COMP3703 - Homework 1

Jared Wood

January 12, 2026

Contents

Summary

"The Most Recent Advances and Uses of AI in Cybersecurity" focuses on the evolving field of cybersecurity threats and how AI is evolving to combat these. It largely focuses on a compare-and-contrast of traditional and modern cybersecurity methodologies and delving into surface-level concepts of how AI is being implemented to improve cybersecurity. The most notable, as one might expect, is the ability to ingest large amounts of data and make conclusions thus producing, flags, event reports, and/or simply completing general menial tasks (Things like paper pushing and file management). Towards this cause, there appears to be a distinct delineation between Machine Learning Algorithms and Deep Learning Networks. Besides atypical coded algorithms of Machine Learning to detect patterns in datasets, the most prominent techniques in Deep Learning according to the paper have to do with Natural Language Processing (NLP) to help summarize and ingest large amounts of textual data to accelerate security work-flow and Long Short-Term Memory (LSTM) primarily for Intrusion Detection Systems (IDS). However, due to the nature of requiring vast amounts of data, there is a concern ethically for arguments around intrusion of privacy, over-surveillance, and potential biases that are learned by the AI during the training process. It is noted that quantum computing is expected to completely change the field of cybersecurity once implemented.

Technical Insight

Two recurring topics in this research paper and AI are Machine Learning and Deep Learning. Both are an extension of the overall AI-framework, but Machine Learning seems to depend on supervised/unsupervised learning coupled with particular algorithms (Classification, Regression, Clustering, etc.) to identify patterns along with typical use-cases for a few; For example, clustering is a good Machine Learning type algorithm to detect things like anomalies and outliers within a dataset. Alternatively, Deep Learning focuses on layers like a Convolutional Neural Network (CNN) or a Recursion Neural Network (RNN) within a network that applies a multitude of algorithms to determine patterns (Input Layer, Hidden Layer, Output Layer). Generally, these techniques help expedite the security work-flow and pipeline for self-explanatory reasons.

Critical Evaluation

This paper excelled at compare-and-contrast methods and rarely deviated from this to better demonstrate the stark improvements that AI brings to the table in terms of cybersecurity. The paper also introduces key terminology or acronyms that I can only surmise are common vocabulary used by people like data scientists, data engineers, or any field that brushes with AI-concepts. Besides raw information gain, most things within the article felt fairly obvious or along the lines of what someone would expect typically from most things technology-wise. That is, the general acceleration of tasks and removing of menial and repetitive tasks to allow for skilled workers to focus on harder and more complex issues. I personally don't think there necessarily needs to be improvements because it is straight-and-to-the-point, thus allowing for information gain to occur sooner rather than later.

Application to Real-World Cybersecurity

Besides the obvious acceleration of work-flows, I think it'd be interesting to see AI applied effectively over the government's IC organization and chain-of-custody and/or used to corroborate intelligence reports to expedite overall intelligence operations and significantly improve the intelligence analysis' work-flow. Depending on the use-case, I can see this concept being applicable directly to cybersecurity or not at all. In a strict sense of safe-keeping digital assets, not so much. But in a more loose sense of needing to understand the capabilities of those who threaten our systems and dissemination of groups of pertinent information in order for operations to start sooner, I would argue yes.

Final Project Prep

I would prefer to work alone since I'm taking 5 classes (MATH3605, PHYS2300, JAPN1416, ASEM2539, COMP3703) and have other responsibilities at home, so collaboration with me might be difficult; Otherwise, I don't have any preference on who I work with, I'll figure it out.

Notes

The Most Recent Advances and Uses of AI in Cybersecurity

- Introduction
  - Cybersecurity threats have been increasing and AI can help counteract it largely due to its fast computing capability, ingest of large data, anomaly detection, etc.
  - Primary defenses of AI are real-time threat detection, automated incident response, predictive analytics, and vulnerability management
- Present Developments In AI-Powered Cybersecurity
  - Old detection systems relied on signature-specific encoding ahead of time
  - Many companies implement Security Information and Event Management (SIEM) Systems that use Machine Learning algorithms to analyze logs and spot anomalies in real time
  - Traditionally, Indicators of Compromise (IoCs) were used to detect threats, but failed to detect newer threats which is where AI excels at
- Machine Learning's Place In Cybersecurity
  - Some specific applications of Machine Learning are behavioral analytics, anomaly detection, threat intelligence, and automated response systems
- Using AI To Improve Cybersecurity
  - AI-driven security orchestration, automation, and response (SOAR) platforms helps automate routine and menial tasks to allow more free-time to harder issues for the worker
- Algorithms and AI Techniques In Cybersecurity
  - Deep learning is increasingly used for Intrusion Detection Systems (IDS) from its proven efficacy, particularly with Long Short-Term Memory (LSTM) networks
  - Natural Learning Processing (NLP) helps digest large amounts of text and summarizes them to accelerate seecurity work-flow
- Obstacles and Restrictions
  - Ethical concerns arise from AI learning from a potentially biased dataset and thereby biasing against particular groups. Additionally, privacy and surveillance concerns arise
  - Increased false positives run the risk of security personnel becoming desensitized to flags potentially ignoring serious threats
  - High quality data typically returns a high performing model, but to do so, usually requires time and investment to ensure high quality data is present

- AI's Future Prospects In Cybersecurity
  - Better algorithms of Machine Learning and explainable AI (AI that can make sensible explanations of its decisions) is a field being researched
  - Embedding an Internet of Things (IoT) is geared towards handling intricate networks
  - Quantum computing and general automation is expected to completely transform cybersecurity
- Analyses of AI Applications In Cybersecurity Case Studies
  - Generally just use-cases that regurgitate self-explanatory expectations of AI's current use in cybersecurity
- Conclusion
  - General reiteration of above talking points

Resources Used

- Hardware Used:
  - Macbook Laptop
- Software Used:
  - Overleaf (PDF editing)
- Resources:
  - COMP3703 Notes
  - Khan, Muhammad Ismaeel, et al. "The Most Recent Advances and Uses of AI in Cybersecurity." BULLET: Jurnal Multidisiplin Ilmu, vol. 3, no. 4, Aug. 2024, pp. 566–578.