Estimation and Hypothesis Testing

Brady Chin

Department of Accounting and Finance, Colorado State University Global

RES500: Fundamental of Quantitative Analysis

Dr. Mohammad Sumadi

April 28th, 2024

Estimation and Hypothesis Testing

In Critical Thinking Assignment 6, we are to find two researched-based articles on a business-related problem. We are to then identify the research problem and describe the authors' research design.

Business-Related Problem and Articles

A business-related problem that I am interested in is "What are the security risks of Generative Artificial Intelligence for businesses".

Generative AI is a subset of artificial intelligence that is used to generate new content. What make generative AI different compared to other subsets of artificial intelligence is that it is capable of creating new data based on the training data that is provided. This can be dangerous because hackers will be able to generate text, audio, and video recordings that may seem authentic, but are actually a ploy to gather sensitive information.

In the modern era, digital security has become extremely important on protecting businesses networks and data from being stolen by competitors, hackers, and even foreign threats. Although it can be used for good, Generative AI can be used to evade cybersecurity defenses by exploiting weaknesses in AI-based security systems to carry out successful cyber attacks.

Through CSU Global's online library, I have found two researched-based articles that are related to this problem. The first article, published in 2024, is titled *Security Risks Concerns of Generative AI in the IoT* written by Xu, Li, Balogun, Wu, Wang, and Cai. The second article is titled *Identifying and Mitigating the Security Risks of Generative AI*. This was written by Barrett, Boyd, Burzstein, Carlini, Chen, Choi, Chowdhury, Christodorescu, Datta, Feizi, Fisher, Hashimoto, Hendrycks, Jha, Kang, Kerschbaum, E. Mitchell, J. Mitchell, Ramzan, Shams, Song, Taly, and Yang and published in 2023.

Research Problem

In the article *Security Risks Concerns of Generative AI in the IoT,* the research problem that is explored is the security risks that emerges through the integration of generative AI in the IoT (Internet of Things). Although generative AI was created to drive innovation, it has been misused to threaten peoples privacy and used for data breaches in businesses. This article investigates the security risks of generative AI and provides strategies to mitigate these risks.

The article *Identifying and Mitigating the Security Risks of Generative AI* identifies how Generative AI can be used for both good and bad. The authors state that Generative AI has many benefits, including in-context learning, code-completion, and text-to-image generation and editing but can also be used to increase the effectiveness of cyber attacks.

Research-Design

The authors of *Security Risks Concerns of Generative AI in the IoT* use a comprehensive analysis to identify the security risks of generative AI. Section III of their paper provides details on data privacy and integrity, model security, security challenges, and malicious use of generative AI. The information that is provided in this section is to highlight key concerns with integrating AI and IoT to ensure that businesses have a full understanding of the risks that come with the deployment of these technologies.

To conduct research for the information in *Identifying and Mitigating the Security Risks of Generative AI,* a one-day workshop was conducted at Google on June 27th, 2023. This workshop was co-organized by Stanford University and the University of Wisconsin-Madison. In this workshop, a group of experts came together to talk about their work focusing on the following questions:

1. How could attackers leverage GenAI technologies?
2. How should security change in response to GenAI technologies?
3. What are some current and emerging technologies we should pay attention to for designing countermeasures?

With these three questions, the authors were able to generate this paper that defines the capabilities of generative AI, how attackers and defenders can leverage these capabilities, and the short and long-term goals of generative AI issues.

Conclusion

Generative AI was created to aid and enhance creative fields, create content, and help with problem-solving. Because generative AI is so powerful, it has been used for the wrong reasons and lead to security risks that businesses must address. By highlighting and understanding the misuse of generative AI, businesses are able to implement safeguards to counter potential cyber attacks.

References

Barnett, C., Boyd, B., Bursztein, E., Carlini, N., Chen, B., Choi, J., Chowdhury, A. R., Christodorescu, M., Datta, A., Feizi, S., Fisher, K., Hashimoto, T., Hendrycks, D., Jha, S., Kang, D., Kerschbaum, F., Mitchell, E., Mitchell, J., Ramzan, Z., … Yang, D. (2024). *Identifying and Mitigating the Security Risks of Generative AI*. https://arxiv.org/pdf/2308.14840

Xu, H., Li, Y., Balogun, O., Wu, S., Wang, Y., & Cai, Z. (2024). *Security Risks Concerns of Generative AI in the IoT*. https://arxiv.org/pdf/2404.00139