSE’s security demands.

Feasibility Analysis: Examining the social implications of implementing proposed AI solutions.

III. Literature Review

In the digital age, characterized by an ever-evolving landscape of cyber threats, the role of artificial intelligence (AI) in cybersecurity becomes increasingly critical.

Engineers affiliated with the Institute of Electrical and Electronic Engineers address the critical issue of cybersecurity vulnerabilities in power grid substations, particularly focusing on the potential for simultaneous cyber intrusions that could lead to cascading events and catastrophic power outages [5]. The authors propose an "integrated Anomaly Detection System" comprising both "host- and network-based anomaly detection systems for individual substations," as well as simultaneous anomaly detection for multiple substations [5]. Their research allowed them to implement network-based anomaly detection algorithms to identify malicious behaviours in substations using Generic Object Oriented Substation Event and Sampled Measured Value (SMV) [5].

Drawing parallels between the challenges faced by the power grid and those encountered by cybersecurity organizations like the CSE, this source underscores the need for innovative solutions. The emphasis on anomaly detection aligns with the proactive approach advocated for the changing landscape within sensitive sectors like the CSE. The implementation of anomaly detection algorithms similar to those proposed for power grid substations but tailored to monitor and analyze network traffic within the CSE's infrastructure using SMV can adapt network-based anomaly detection to identify unusual patterns in communication protocols and activities specific to the CSE's operations.

Abel Yeboua-Ofori and Charles Boachie from the School of Architecture, Computing and Engineering at the University of East London discuss the use of machine learning (ML) techniques to predict cyber attacks on the cyber supply chain (CSC) [6]. The authors highlight the vulnerability of CSC systems due to their integrated and distributed nature, making them susceptible to various types of malware attacks [6].

The authors introduce the use of "Logistic Regression…, Decision Tree…, and Support Vector Machine algorithms" to predict cyber attacks on CSC nodes [6]. The authors use a dataset from the "Microsoft Malware Prediction website" to train and test their ML models [6]. An ensemble approach, specifically Majority Voting (MV), is employed to "combine the predictions of the three algorithms" and improve overall accuracy [6]. The emphasis on using Predictive analytics and the implementation of machine learning in decision-making to determine if a threat is real or a "false alarm" in cyber security can be utilized in predicting and preventing cyber attacks within the CSE [6].

In Daron Acemoglu's essay on redesigning AI, he provides a comprehensive analysis of the economic, political, and social implications of artificial intelligence and automation. Acemoglu emphasizes the need for intentional "redirection of AI development," advocating for government policy, societal norms, and democratic oversight to shape the trajectory of AI in a way that benefits society [4]. One key argument centers on the potential negative impacts of the concentration of AI influence in major tech companies and the focus on automation at the expense of job creation.

Acemoglu's insights are particularly relevant to responsible and ethical applications of AI for cybersecurity within the CSE. By delving into his arguments, I can draw parallels between the broader societal implications of AI discussed in the essay and the specific considerations within cybersecurity. Acemoglu's emphasis on democratic oversight and the need for a measurement framework aligns with the ethical concerns in deploying AI for cybersecurity, where issues of privacy, transparency, and accountability are paramount in a government security organization. Furthermore, his call for international coordination echoes the global nature of cybersecurity threats, emphasizing the importance of collaborative efforts in developing ethical and responsible AI solutions that transcend geographical boundaries.

IV. Results and Discussion

The current situation within the Canadian Communications Security Establishment (CSE) provides valuable insights into the organization's cybersecurity landscape and lays the groundwork for implementing Anomaly Detection and Predictive Analytics.

A. Analysis of CSE Cyber Defense Systems

According to the Canadian Securities Establishment, significant funding has been allocated to bolster cybersecurity efforts, indicating a strong commitment to addressing evolving threats [7]. The budget of "$57.5 million over 5 years, starting in 2022 to 2023 and $12.8 million ongoing" from Budget 2022 underscores the importance placed on enhancing the resilience of critical government systems to cyber incidents [7].

The evolution of the Security Review Program, outlined in June 2022, reveals a proactive approach to mitigating cybersecurity risks [7]. The program's history of working with Canadian Telecommunications Service Providers since 2013, including reviews of products from designated suppliers such as Huawei and ZTE, demonstrates a commitment to scrutinizing and regulating the technology landscape [7]. Leveraging this program as a foundation, the integration of advanced technologies like anomaly detection and predictive analytics aligns seamlessly with the CSE's existing initiatives.

The use of sensors within the Cyber Centre is a critical aspect of the CSE's cybersecurity strategy. These sensors, including Host-based sensors, Cloud-based sensors, Network-based sensors, and Virtual network-based sensors, are tools for detecting malicious cyber activity. The sensors monitor patterns of network traffic, identifying attempts to deploy malware, map systems and networks, and extract information [8]. The automated defences, in conjunction with expert analysts, actively search for unusual flows in sensor data, allowing the CSE to thwart malicious activities promptly.

