| | |
|---|---|
| **Department** | School of Computing |
| **Supervisors** | Director of Studies: Dr. Christos Chrysoulas, Second Supervisor: Dr. Nikolaos Pitropakis |
| | |
| | |
| **Project Title** | Applied Machine Learning And Cybersecurity |

**PROJECT DESCRIPTION**

Today, it's impossible to deploy effective cybersecurity defence layers without relying heavily on machine learning.

There are several reasons why machine learning considered so crucial to cybersecurity. With machine learning, cybersecurity systems are in position to analyse patterns and learn from them - to efficiently help them preventing similar attacks and responding to changing behaviour. It this way, machine learning can help cybersecurity teams be more proactive in preventing threats and responding to active attacks in real time. On top of that, machine learning can reduce the amount of time spent on routine tasks and enable organizations to use their resources more efficiently.

Machine learning can make threat detection and mitigation simpler, more proactive, less expensive and far more effective. This is only feasible if the underlying data that supports the machine learning provides the complete picture of the environment. We must always have in mind that is not just about the quantity of data, but the quality of data we should focus on. The data must have complete, relevant and rich context collected from every potential source—whether that is at the endpoint, on the network or in the cloud. Additionally, we should never forget that adversaries in the arms race with defenders, always employ new solutions to attack the machine learning models. The latter activities that have manifested during the past five (5) years, demand from the research community robust algorithms against adversarial examples.

In short, the combination of machine learning and cybersecurity can be the cornerstone on which we can built robust and efficient systems.

PhD candidates would be expected to work on challenges/topics such as: Advanced Machine Learning, Adversarial Machine Learning, Threat Detection, Critical System Protection, Big Data Analytics and so on.

Prospective applicants are encouraged to contact the Supervisor before submitting their applications. Applications should make it clear the project you are applying for and the name of the supervisor(s).

**Academic qualifications**

A first degree (at least a 2.1) ideally in ideally in Computer Science or Electrical and Computer Engineering with a good fundamental knowledge of of Machine Learning, Basic Security algorithms and programming (eg. Python). An inquisitive and analytical mind, self-motivation and the ability to work independently, are considered essential.

**English language requirement**

IELTS score must be at least 6.5 (with not less than 6.0 in each of the four components). Other, equivalent qualifications will be accepted. Full details of the University's policy are available online.

**Essential attributes:**

- Experience of fundamental Machine Learning and/or Cybersecurity techniques.
- Competent in applying Machine Learning and Cybersecurity toolkits.
- Knowledge of Machine Learning and/or Cybersecurity theory.

- Good written and oral communication skills

- Good time management
- Strong motivation, with evidence of independent research skills relevant to the project

**Desirable attributes:**

- A master's degree with courses on Machine Learning, and/or Security/Cybersecurity.
- Background in machine learning (deep feed-forward neural networks, deep recurrent neural networks, deep convolutional neural networks, etc.).
- Background in cybersecurity (secure multi-party computation, homomorphic encryption, authentication, etc.).
- Background in stochastic modeling (Markov chains, Graph Probabilistic Models, etc.).
- Publication record in academic conferences and journals.

| | |
|---|---|
| **Indicative Bibliography** | A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," in IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153-1176, Secondquarter 2016, doi: 10.1109/COMST.2015.2494502.<br>B. G. Apruzzese, M. Colajanni, L. Ferretti, A. Guido and M. Marchetti, "On the effectiveness of machine and deep learning for cyber security," 2018 10th International Conference on Cyber Conflict (CyCon), Tallinn, 2018, pp. 371-390, doi: 10.23919/CYCON.2018.8405026.<br>C. Pitropakis, N., Panaousis, E., Giannetsos, T., Anastasiadis, E., & Loukas, G. (2019). A taxonomy and survey of attacks against machine learning. Computer Science Review, 34, 100199. |
| | |
| **Enquiries** | For informal enquiries about this PhD project, please contact c.chrysoulas@napier.ac.uk |
| **Web page** | https://www.napier.ac.uk/research-and-innovation/research-degrees/application-process |