Advanced Program Summary

1 November 2023 (Wednesday)								
	Meeting Room: Devonshire A and B							
9:15-9:45	Opening Ceremony							
9:45-10:30	Keynote Speech 1							
10:30-11:00	**Coffee Break**							
11:00-11:45	Keynote Speech 2							
11:45-12:30	Keynote Speech 3							
12:30-13:30	**Conference Lunch**							
	Devonshire A	**Devonshire B**	**Burlington**	**Online Room 1**	**Online Room 2**	**Online Room 3**	**Online Room 4**	**Online Room 5**
13:30-15:30	TrustCom-1	ITCCN-1	CSE-1+ BigDataSE	TrustCom-5	TrustCom-11	ITCCN-6	BDRA-1	UbiSec-3+ ColTrust
15:30-16:00	**Coffee Break**							
16:00-18:00	TrustCom-2	ITCCN-2	ACE-1	TrustCom-6	TrustCom-12	ITCCN-7	BDRA-2	UbiSec-4+ SPoiT+CAI-2

2 November 2023 (Thursday)								
	Meeting Room: Devonshire A and B							
9:00-9:45	Keynote Speech 4							
9:45-10:30	Keynote Speech 5							
10:30-11:00	**Coffee Break**							
11:00-11:45	Keynote Speech 6							
11:45-12:30	Keynote Speech 7							
12:30-13:30	**Conference Lunch**							
	Devonshire A	**Devonshire B**	**Burlington**	**Online Room 1**	**Online Room 2**	**Online Room 3**	**Online Room 4**	**Online Room 5**
13:30-15:30	TrustCom-3	ITCCN-3	UbiSec-1	TrustCom-7	TrustCom-13	ITCCN-8	AINET-1	CIT
15:30-16:00	**Coffee Break**							
16:00-18:00	TrustCom-4	ITCCN-4	UbiSec-2	TrustCom-8	TrustCom-14	ITCCN-9	MLSys-1	DSCI +SmartCNS
19:00-21:30	**Conference Dinner**							

3 November 2023 (Friday)								
	Burlington	**Chartsworth**	**Online Room 1**	**Online Room 2**	**Online Room 3**	**Online Room 4**	**Online Room 5**	**Online Room 6**
9:00-10:30	ITCCN-5+IUCC-2	EUC-1	TrustCom-9	TrustCom-15	ITCCN-10	SAGIINAT-1	CSE-2+iSCI	TrustCom-17 +EUC-3
10:30-11:00	**Coffee Break**							
11:00-12:30	CAI-1+ACE-2 +CSE-4	EUC-2	TrustCom-10 +ITCCN-13	TrustCom-16	ITCCN-11	SAGIINAT-2+ AINet-2 +MLSys-2	CSE-3+ITCCN-14	IUCC-1+ ITCCN-12
12:30-13:30	**Conference Lunch**							

The papers published in the conference proceedings can be downloaded **HERE**:username: **trustcompub23**, password: **conf23//**

*Greenwich Mean Time (GMT).

TABLE OF CONTENTS

The opening ceremony/keynote speech:
https://Universityofexeter.zoom.us/j/94496458616?pwd=Mk1HSzlJS2RxbmUzZ29ZcHJISllUQT09
Online Room 1:
https://Universityofexeter.zoom.us/j/91065143667?pwd=ZzFXMnJnUlk2VmMybERveThkM0UrUT09
Online Room 2:
https://Universityofexeter.zoom.us/j/99685207462?pwd=ekxlN1VRdmlQUFpKdjh5a0Z1WWdOUT09
Online Room 3:
https://Universityofexeter.zoom.us/j/98123997085?pwd=QWpkWEZyUWRsWlM4WXpuZkFwWHBzQT09
Online Room 4:
https://Universityofexeter.zoom.us/j/96531912194?pwd=dC84SzBMN0RGTmswRFZjUER6UTZ3dz09
Online Room 5:
https://Universityofexeter.zoom.us/j/92147395381?pwd=N2xkKzZUeUlqbGZjbWlHRmtOZVhnZz09
Online Room 6:
https://Universityofexeter.zoom.us/j/92547982685?pwd=TlBlWS9nZ2FjK1Y5cWUweVlMSG1oUT09

