Week 1 Journal: Tools, Challenges, and Insights in Research

Amanul Islam

August 30, 2024

1 Goals for the Course

Figure 1: Amanul Islam

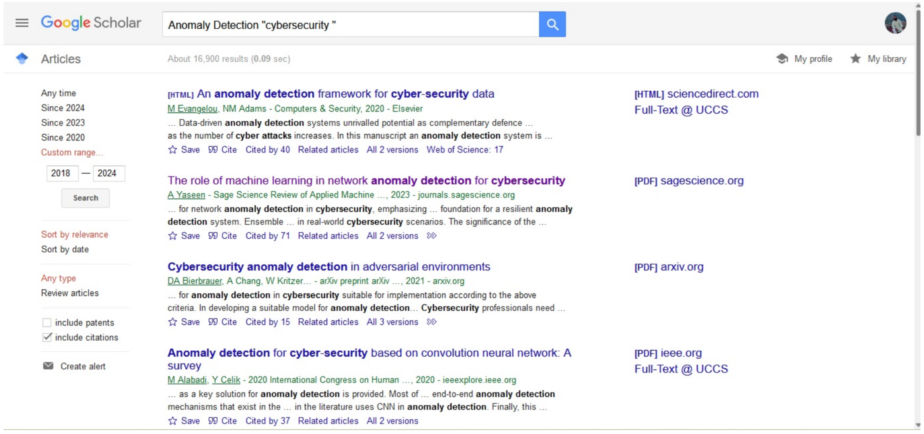
As a PhD candidate in Security under the guidance of Dr Sang-Yoon Chang, my primary goal in the "Computer Science Research - CS 6000" course is to deepen my understanding of advanced research methodologies and refine my ability to conduct impactful research in security. This course represents a pivotal opportunity to explore the latest trends, challenges, and innovations in cybersecurity, allowing me to develop a comprehensive framework for addressing complex issues in this domain. Through rigorous analysis and the application of various research techniques, I aim to contribute novel insights to the academic community while also developing practical solutions that can be applied in real-world scenarios.

In particular, I am eager to enhance my skills in identifying, analyzing, and solving complex security problems, focusing on areas such as adversarial attacks, secure system design, and the development of robust defence mechanisms. By the end of this course, I hope to have a well-rounded understanding of how to conduct high-quality research that not only advances theoretical knowledge but also has tangible impacts on the security landscape. My ultimate goal is to leverage this knowledge to produce a dissertation that is both academically rigorous and practically significant, contributing to the field of cybersecurity in meaningful ways.

Personally, I am married and the father of two energetic boys, both seven years old. Balancing family life with academic pursuits is both challenging and rewarding, and I find that travelling with my family during free time and vacations provides the perfect opportunity to relax and gain new perspectives. My journey from Bangladesh to my current PhD program represents not just a professional ambition but also a personal commitment to growth and learning.

2 Rationale for Selecting Papers

In this section, I presented the rationale behind selecting two specific research papers related to my area of interest in cybersecurity. Figure 2 and Figure 3 are examples of the rationale selection of the papers.



Anomaly Detection "cybersecurity "

About 16,900 results (**0.09** sec)

2018 — 2024

□ include patents
☑ include citations

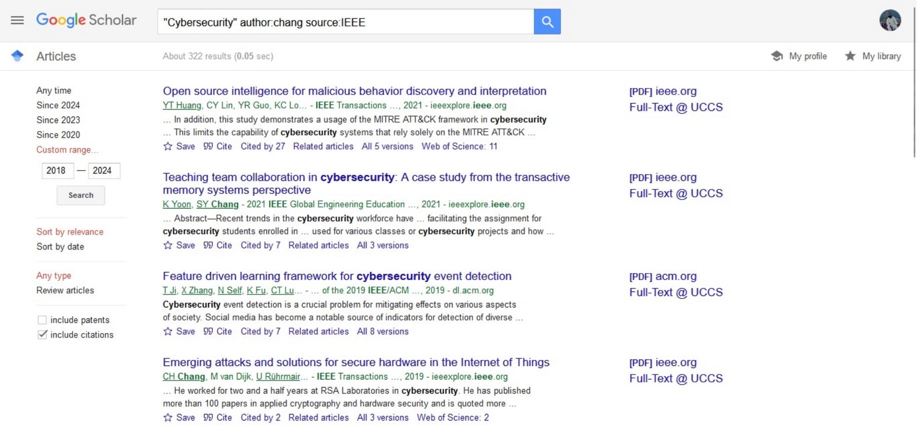
[HTML] An **anomaly detection** framework for **cyber-security** data
M Evangelou, NM Adams - Computers & Security, 2020 - Elsevier
... Data-driven **anomaly detection** systems unrivalled potential as complementary defence ...
as the number of **cyber attacks** increases. In this manuscript an **anomaly detection** system is ...
☆ Save 99 Cite Cited by 40 Related articles All 2 versions Web of Science: 17
[HTML] sciencedirect.com
Full-Text @ UCCS

