School of Computing, Engineering, and the Built Environment
Edinburgh Napier University

PHD STUDENT PROJECT

Funding and application details

Funding status: Self funded students only

Application instructions:
Detailed instructions are available at https://blogs.napier.ac.uk/scebe-research/available-phd-student-projects/

Prospective candidates are encouraged to contact the Director of Studies (see details below) to discuss the project and their suitability for it.

Project details

Supervisory Team:

- DIRECTOR OF STUDY: Pavlos Papadopoulos (Email: P.Papadopoulos@napier.ac.uk)
- 2ND SUPERVISOR: Nikolaos Pitropakis

Subject Group: Cyber-security and system engineering

Research Areas: Computer Science: Cyber Security or Other

Project Title: Privacy-preserving Systems around Security, Trust and Identity

Project description:

Blockpass and the School of Computing at Edinburgh Napier University have set up an advanced Blockchain Identity Lab (BIL), which aims to support world-leading research related to cryptography, blockchain, distributed ledger technologies, privacy-preserving machine learning, and their linkage to sovereign identities such as decentralised identities and verifiable credentials. It currently supports several PhD studentships, and due to the successful commercialisation of its work, it aims to increase this number. Successful applicants in this role will investigate, but are not limited to, a wide range of areas related to security, privacy, identity, trust/consent/delegation, and secure software development processes. A key

focus will be on privacy-preserving methods, trusted smart contracts, anonymised machine learning, and the integration of trust, governance and consent around distributed models.

References:

[1] Bernabe, J. B., Canovas, J. L., Hernandez-Ramos, J. L., Moreno, R. T., & Skarmeta, A. (2019). Privacy-preserving solutions for blockchain: Review and challenges. IEEE Access, 7, 164908-164940.

[2] Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., ... & Yellick, J. (2018, April). Hyperledger fabric: a distributed operating system for permissioned blockchains. In Proceedings of the thirteenth EuroSys conference (pp. 1-15).

[3] Yin, X., Zhu, Y., & Hu, J. (2021). A comprehensive survey of privacy-preserving federated learning: A taxonomy, review, and future directions. ACM Computing Surveys (CSUR), 54(6), 1-36.

[4] Mohammed, N. M., Niazi, M., Alshayeb, M., & Mahmood, S. (2017). Exploring software security approaches in software development lifecycle: A systematic mapping study. Computer Standards & Interfaces, 50, 107-115.

[5] Corallo, A., Lazoi, M., & Lezzi, M. (2020). Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. Computers in industry, 114, 103165.

[6] Kurakin, A., Goodfellow, I. J., & Bengio, S. (2018). Adversarial examples in the physical world. In Artificial intelligence safety and security (pp. 99-112). Chapman and Hall/CRC.

Candidate characteristics

Education:

A first-class honours degree, or a distinction at master level, or equivalent achievements in Computer Science with a good fundamental knowledge of computer science and computer security.

Subject knowledge:

Essential attributes:

- Essential attributes
- Experience of fundamental computer science areas, including a background in computer security
- Competent in programming and software testing
- Knowledge of computer security methods, including the fundamentals of cryptography
- Good written and oral communication skills
- Strong motivation, with evidence of independent research skills relevant to the project
- Good time management

Desirable attributes:

- Desirable attributes
- A strong desire to build trusted architectures, which integrate privacy and trust.