ICRAMCS 2026

THE EIGHTHEDITION OF THE INTERNATIONAL CONFERENCE ON RESEARCH IN APPLIED MATHEMATICS AND COMPUTER SCIENCE
April23-24-25, 2026 | Marrakech, Morocco

A Hybrid Neuro-Ontological Framework for Explainable Cyberattack Detection: Integrating Machine Learning and Semantic Reasoning

Communication Info

Authors:
First name LAST NAME[1]
Akram Bourichi[1]
[0009−0001−8432−6301]
Khalid Chougdali[1]

[1]*National School of Applied Sciences, Ibn Tofail University, Kenitra, Morocco*
{akram.bourichi, khalid.chougdali}@uit.ac.ma
http://www.uit.ac.ma

Keywords:
(1) Explainable AI
(2) Cybersecurity
(3) MITRE ATT&CK
(4) Hybrid Intelligence
(5) Intrusion Detection

Abstract

There is an urgent need for transparent and comprehensible detection systems due to the growing opacity of machine learning models in security operations centers (SOCs). In order to convert "black-box" machine learning detections into threat intelligence that can be understood by humans, this study presents a preliminary version of the NOHI (Neuro-Ontological Hybrid Intelligence) framework. Our method combines a formal cybersecurity knowledge base with a Random Forest classifier in a synergistic manner. The systematic alignment of detection outputs with the MITRE ATT&CK framework is a significant contribution of this work [1]. The system gives analysts instant operational context by mapping statistical anomalies to standardized tactics and techniques (e.g., T1498.001 for DDoS attacks). Validation was performed using 5,000 network traffic samples from a controlled dataset [2]. In addition to producing detailed risk assessments and practical mitigation strategies, preliminary results show an impressive detection accuracy of 98.1% [3]. Our hybrid architecture guarantees logical traceability by basing decisions on well-established domain knowledge [4], building upon our previous work on neuro-ontological hybrid frameworks [5]. This study lays the groundwork for future improvements in real-time computational efficiency by confirming the architectural viability of reliable AI in cybersecurity.

References

[1] Strom, B.E., Applebaum, A., Miller, D.P., Nickels, K.C., Pennington, A.G., Thomas, C.B.: MITRE ATT&CK: Design and Philosophy. Technical Report, The MITRE Corporation (2018)
[2] Lundberg, S.M., Lee, S.I.: A unified approach to interpreting model predictions. In: Proceedings of the 31st International Conference on Neural Information Processing Systems (NIPS), pp. 4768–4777. Curran Associates, Red Hook (2017)
[3] Undercoffer, J., Joshi, A., Pinkston, J.: Modeling computer attacks: An ontology for intrusion detection. In: Vigna, G., Jonsson, E., Krügel, C. (eds.) Recent Advances in Intrusion Detection (RAID 2003). Lecture Notes in Computer Science, vol. 2820, pp. 113–135. Springer, Berlin (2003)
[4] Obrst, L., Chase, P., Markeloff, R.: Developing an ontology of the cyber security domain. In: Proceedings of the 7th International Conference on Semantic Technologies for Intelligence, Defense, and Security (STIDS), pp. 54–61. CEUR-WS.org, Aachen (2012)
[5] Bourichi, A., Chougdali, K.: Neuro-Ontological Hybrid Framework for Threat Detection. In: Proceedings of the International Conference on Advanced Science and Engineering Technologies (ICASET 2026), Springer (to appear)