The role of machine learning in network **anomaly detection** for **cybersecurity**
A Yaseen - Sage Science Review of Applied Machine ..., 2023 - journals.sagescience.org
... for network **anomaly detection** in **cybersecurity**, emphasizing ... foundation for a resilient **anomaly detection** system. Ensemble ... in real-world **cybersecurity** scenarios. The significance of the ...
☆ Save 99 Cite Cited by 71 Related articles All 2 versions
[PDF] sagescience.org

Cybersecurity anomaly detection in adversarial environments
DA Bierbrauer, A Chang, W Kritzer... - arXiv preprint arXiv ..., 2021 - arxiv.org
... for **anomaly detection** in **cybersecurity** suitable for implementation according to the above criteria. In developing a suitable model for **anomaly detection**... **Cybersecurity** professionals need ...
☆ Save 99 Cite Cited by 15 Related articles All 3 versions
[PDF] arxiv.org

Anomaly detection for **cyber-security** based on convolution neural network: A survey
M Alabadi, Y Celik - 2020 International Congress on Human ..., 2020 - ieeexplore.ieee.org
... as a key solution for **anomaly detection** is provided. Most of ... end-to-end **anomaly detection** mechanisms that exist in the ... in the literature uses CNN in **anomaly detection**. Finally, this ...
☆ Save 99 Cite Cited by 37 Related articles All 2 versions
[PDF] ieee.org
Full-Text @ UCCS

Figure 2: Figure 1: An overview of my search strategy on academic databases like Google Scholar. I used keywords such as ”Anomaly Detection” and ”cybersecurity” to identify papers that are highly cited and published in reputable journals.



"Cybersecurity" author:chang source:IEEE

About 322 results (**0.05** sec)

Any time
Since 2024
Since 2023
Since 2020
Custom range...

2018 — 2024

Search

Sort by relevance
Sort by date

Any type
Review articles

□ include patents
☑ include citations

Open source intelligence for malicious behavior discovery and interpretation
YT Huang, CY Lin, YR Guo, KC Lo... - **IEEE** Transactions ..., 2021 - ieeexplore.**ieee**.org
... In addition, this study demonstrates a usage of the MITRE ATT&CK framework in **cybersecurity** ... This limits the capability of **cybersecurity** systems that rely solely on the MITRE ATT&CK ...
☆ Save 99 Cite Cited by 27 Related articles All 5 versions Web of Science: 11
[PDF] ieee.org
Full-Text @ UCCS

Teaching team collaboration in **cybersecurity**: A case study from the transactive memory systems perspective
K Yoon, SY **Chang** - 2021 **IEEE** Global Engineering Education ..., 2021 - ieeexplore.**ieee**.org
... Abstract—Recent trends in the **cybersecurity** workforce have ... facilitating the assignment for **cybersecurity** students enrolled in ... used for various classes or **cybersecurity** projects and how ...
☆ Save 99 Cite Cited by 7 Related articles All 3 versions
[PDF] ieee.org
Full-Text @ UCCS

Feature driven learning framework for **cybersecurity** event detection
T Ji, X Zhang, N Self, K Fu, CT Lu... - ... of the 2019 **IEEE**/ACM ..., 2019 - dl.acm.org
Cybersecurity event detection is a crucial problem for mitigating effects on various aspects of society. Social media has become a notable source of indicators for detection of diverse ...
☆ Save 99 Cite Cited by 7 Related articles All 8 versions
[PDF] acm.org
Full-Text @ UCCS