In the dynamic realm of cybersecurity, the CSE faces the challenge of defending against modern hacking systems that continually evolve to exploit vulnerabilities. These threats include “advanced persistent threats” that operate stealthily, “social engineering tactics targeting human vulnerabilities,” much like the Greek myth of Troy, the utilization of “zero-day exploits to exploit undiscovered software vulnerabilities,” supply chain attacks that compromise components before reaching the CSE, insider threats exploiting access privileges, evolving malware techniques such as “polymorphic and metamorphic malware,” and the “exploitation of encrypted traffic to conceal malicious activities” [9].

To fortify the CSE's cybersecurity defences, a proactive and adaptive approach is required to meet the evolving industry of malicious software.

B. Implementation of Anomaly Detection

The integration of anomaly detection and predictive analytics into the CSE's existing sensor infrastructure is feasible. Anomaly detection can complement the existing efforts by identifying deviations from normal network behaviour, signalling potential threats that might escape traditional rule-based detection. Predictive analytics, with its ability to forecast cyber threats based on historical data, can enhance the proactive nature of the CSE's defences.

Anomaly Detection operates by discerning deviations from the expected behaviour of a system, which can be formulated mathematically as follows:

$$Anomaly\ Score \ = \ P(Observation) \text{ [10].}$$

Here, $P(Observation)$ represents the probability of a given observation occurring. Anomalies are identified when this probability falls below a predefined threshold [10]. The integration of anomaly detection into the CSE's sensor infrastructure entails the continuous monitoring of network behaviour. Using statistical methods such as Gaussian Mixture Models[2] (GMM) (Figure 1), the system establishes a baseline of normal activities [11]. To implement the GMM we will first need to represent the probability densifity function:

$$p(x|\psi) \ = \ \sum_{i=1}^{M} w_i\, g(x|\mu_{i,}\ \Sigma_{\ i}) \text{ [11].}$$

$p(x|\psi)$ expresses the idea that the overall likelihood of observing the data point *x* is the weighted sum of the likelihoods under each individual Gaussian component. The weights w_i determine the contribution of each component, and $g(x|\mu_{i,}\ \Sigma_{\ i})$ gives the likelihood of *x* under the *i*-th Gaussian distribution. The sum is taken over all *M* components in the mixture.

The implementation of GMM wil require the Expectation-Maximization algorithm which involves iteratively updating the parameters (mean, covariance, and weights) of the mixture model based on the observed data [11].

For each data point in the training set, compute the likelihood of that point under the GMM by computing the probability density function for each component and combining them according to the GMM formula [11].

For anomaly detection using GMMs, the idea is to fit the GMM to the normal (non-anomalous) data and then use the model to

[2] A Gaussian Mixture Model is a probabilistic model that represents a mixture of multiple Gaussian distributions. It is a type of generative probabilistic model commonly used for clustering and density estimation tasks. It’s dataset is composed of several subpopulations, each of which is approximated by a Gaussian distribution.

identify anomalies based on how well they fit the learned distribution [11].

$$L(\Psi) = \prod_{i=1}^{n} f(x_i; \Psi)^3 \text{ [11].}$$

The anomaly score is then calculated for each new observation, allowing the system to flag deviations that might escape traditional rule-based detection [12].

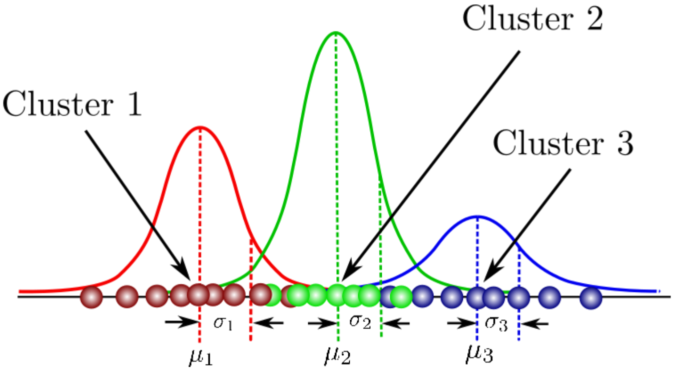

Fig 1, a visulization of Gaussian Mixture Models [11, Table 4]

C. Implementation of Predictive Analytics

Predictive analytics involves forecasting future events based on historical data patterns. In the context of cybersecurity, this can be expressed through the following equation:

$$Cyber\ Threat\ Forecast = f(Historical\ Data)$$

[10].

In this equation, f(Historical Data) represents the predictive function that learns from past cyber threat data to anticipate future threats. Machine learning algorithms such as “Time Series Analysis” or “Long Short-Term Memory” networks can be employed to discern temporal patterns in historical data and predict potential cyber threats [13]. By integrating predictive analytics into the CSE's infrastructure, the organization gains the ability to proactively identify and mitigate emerging threats before they can infiltrate the system.