Keynote Speech 1

Random Neural Networks (RNN) for Accurate Cyber Attack Detection and Mitigation at the Edge

Prof. Erol Gelenbe

FIEEE FACM MAE
Fellow of the French National Academy of Engineering
Fellow of the Science Academies of Belgium, Poland and Turkey
Honorary Fellow of the Hungarian and Islamic Academy of Sciences
Institute of Theoretical & Applied Informatics, Polish Academy of Sciences,
& University Côte d'Azur I3S CNRS, 06100 Nice, France

Abstract

Even simple cyberattacks can impair the operation and performance of network systems substantially for many hours and sometimes days, and also increase the system's energy consumption. Their impact on data security, and the effects of the malware that they convey and install, are also well known. Thus there is a widespread need for accurate cyberattack detection, and rapid reaction and mitigation when attacks occur. On the other hand, the detection must avoid false alarms, to avoid impairing the smooth operation of a system which is not under attack. Thus considerable research has been conducted in this important field. Our presentation will briefly introduce the subject, and then focus on some recent results from the last 4-5 years, that are based on the Random Neural Network (RNN). The mathematical model will be described, and its extensions and deep learning algorithms will be discussed in the context of cyberattack detection and mitigation. The presentation will then focus on practical applications illustrated with different cyberattack datasets, showing the high accuracy and low false alarm rates that can be achieved. Measurements of active control schemes for attack mitigation will also be shown. Finally we will also show how the RNN can be used with Reinforcement Learning and SDN (Software Defined Networks), to dynamically control an Edge System that optimises Security, QoS and Energy Consumption.

Note. The talk will be based on our publications in the following journals and conferences: Proceedings of the IEEE (2020), Sensors (2021, 2023), ACM SIGCOMM Flexnets (2021), ICC (2016, 2022), IEEE Access (2022, 2023), Performance Evaluation (2022).

Biography

Erol Gelenbe ChEng FIEEE FACM held named personal chairs at NJIT (USA), Duke University (USA), University of Central Florida (USA), and Imperial College (UK). He served as Department Head at Duke University, Director of the School of EECS at UCF, and Dennis Gabor Chair & Head of Intelligent Systems and Networks (Imperial College). His research, which focuses on QoS, Security and Energy, was funded by Industry, DoD and NSF in the USA, EPSRC and MoD in the UK, and he has benefited from numerous EU FP5, FP6, FP7, and Horizon 2020 projects since 2003. Currently Professor at the Institute of Theoretical & Applied Informatics, Polish Academy of Sciences, he cooperates on research with the CNRS I3S Laboratory of University Côte d'Azur (Nice, France), and Yasar University (Izmir, Turkey). His current work is supported by grants from H2020 Horizon and UKRI. He is ranked among the top 25 PhD advisors by the American Mathematical Society Math. Genealogy Project, and has won the Grand Prix France Telecom 1996 (French Academy of Sciences), the ACM SIGMETRICS 2008 Life-Time Award, the 2008 Imperial College Rector's Research Award, the 2010 IET Oliver Lodge Medal (IET Innovation Award for Information Technology), and the Mustafa Prize 2017. He was awarded high honours of Commander of the Order of the Crown, Belgium (2022), Commander of the Order of Merit, France (2019), Knight of the Legion of Honour, France (2014), Commander of the Order of Merit, Italy (2005), Grand Officer of the Order of the the Star, Italy (2007). He is a Fellow of several national academies, and currently chairs the Informatics Section of Academia Europaea.

