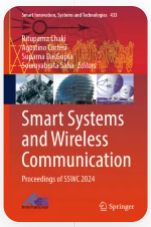
Graph-Based Approaches in Cybersecurity: A Comprehensive Survey

| Conference paper | First Online: 18 April 2025

| pp 465–477 | Cite this conference paper



Smart Systems and Wireless Communication

(SSWC 2024)

Uttaran Ghosh, Aditya Paul, Darothi Sarkar, Monalisa Dey & Prithwineel Paul

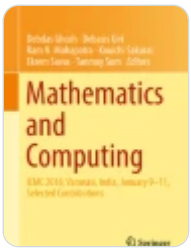
Part of the book series: Smart Innovation, Systems and Technologies ((SIST,volume 433))

Included in the following conference series:
International Conference on Smart Systems and Wireless Communication

Abstract

For the ever-expanding threat cybersecurity needs some advanced methodologies for threat detection, vulnerability, assessment, and incident response. This comprehensive survey

paper explores the pervasive role of graph-based approaches in fortifying cybersecurity measures. The survey begins with navigations through the landscape of intrusion detection systems (IDSs) that leverage algorithms like PageRank. The paper elucidates how threat intelligence graphs enhance the understanding of cyber threats by modeling relationships between threat indicators. Furthermore, the survey investigates the vital role of Graph-Based Approaches in Cybersecurity assessment. It examines attack surface analysis and dependency mapping, elucidating how these techniques prioritize security efforts by identifying critical entry points and assessing the impact of potential vulnerabilities. The integration of blockchain technology with graph theory is discussed. The survey paper also explores real-world applications, comparative studies, and the challenges faced in deploying graph-based cybersecurity approaches at scale. In summary, this survey paper offers a panoramic view of the graph-based approaches employed in cybersecurity. It illuminates the strengths, limitations, and real-world implications of these methodologies, providing a valuable resource for cybersecurity practitioners, researchers, and policymakers navigating the complex and dynamic landscape of securing digital ecosystems.



Cybersecurity: A Survey of Vulnerability Analysis and Attack Graphs

Chapter | © 2018

PR-DRA: PageRank-based defense resource allocation methods for securing interdepende...

Article | 23 December 2024

Efficient Post Event Analysis and Cyber Incident Response in IoT and E-commerce...

Chapter | © 2022

References

1. Islam, R., Refat, R.U.D., Yerram, S.M., Malik, H.: Graph-based intrusion detection system for controller area networks. IEEE Trans. Intell. Transp. Syst. **23**(3), 1727–1736 (2020)

Article Google Scholar

2. Easttom, C.: On the application of algebraic graph theory to modeling network intrusions (2020)

Google Scholar

3. Gümüşbaş, D., Yıldırım, T., Genovese, A., Scotti, F.: A comprehensive survey of databases and deep learning methods for cybersecurity and intrusion detection systems. IEEE Syst. J. **15**(2), 1717–1731 (2020)

Article Google Scholar

4. Deepa, A.J., Kavitha, V.: A comprehensive survey on approaches to intrusion detection system (2012)

Google Scholar

5. Piplai, A., Mittal, S., Joshi, A., Finin, T., Holt, J., Zak, R.: Creating cybersecurity knowledge graphs from malware after action reports. IEEE Access **8**, 211691–211703 (2020)

Article Google Scholar

6. Böhm, F., Menges, F., Pernul, G.: Graph-based visual analytics for cyber threat intelligence. Cybersecurity **1**(1), 16 (2018)

Article Google Scholar

7. Mittal, S., Joshi, A., Finin, T.: Cyber-all-intel: an AI for security related threat intelligence (2019)

Google Scholar

8. Sarhan, I., Spruit, M.: Open-CyKG: an open cyber threat intelligence knowledge graph. Knowledge-Based Syst. **233**, 107524 (2021)

Article Google Scholar

9. Ghirardello, K., Maple, C., Ng, D., Kearney, P.: Cyber security of smart homes: development of a reference architecture for attack surface analysis (2018)