Emerging attacks and solutions for secure hardware in the Internet of Things
CH **Chang**, M van Dijk, U Rührmair... - **IEEE** Transactions ..., 2019 - ieeexplore.**ieee**.org
... He worked for two and a half years at RSA Laboratories in **cybersecurity**. He has published more than 100 papers in applied cryptography and hardware security and is quoted more ...
☆ Save 99 Cite Cited by 2 Related articles All 3 versions Web of Science: 2
[PDF] ieee.org
Full-Text @ UCCS

Figure 3: The provided image shows the advanced search I used to search my research-related papers including cybersecurity and privacy with custom dates and other options on this page.

3 Related Research Papers

Below is a list of 25 research papers that are related to my area of interest in cybersecurity, particularly focusing on adversarial attacks, secure system design, and defense mechanisms.

3.1 Adversarial Attacks and Defenses

1. Xu, H., Ma, Y., Liu, H. C., Deb, D., Liu, H., Tang, J. L., & Jain, A. K. (2020). Adversarial attacks and defenses in images, graphs and text: A review. *International Journal of Automation and Computing*, *17*, 151-178.

2. Akhtar, N., Mian, A., Kardan, N., & Shah, M. (2021). Advances in adversarial attacks and defenses in computer vision: A survey. *IEEE Access*, *9*, 155161-155196.

3. Ren, K., Zheng, T., Qin, Z., & Liu, X. (2020). Adversarial attacks and defenses in deep learning. *Engineering*, *6*(3), 346-360.

4. Liu, N., Du, M., Guo, R., Liu, H., & Hu, X. (2021). Adversarial attacks and defenses: An interpretation perspective. *ACM SIGKDD Explorations Newsletter*, *23*(1), 86-99.

5. Zhou, S., Liu, C., Ye, D., Zhu, T., Zhou, W., & Yu, P. S. (2022). Adversarial attacks and defenses in deep learning: From a perspective of cybersecurity. *ACM Computing Surveys*, *55*(8), 1-39.

3.2 Secure System Design

1. Fernandez, E. B., Yoshioka, N., Washizaki, H., & Yoder, J. (2022). Abstract security patterns and the design of secure systems. *Cybersecurity*, *5*(1), 7.

2. Ooi, S. E., Beuran, R., Tan, Y., Kuroda, T., Kuwahara, T., & Fujita, N. (2022, April). Secureweaver: Intent-driven secure system designer. In *Proceedings of the 2022 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems* (pp. 107-116).

3. Huang, Y., Chen, J., Huang, L., & Zhu, Q. (2020). Dynamic games for secure and resilient control system design. *National Science Review*, *7*(7), 1125-1141.

4. Mun, H., Han, K., & Lee, D. H. (2020). Ensuring safety and security in CAN-based automotive embedded systems: A combination of design optimization and secure communication. *IEEE Transactions on Vehicular Technology*, *69*(7), 7078-7091.

5. Cheng, X., Chen, F., Xie, D., Sun, H., & Huang, C. (2020). Design of a secure medical data sharing scheme based on blockchain. *Journal of Medical Systems*, *44*(2), 52.

3.3 Cybersecurity Defenses

1. Zhou, S., Liu, C., Ye, D., Zhu, T., Zhou, W., & Yu, P. S. (2022). Adversarial attacks and defenses in deep learning: From a perspective of cybersecurity. *ACM Computing Surveys*, *55*(8), 1-39.

2. Sun, N., Ding, M., Jiang, J., Xu, W., Mo, X., Tai, Y., & Zhang, J. (2023). Cyber threat intelligence mining for proactive cybersecurity defense: A survey and new perspectives. *IEEE Communications Surveys & Tutorials*, *25*(3), 1748-1774.

3. Jimmy, F. (2021). Emerging threats: The latest cybersecurity risks and the role of artificial intelligence in enhancing cybersecurity defenses. *Valley International Journal Digital Library*, 564-574.