Keynote Speech 2

IoT Autonomics: Building the Autonomous IoT Environment of the Future

Nektarios Georgalas

Senior and Principal Researcher
Manager for Innovation, Solutions Architecture and Technical Programme (IoT)
BT, UK

Abstract

The Internet of Things is rapidly expanding at an unprecedented rate. Presently, there is an estimated over 15 billion connected IoT devices, which is predicted to increase by a factor of 2 by 2030. This results in IoT ecosystems with increasing complexity due to the sheer volume of sensors, variety of network connectivity, different IoT platforms and systems spanning from edge to cloud or originating from a plethora of vendors/hyperscalers. Managing complexity at this scale requires automation, since manual processes are inefficient. We are developing the Autonomous IoT. We engage AI and Machine Learning techniques in managing this complexity autonomously through self-initiated capabilities, where IoT ecosystems become self-serviced and self-managed. In this talk we will present the business case and motivation for IoT Autonomics, introduce the IoT Value Added Services layer, whose purpose is to deliver this intelligence in IoT Ecosystems transforming them to autonomously managed entities, contextualise our work with experiences/use-cases from a recent trial in Belfast Harbour and conclude with a deep dive into a few of these IoT VAS with live demos of the capabilities.

Biography

Nektarios Georgalas has 26 years in BT, as a Senior and Principal Researcher in BT Research and Network Strategy and more recently as a Manager for Innovation, Solutions Architecture and Technical Programme (IoT) in BT Digital. He currently leads the IoT programme in the BT Ireland Innovation Centre (BTIIC) where in collaboration with Universities, BT Research and BT Engineering teams, BT partners and customers he is driving the delivery and realisation of the Autonomous IoT vision to implement self-serviced and self-managed IoT Ecosystems by means of AI, machine learning, advanced analytics, Edge/Fog/Cloud Computing, IoT SLA management and optimisation. In his career, he pioneered several areas for BT leading to strategy, tools and architecture or platform interventions, with major driver always being value creation. He has been the BT director for two co-innovation programmes with BT partners delivering innovations in the areas of Cloud Services and Security, Data Centres, Network Virtualisation, Smart Cities, IoT and Mobility. He established and led two standards teams in the TeleManagement Forum where he also led multiple international consortia of major market players and vendors to deliver impactful Catalyst projects, awarded for excellence and best innovation, with influence on the telecoms market and the Forum's strategy towards a model-driven and software-defined ecosystem of digital services in dynamic marketplaces. Overall, his work has been recognised by 22 awards including the TMForum's "Excellence Award for Innovation" 2010, "Most Innovative Catalyst Award" 2014, "Best New Catalyst Award" 2015 and "Most Significant Contribution to Frameworx Award" 2015, “Most Innovative Catalyst – Smart X Commercial” 2016, “Outstanding Performance in the Catalyst Programme” 2017 and “Smart City Innovator of the Year” Excellence Award 2017. Other recognition accolades include Global Telecoms Business's "Business Service Innovation Award" 2010, 2012 and 2013. He has been Finalist in UK IT Industry Award for "Best IT Innovation" in 2013 and Highly Commended for the IET Innovation Award for Telecommunication in 2009. He has also achieved "Best innovation for Large Enterprise" and "Best Customer Experience Innovation" Finalists in BT Innovation Awards 2010. Nektarios has been recognised in BT's TSO "Brilliant People" 2015. For IEEE service Nektarios has been awarded 2 IEEE Outstanding Awards and 2 IEEE Outstanding Leadership Awards. Nektarios is inventor and co-inventor of 16 patents. He has been actively publishing in major high impact factor international IEEE Journals and Conferences, totalling more than 90 peer-reviewed papers. He has served as guest editor in IEEE journals on topics of IoT, Big Data and Data Science. He chaired 6 IEEE Conferences and frequently presents as invited Keynote Speaker. Finally, he has co-edited 6 Conference proceedings books.