Google Scholar

10. Shandilya, V., Simmons, C.B., Shiva, S.: Use of attack graphs in security systems. J. Comput. Netw. Commun. **2014**(1), 818957 (2014)

Google Scholar

11. Phillips, C., Swiler, L.P.: A graph based system for network-vulnerability analysis (1998)

Google Scholar

12. Akbarzadeh, A., Katsikas, S.K.: Dependency-based security risk assessment for cyber-physical systems (2022)

Google Scholar

13. Taylor, P.J., Dargahi, T., Dehghantanha, A., Parizi, R.M., Choo, K.K.R.: A systematic literature review of blockchain cyber security. Digital Commun. Netw. **6**(2), 147–156 (2020)

Article Google Scholar

14. Zhuang, P., Zamir, T., Liang, H.: Blockchain for cybersecurity in smart grid: a comprehensive survey. IEEE Trans. Indus. Inform. **17**(1), 3–19 (2020)

Article Google Scholar

15. Stergiopoulos, G., Dedousis, P., Gritzalis, D.: Automatic network restructuring and risk mitigation through business process asset dependency analysis. Comput. Secur. **96**, 101869 (2020)

Article Google Scholar

16. Wei, R., Cai, L., Zhao, L., Yu, A., Meng, D.: Deephunter: a graph neural network based approach for robust cyber threat hunting (2021)

Google Scholar

17. Eberle, W., Graves, J., Holder, L.: Insider threat detection using a graph-based approach. J. Appl. Secur. Res. **6**(1), 32–81 (2010)

Article Google Scholar

18. Raharjo, D. H. K., Salman, M.: Anomaly detection analysis with graph-based cyber threat hunting scheme. KINETIK **8**(4) (2023)

Google Scholar

19. Zhang, Z., Li, Y., Dong, H., Gao, H., Jin, Y., Wang, W.: Spectral-based directed graph network for malware detection. IEEE Trans. Netw. Sci. Eng. **8**(2), 957–970 (2020)

Article Google Scholar

20. Sahu, M.K., Ahirwar, M., Shukla, P.K.: Improved malware detection technique using ensemble based classifier and graph theory. IEEE (2015)

Google Scholar

21. Xiao, F., Lin, Z., Sun, Y., Ma, Y.: Malware detection based on deep learning of behavior graphs. Math. Probl. Eng. **2019**(1), 8195395 (2019)

Article Google Scholar

Author information

Authors and Affiliations

Institute of Engineering and Management, University of Engineering and Management, Kolkata, India

Uttaran Ghosh, Aditya Paul, Darothi Sarkar, Monalisa Dey & Prithwineel Paul

Corresponding author

Correspondence to Uttaran Ghosh .

Editor information

Editors and Affiliations

School of Information Technology, University of Calcutta, Kolkata, West Bengal, India

Rituparna Chaki

DAIS, Ca' Foscari University, Venezia, Italy

Agostino Cortesi

Department of Information Technology, JIS College of Engineering, West Bengal, West Bengal, India

Suparna DasGupta

Department of Information Technology, JIS College of Engineering, Kalyani, West Bengal, India

Soumyabrata Saha

Rights and permissions

Copyright information

About this paper

Cite this paper

Ghosh, U., Paul, A., Sarkar, D., Dey, M., Paul, P. (2025). Graph-Based Approaches in Cybersecurity: A Comprehensive Survey. In: Chaki, R., Cortesi, A., DasGupta, S., Saha, S. (eds) Smart Systems and Wireless Communication. SSWC 2024. Smart Innovation, Systems and Technologies, vol 433. Springer, Singapore. https://doi.org/10.1007/978-981-96-1348-9_35

.RIS .ENW .BIB

DOI	Published	Publisher Name
https://doi.org/10.1007/978-981-96-1348-9_35	18 April 2025	Springer, Singapore

Print ISBN	Online ISBN	eBook Packages
978-981-96-1347-2	978-981-96-1348-9	Engineering Engineering (R0)

Publish with us

Policies and ethics