4. Zheng, Y., Li, Z., Xu, X., & Zhao, Q. (2022). Dynamic defenses in cyber security: Techniques, methods and challenges. *Digital Communications and Networks*, *8*(4), 422-435.

5. Okoli, U. I., Obi, O. C., Adewusi, A. O., & Abrahams, T. O. (2024). Machine learning in cybersecurity: A review of threat detection and defense mechanisms. *World Journal of Advanced Research and Reviews*, *21*(1), 2286-2295.

3.4 Network Security

1. Zhao, J., Masood, R., & Seneviratne, S. (2021). A review of computer vision methods in network security. *IEEE Communications Surveys & Tutorials*, *23*(3), 1838-1878.

2. Sengupta, S., Chowdhary, A., Sabur, A., Alshamrani, A., Huang, D., & Kambhampati, S. (2020). A survey of moving target defenses for network security. *IEEE Communications Surveys & Tutorials*, *22*(3), 1909-1941.

3. Arogundade, O. R. (2023). Network security concepts, dangers, and defense best practical. *Computer Engineering and Intelligent Systems*, *14*(2).

4. Bansal, B., Jenipher, V. N., Jain, R., Dilip, R., Kumbhkar, M., Pramanik, S., ... & Gupta, A. (2022). Big data architecture for network security. *Cyber Security and Network Security*, 233-267.

5. Jacobs, A. S., Beltiukov, R., Willinger, W., Ferreira, R. A., Gupta, A., & Granville, L. Z. (2022, November). AI/ML for network security: The emperor has no clothes. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1537-1551).

3.5 Privacy and Data Security

1. Yang, P., Xiong, N., & Ren, J. (2020). Data security and privacy protection for cloud storage: A survey. *IEEE Access*, *8*, 131723-131740.

2. Thantilage, R. D., Le-Khac, N. A., & Kechadi, M. T. (2023). Healthcare data security and privacy in Data Warehouse architectures. *Informatics in Medicine Unlocked*, *39*, 101270.

3. Thapa, C., & Camtepe, S. (2021). Precision health data: Requirements, challenges and existing techniques for data security and privacy. *Computers in Biology and Medicine*, *129*, 104130.

4. Yigzaw, K. Y., Olabarriaga, S. D., Michalas, A., Marco-Ruiz, L., Hillen, C., Verginadis, Y., ... & Chomutare, T. (2022). Health data security and privacy: Challenges and solutions for the future. *Roadmap to Successful Digital Health Ecosystems*, 335-362.

5. Farayola, O. A., Olorunfemi, O. L., & Shoetan, P. O. (2024). Data privacy and security in IT: A review of techniques and challenges. *Computer Science & IT Research Journal*, *5*(3), 606-615.

4 Tools Used

In my research, I utilized a variety of tools to streamline the process of searching for, managing, and analyzing research papers. These tools played a crucial role in efficiently handling the vast amount of information and data I encountered.

I relied on well-established research databases like **IEEE Xplore**, **ACM Digital Library**, and **Google Scholar**, which provided access to a vast repository of peer-reviewed journal articles, conference papers, and other scholarly publications. I used keywords such as “adversarial attacks,” “cybersecurity defences,” “secure system design,” and “network security” to search for relevant literature.

To manage the references effectively, I used **Zotero**, a reference management software that allowed me to organize citations, generate bibliographies, and store research papers systematically. Zotero’s integration with LaTeX via `bibtex` was particularly useful for seamlessly incorporating citations into my document.

For document preparation, I used **LaTeX**, which provided a powerful and flexible environment to create well-structured academic documents. I chose LaTeX due to its ability to handle complex formatting requirements, particularly when dealing with mathematical equations, tables, and references. The `Overleaf` platform was used to collaborate and compile the LaTeX document online.

One of the primary challenges I faced was narrowing down the vast amount of available research to identify the most relevant papers. The initial search results were often overwhelming, with hundreds of papers to sift through. To overcome this, I refined my search queries following the class and video by using more specific keywords and applying filters such as publication date and citation count. An important insight from this week’s exercises was maintaining a critical mindset when approaching any research topic.