Session Chair: Jia Hu, University of Exeter, UK

Keynote Speech 3

Towards Distributed MLOps: Theory and Practice

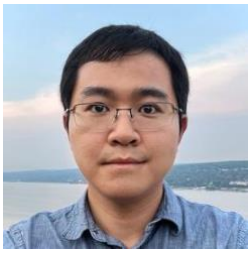
Dr. Shiqiang Wang

Staff Research Scientist
IBM T.J. Watson Research Center, United States

Abstract

As machine learning (ML) technologies get widely applied to many domains, it has become essential to rapidly develop and deploy ML models. Towards this goal, MLOps has recently emerged as a set of tools and practices for operationalizing production-ready models in a reliable and efficient manner. However, several open problems exist, including how to automate the ML pipeline that includes data collection, model training, and deployment (inference) with support for distributed data and models stored at multiple edge sites. In this talk, I will cover some theoretical foundations and practical approaches towards enabling distributed MLOps, i.e., MLOps in large-scale edge computing systems. I will start with explaining the requirements and challenges. Then, I will describe how our recent theoretical developments in the areas of coreset, federated learning, and model uncertainty estimation can support distributed MLOps. As a concrete example, I will dive into the details of a federated learning algorithm with flexible control knobs, which adapts the learning process to accommodate time-varying and unpredictable resource availabilities, as often seen in systems in operation, while conforming to a given budget for model training. I will finish the talk by giving an outlook on some future directions.

Biography



Shiqiang Wang is a Staff Research Scientist at IBM T. J. Watson Research Center, NY, USA. He received his Ph.D. from Imperial College London, United Kingdom, in 2015. His current research focuses on the intersection of distributed computing, machine learning, networking, and optimization, with a broad range of applications including data analytics, edge-based artificial intelligence (Edge AI), Internet of Things (IoT), and future wireless systems. He received the IEEE Communications Society (ComSoc) Leonard G. Abraham Prize in 2021, IEEE ComSoc Best Young Professional Award in Industry in 2021, IBM Outstanding Technical Achievement Awards (OTAA) in 2019, 2021, 2022, and 2023, and multiple Invention Achievement Awards from IBM since 2016. For more details, please visit his homepage at: https://shiqiang.wang.

Keynote Speech 4

Blockchain Technology and System

Prof. Keqiu Li

IEEE Fellow
Tianjin University, China

Abstract

This talk starts with the brief introduction of blockchain and the milestones in development process. Through the analysis of cutting-edge blockchain technologies, this talk summarizes the critical challenges in the blockchain research area. Furthermore, this talk presents a blockchain system named Haihe-Smart-Chain developed by the research group, and key techniques involved in it. Finally, this talk discusses the future directions of blockchain.

Biography

Keqiu Li is a professor and dean of the College of Intelligence and Computing, Tianjin University, China. He is the recipient of National Science Foundation for Distinguished Young Scholars of China. He received his bachelor's and master's degrees from the Department of Applied Mathematics at the Dalian University of Technology in 1994 and 1997, respectively. He received the Ph.D. degree from the Graduate School of Information Science, Japan Advanced Institute of Science and Technology in 2005. He keeps working on the topics of blockchain system, mobile computing, datacenter, and cloud computing. He has more than 150 papers published on prestigious journals or conferences such as TON, TPDS, TC, TMC, MobiCom, INFOCOM, ICNP, etc.

Keynote Speech 5

Scalable Deep Learning from Big Data

Prof. Liangxiu Han

Co-Director of Centre for Advanced Computational Science
Deputy Director of MMU Crime & Wellbeing Big Data Centre
Manchester Metropolitan University, UK

Abstract

In recent years, deep learning has attracted much attention due to its nature in discovering correlation structure in data in an unsupervised fashion and has been applied into various domains such as in speech recognition and image classification, nature language processing and computer vision. In typical neural networks, it requires large-scale data to learn parameters (often reach to millions), which is a computationally intensive process and takes a lot of time to train a model. Scalable deep learning is therefore much needed, which can train complex models over a vast amount of data, allowing for optimal training performance in terms of computing time and accuracy. This talk will focus on the latest developments and real-world applications of scalable deep learning from big data.

