Multi-Disciplinary Aspect of Cyber Security Data Privacy and Security (Code: 1se23)

Goal:

Data breaches represents one of the key challenges facing the Cyber Security community. Everyday there are data breaches occurred in business organizations and the economic and reputation loss suffered by organizations are in the millions of dollars and sometimes incalculable.
In the world of increasing cyber threats and multi-facet influence of technologies, automation techniques and social justice to Cyber Security, the Cyber Security is increasingly multidisciplinary in its research methodology. Indeed, questions have been asked whether data breach prevention can be achieved through multidisciplinary approach for example by employing automation techniques, utilization of Machine Learning algorithms, and technology such as open AI. In fact, this has been the justifiable reason for gathering researchers around the world to dive deeper into the research problems facing the Cyber Security community. Through this special session, contributions can be made in the field of Cyber Security in relation to the Internet of Things (IoT), Web Applications, metaverse, to name a few.
Therefore, the objectives of this special session are as follows:

- To share the knowledge and experience of multidisciplinary Cyber Security research topics from the research community. These topics will be multidisciplinary in nature, culminating both domain-specific knowledge and experience from the researchers.
- To increase the opportunity for cross-discipline collaboration among the Cyber Security and related field research community. These collaborations could lead to improved system design, better understanding of Cyber Security components involved in complex system design.
- To further advance the Cyber Security research through scientific publication and contribution to the algorithms, automation techniques and innovative ideas, especially pertinent to the data security, data breaches and privacy.

This proposed special session would produce innovative ideas through mutual open dialogue, encourage scientific publications in topics related to Cyber Security, and would result in closer networking and collaboration among the session participants. The up-coming and incremental research direction can be reinforced, and follow-up calls can be made to encourage international funding exploration.

Topics:

- Application of AI and Automation technologies in combating cyber-attacks.
- Security Architecture, risk management and Control Frameworks – Review and Analysis.
- Social media system, Metaverse, and public system security, mitigation techniques.
- Multi-facet authentication, exploring AI/ML/DL, with open-source security components.
- Specific research problems, issues and mitigation in security operation center (SOC), defensive Cyber Security research area (such as flag escalation, hidden risk identification).
- Smart malware, virus, trojan, worm detection and prediction, prevention methods
- Data breach, data security, data governance, data loss prevention (DLP) effectiveness and performance evaluation.
- Automating threat intelligence, identification of hidden cybersecurity risks, problems, issues, etc.

Contact the lead Organizer:

Soonleh Ling**, Dr**
Leader, York St John University, UK
E-mail: s.ling@yorksj.ac.uk
Phone: +44-(0)7827316127