ICS project description and requirements

Dr. Alexandru ARCHIP

academic year 2025 - 2026

1 Topics

The ICS project encourages students to dive into analysing concrete defensive and offensive scenarios, and to develop original ideas for how applications of Artificial Intelligence/Machine Learnig (AI/ML) could enhance either use case. Apruzzese *et al.*'s 2023 review [1] offers a broad overview of existing approaches and may serve as a useful starting point. Students are, however, encouraged to look beyond established methods and explore novel directions inspired by, but not limited to, the ideas surveyed in this work.

1.1 Sample topics

Attack mitigation ML/AI techniques:

Attack type	code/command injection in public-facing applications (e.g. web applications);
Input data	values for different parameters that include both normal and attack patterns;
	sample datasets are available in [2];
Problem type	classification problem (either binary or multiclass, depending on the attack type and classification technique);
Result	trained model that detects potential threats;
	recall should be at least 95%;

Attack enhancing techniques:

Target attack	code/command injection;
Input data	existing attack patterns, grouped into successful and unsuccessful patterns;
Problem type	language processing problem;
	example study: DeepSQLi [3];
Result	an enhanced set of attack patterns for the chosen code/command injection attack.

AI/ML-based techniques enhancing classic N/HIDPS:

Input data	known firewall and firewall-like applications (e.g. Snort [4] and Suricata [5]);
	threat intelligence data (such as MITRE ATT&CK [6] and OWASP [7]);
Problem type	language processing and pattern matching;
Result	inference model able to update signature-based rules of firewalls and firewall-like applications.

Students are encouraged to study the chosen attacks in simulated scenarios using virtualised environments. Easily accessible tools include Oracle VirtualBox [8] and Kali Linux [9]. The purpose of this study is to gain valuable insights into actual attacks and attack techniques, the weaknesses and vulnerabilities that enable attacks to succeed, and the features that contribute to the effectiveness of AI/ML-based mitigation techniques.

2 Requirements

1. Students are expected to provide the following materials for the practical demonstrative application:
   (a) the dataset used to train the AI/ML module;
   (b) the source code and any required dependencies;
   (c) the obtained results.
2. Each project must include a theoretical report, no longer than four pages, describing:
   (a) the selected features and an assessment of their suitability for the project's objective;
   (b) the chosen AI/ML technique and the rationale for this choice;
   (c) evidence supporting the correctness of the results.
3. Students are encouraged to work in teams of up to three persons. Teams must be established by the end of week nine and are considered final after this deadline. Each team member should have a clearly defined role, and their contribution must be explicitly stated in the final report.
4. While following these requirements, students are encouraged to explore novel approaches, challenge conventional methods, and consider creative applications of AI/ML to both offensive and defensive scenarios.

References

[1] Giovanni Apruzzese, Pavel Laskov, Edgardo Montes de Oca, Wissam Mallouli, Luis Brdalo Rapa, Athanasios Vasileios Grammatopoulos, and Fabio Di Franco. The role of machine learning in cybersecurity. *Digital Threats*, 4(1), March 2023.

[2] Kaggle LLC. Kaggle: Your home for data-science competitions. https://www.kaggle.com, 2025. Accessed: 2025-11-17.

[3] Muyang Liu, Ke Li, and Tao Chen. Deepsqli: deep semantic learning for testing sql injection. In *Proceedings of the 29th ACM SIGSOFT International Symposium on Software Testing and Analysis*, ISSTA 2020, pages 286–297, New York, NY, USA, 2020. Association for Computing Machinery.

[4] Cisco Systems. Snort – network intrusion detection & prevention system. https://www.snort.org. Accessed: 2025-11-20.

[5] Open Information Security Foundation (OISF). Suricata — high-performance ids / ips / nsm engine. https://suricata.io. Accessed: 2025-11-20.

[6] MITRE Corporation. Mitre att&ck® knowledge base. https://attack.mitre.org. Accessed: 2025-11-20.

[7] OWASP Foundation. Owasp — open web application security project. https://owasp.org. Accessed: 2025-11-20.

[8] Oracle Corporation. Virtualbox. https://www.virtualbox.org. Accessed: 2025-11-20.

[9] Offensive Security. Kali linux. https://www.kali.org. Accessed: 2025-11-20.