Biography

Prof. Liangxiu Han has a PhD in Computer Science from Fudan University, Shanghai, P.R. China (2002). Prof. Han is currently a Professor of Computer Science at the Department of Computing and Mathematics, Manchester Metropolitan University. She is a co-Director of Centre for Advanced Computational Science and Deputy Director of ManMet Crime and Well-Being Big Data Centre. Han's research areas mainly lie in the development of novel big data analytics/Machine Learning/AI, and development of novel intelligent architectures that facilitates big data analytics (e.g., parallel and distributed computing, Cloud/Service-oriented computing/data intensive computing) as well as applications in different domains (e.g. Precision Agriculture, Health, Smart Cities, Cyber Security, Energy, etc.) using various large scale datasets such as images, sensor data, network traffic, web/texts and geo-spatial data. As a Principal Investigator (PI) or Co-PI, Prof. Han has been conducting research in relation to big data/Machine Learning/AI, cloud computing/parallel and distributed computing (funded by EPSRC, BBSRC, Innovate UK, Horizon 2020, British Council, Royal Society, Industry, Charity, respectively, etc.).

Prof. Han has served as an associate editor/a guest editor for a number of reputable international journals and a chair (or Co-Chair) for organisation of a number of international conferences/workshops in the field. She has been invited to give a number of keynotes and talks on different occasions (including international conferences, national and international institutions/organisations).

Prof. Han is a member of EPSRC Peer Review College, an independent expert for European Commission proposal evaluation, and British Council Peer Review Panel.

Keynote Speech 6

Enabling Artificial Intelligence of Things through Interdisciplinary AI and Data Science Research

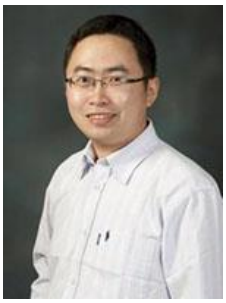
Prof. Lu Liu

Fellow of BCS (British Computer Society)
University of Leicester, UK

Abstract

In the era of the Internet of Things (IoT), an extensive network of interconnected physical devices spanning the globe continuously gathers and shares data. The convergence of IoT with cutting-edge Artificial Intelligence (AI) is giving rise to a transformative wave of innovation. This synergy, known as Artificial Intelligence of Things (AIoT), is set to reshape our future in the realm of smart technologies. Professor Liu will introduce his interdisciplinary research in AI and Data Science, focused on catalysing the emergence of AIoT. His work encompasses foundational investigations within this domain, as well as a diverse range of applications, spanning AI's role in healthcare and Net Zero, and its utilization in commercial data analytics, social media data analytics and sustainable data centre workload analytics.

Biography



Professor Lu Liu is a Professor at the School of Computing and Mathematical Sciences with expertise in AI, Data Science, Sustainable Systems and the Internet of Things, focusing on developing trustworthy and sustainable systems based on machine learning for health, Net Zero and digital manufacturing. Professor Liu received his PhD degree from Surrey Space Centre at the University of Surrey. He had worked as a Research Fellow at the WRG e-Science Centre at the University of Leeds. Professor Liu has over 250 scientific publications in reputable journals and international conferences. Professor Liu has secured over 30 grants which are supported by UKRI/EPSRC, Innovate UK, Royal Society, British Council and leading industries (e.g. BT, Royce-Royce, CGI). He received the Staff Excellence Award in Doctoral Supervision in 2018. He has been the recipient of 7 Best Paper Awards from international conferences and was invited to deliver 8 keynote speeches at international conferences. Professor Liu is currently the University Turing Liaison (Academic) for the Turing University Network (The Alan Turing Institute) at the University of Leicester.

Keynote Speech 7

Machine Learning for Optimal Resource Allocation in Communication Networks and Computing Infrastructures

Prof. Kin K. Leung

Fellow of the Royal Academy of Engineering
IEEE Fellow
IET Fellow
EEE and Computing Departments
Imperial College, London, UK

Abstract

Optimization techniques are widely used to allocate and share limited resources to competing demands in communication networks and computing infrastructures. The speaker will start by showing the well-known Transport Control Protocol (TCP) on the Internet as a distributed solution to achieve the optimal allocation of network bandwidth. Unfortunately, factors such as multiple grades of service quality, variable transmission power, and tradeoffs between communication and computation often make the optimization problem for resource allocation non-convex. New distributed solution techniques are needed to solve these problems.

