AI-CyberSec 2021

Workshop Proceedings

Selected Papers from the AI-CyberSec 2021 Workshop in the 41st SGAI International Conference on Artificial Intelligence

14 December 2021

Sadiq Sani | Harsha Kalutarage

AI-CyberSec 2021- 1st International Workshop on Artificial Intelligence and Cyber Security

Artificial intelligence (AI) is currently driving transformations in many fields, and cybersecurity is no exception. With recent advances in AI, security practitioners have applied AI to improve the security posture of networks, systems, and devices with significant success. However, along with the benefits of AI, new concerns are emerging; including safety & ethics, privacy & data protection, and data quality and adversarial attacks that exploit the vulnerabilities of AI systems. In addition, AI can be used to create more sophisticated attacks triggering an AI arms race between defenders and attackers. In order to effectively use AI for cybersecurity and to address these challenges, novel ideas and effective approaches must be explored.

This volume consists of the papers that were presented at the 1st International Workshop on Artificial Intelligence and Cyber Security[1], co-located with the 41st SGAI International Conference on Artificial Intelligence (AI-2021) on December 14th, 2021. The workshop focused on three research areas that intersect with AI and Security:

1. **AI for cybersecurity** - studies that cover effective use of AI techniques to improve the security of systems and networks
2. **Malicious use of AI** - studies that cover how advances in AI lead to new types of threats, expanding the existing threat landscape
3. **Cybersecurity for AI** - studies that cover vulnerabilities of AI-enabled systems and how to protect AI-enabled systems from potential threats

On this occasion, 22 submissions were received, of which 9 were accepted for presentation at the workshop and inclusion in the proceedings. Each submission was reviewed by two or more subject matter experts.

06 March 2022 Sadiq Sani, Harsha Kalutarage
(Editors)

[1] - https://sites.google.com/view/ai-cybersec-2021/home

Program Chairs

Applications chair: Sadiq Sani, British Telecom Applied Research, UK

Technical chair: Harsha Kalutarage, Robert Gordon University, UK

Program Committee

Paul Miller, Centre for Secure Information Technologies (CSIT), Queen's University Belfast, UK
Jingyue Li, Department of Computer Science, Norwegian University of Science and Technology, Norway
Siraj Shaikh, Institute for Future Transport and Cities, Coventry University, UK
Ivan Palomares Carrascosa, DaSCI Institute of Data Science and Computational Intelligence
Jorge Blasco Alis, Department of Information Security, Royal Holloway, University of London, UK
Toktam Mahmoodi, King's College London, UK
Martin Gilje Jaatun, Department of Electrical Engineering and Computer Science at University of Stavanger, SINTEF Digital in Trondheim, Norway.
Alex Healing, Cybersecurity Research, British Telecom.
Max Smith-Creasey, Cybersecurity Research, British Telecom
Ali Niknejad, Microsoft, Redmond, Washington, United States

Organisers

Nektaria Kaloudi, Norwegian University of Science and Technology, Norway
Nirmalie Wiratunga, Robert Gordon University, UK
Jin Zhang, Norwegian University of Science and Technology, Norway
Chamath Palihawadana, Robert Gordon University, UK

Acknowledgements

We would like to express our gratitude to a number of reviewers who willingly assisted in reviewing and proofreading the manuscripts.
M.Omar Al-Kadri, Birmingham City University, UK
Anjana Wijekoon, Robert Gordon University, UK
Xin Hong, Queen's University Belfast, UK
Indika Rathnathungalage, Prairie View A&M University, USA
Federico Cruciani, Ulster University, UK
Samuel Moore, Ulster University, UK
Zeinab Rezaeifar, Ulster University, UK
Idris Zakariyya, Robert Gordon University, UK
Shadi Hajar, Robert Gordon University, UK