The incorporation of these AI methodologies within the CSE would bring the subject government policy to the Canadian government and create democratic oversight to manage and bookkeep AI technologies under the insight of democratic policies through rules on sets of training data, sectors where AI and ML technologies can or cannot be implemented and the need for qualified people to implement, operate and maintain these systems.

V. Implications

The proposed AI-driven preventive measures are contingent on the assumption that the models, algorithms, and technologies employed will be effective in mitigating a wide range of cyber threats. The rapidly evolving nature of cyber threats poses a challenge, and the effectiveness of these AI applications may vary over time [5]. Additionally, the integration of AI raises concerns about privacy, transparency, and accountability, which must be addressed to ensure responsible AI usage within government cybersecurity organizations [4].

VI. Conclusion

The synergy between anomaly detection and predictive analytics lies in their collective power to enhance the CSE's situational awareness. Anomalies detected in real-time provide immediate alerts, while predictive analytics contributes to the strategic foresight needed to pre-emptively address evolving cyber threats. In a rapidly evolving industry of technology, malevolent uses of technology will drive the need for evolving changes of preventive technologies against cyber attacks, thus evolving and advancing the field in continuous research on data science and the specialized training on relevant data of cyber attacks within ML models which will help build a robust future for the CSE. The amalgamation of these techniques forms a robust foundation for the CSE's cybersecurity strategy, aligning with the organization's mission to protect Canada's digital infrastructure from a spectrum of cyber adversaries and bringing the subject of government policy to enforce AI to

[3] Expectation-Maximization algorithm

ensure the future development of AI aligns with Acemoglus mission [4].

References

[1] M. Burgess, “Hacking the hackers: Everything you need to know about shadow brokers’ attack on the NSA,” WIRED UK, https://www.wired.co.uk/article/nsa-hacking-tools-stolen-hackers.

[2] O. Solon, “Hacking group auctions ‘cyber weapons’ stolen from NSA,” The Guardian, https://www.theguardian.com/technology/2016/aug/16/shadow-brokers-hack-auction-nsa-malware-equation-group

[3] A. K. Agarwal, “Cybersecurity incidents in Canada increased by 160% year over year according to PWC Canada’s 2016 Global State of Information Security Survey,” PwC, https://www.pwc.com/ca/en/media/release/2016-1-13-cyber-security-in-canada.html.

[4] D. Acemoglu, "REDESIGNING AI," Boston Review, pp. 9-37,173, 2021. Available: https://proxy.lib.uwaterloo.ca/login?url=https://www.proquest.com/magazines/redesigning-ai/docview/2527608606/se-2.

[5] J. Hong, C. C. liu, and M. Govindarasu, “Integrated anomaly detection for cyber security of the ... - IEEE xplore,” IEEE Xplore, https://ieeexplore.ieee.org/document/6786500/

[6] A. Y. Ofori and C. Boachie, “IEEE Xplore | IEEE Journals & Magazine | IEEE Xplore,” IEEE Xplore, https://ieeexplore.ieee.org/abstract/document/7876843/

[7] Communications Security Establishment, “Communications security establishment annual report 2022-2023,” Communications Security Establishment, https://www.cse-cst.gc.ca/en/accountability/transparency/reports/communications-security-establishment-annual-report-2022-2023.

[8] Canadian Centre for Cyber Security, “Cyber threats to Canada’s democratic process,” Canadian Centre for Cyber Security, https://www.cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process

[9] N. K. Pandey, K. Kumar, G. Saini, and A. K. Mishra, “Security issues and challenges in cloud of things-based applications for industrial automation - annals of operations research,” SpringerLink, https://link.springer.com/article/10.1007/s10479-023-05285-7#:~:text=The%20major%20security%20challenges%20include,%2C%20and%20DoS%2FDDoS%20attack.

[10] I.H. Sarker, M.H. Furhad, and R. Nowrozy, "AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions," SN COMPUT. SCI., vol. 2, p. 173, Mar. 2021. [Online]. Available: https://doi.org/10.1007/s42979-021-00557-0.

[11] [1] C. C. Gomes, J. Boisvert, and C. V. Deutsch, Gaussianmixturemodels - geostatistics lessons, https://geostatisticslessons.com/pdfs/gmm.pdf.

[12] O. C. Carrasco, “Gaussian mixture models explained,” Medium, https://towardsdatascience.com/gaussian-mixture-models-explained-6986aaf5a95

[13] “Time series analysis: Definition, types, techniques, and when it’s used,” Tableau, https://www.tableau.com/learn/articles/time-series-analysis#:~:text=Time%20series%20analysis%20is%20a,data%20points%20intermittently%20or%20randomly.