Gradient-based iterative algorithms are commonly used to solve these optimization problems. Much research focuses on improving the iteration convergence. However, when the system parameters change, it requires a new solution from the iterative methods. The speaker will present a new machine-learning method by using two Coupled Long Short-Term Memory (CLSTM) networks to quickly and robustly produce the optimal or near-optimal solutions to constrained optimization problems over a range of system parameters. Numerical examples for allocation of network resources will be presented to confirm the validity of the proposed method.

Biography

Kin K. Leung received his B.S. degree from the Chinese University of Hong Kong, and his M.S. and Ph.D. degrees from University of California, Los Angeles. He joined AT&T Bell Labs in New Jersey in 1986 and worked at its successor companies until 2004. Since then, he has been the Tanaka Chair Professor in the Electrical and Electronic Engineering (EEE), and Computing Departments at Imperial College in London. He serves as the Head of Communications and Signal Processing Group in the EEE Department at Imperial. His current research focuses on optimization and machine-learning techniques for system design and control of large-scale communications, computer and sensor networks. He also works on multi-antenna and cross-layer designs for wireless networks.

He is a Fellow of the Royal Academy of Engineering, IEEE Fellow, IET Fellow, and member of Academia Europaea. He received the Distinguished Member of Technical Staff Award from AT&T Bell Labs (1994) and the Royal Society Wolfson Research Merits Award (2004-09). Jointly with his collaborators, he received the IEEE Communications Society (ComSoc) Leonard G. Abraham Prize (2021), the IEEE ComSoc Best Survey Paper Award (2022), the U.S.–UK Science and Technology Stocktake Award (2021), the Lanchester Prize Honorable Mention Award (1997), and several best conference paper awards. He currently serves as the IEEE ComSoc Distinguished Lecturer (2022-23). He was a member (2009-11) and the chairman (2012-15) of the IEEE Fellow Evaluation Committee for the ComSoc. He has served as guest editor and editor for 10 IEEE and ACM journals and chaired the Steering Committee for the IEEE Transactions on Mobile Computing. Currently, he is an editor for the ACM Computing Survey and International Journal on Sensor Networks.

Part I: TECHNICAL SESSIONS OF TrustCom/BigDataSE/CSE/EUC/iSCI-2023 and Associated Workshops/Symposia

TrustCom-2023 TECHNICAL SESSIONS

1 November 2023 Wednesday

13:30-15:30 Session TrustCom-1: Network and System Security (I) (Room: Devonshire A)

Session Chair: Xiaofang Maggie Wang, Villanova University, USA

- Protecting IoT Servers Against Flood Attacks with the Quasi Deterministic Transmission Policy
  Erol Gelenbe, Mohammed Nasereddin
- Extracting Length Field of Unknown Binary Network Protocol from Static Trace
  Xiuwen Sun, Zhihao Wu, Jing Lin, Pengfei Fu, Jie Cui, Hong Zhong
- Detecting DDoS Attacks on the Network Edge: An Information-Theoretic Correlation Analysis
  Ryosuke Araki, Kshira Sagar Sahoo, Yuzo Taenaka, Youki Kadobayashi, Erik Elmroth, Monowar Bhuyan
- RCA-IDS: A Novel Real-time Cloud-based Adversarial IDS for Connected Vehicles
  Zahra Pooranian, Mohammad Shojafar, Pedram Asef, Matthew Robinson, Harry Lees, Mark Longden
- MEDICALHARM - A Threat Modeling designed for Modern Medical Devices
  Emmanuel Kwarteng, Mumin Cebe
- Towards Understanding Checkpointing in Transiently Powered IoT Networks
  Jawaher Alharbi, Adam Chester, Arshad Jhumka

13:30-15:45 Session TrustCom-5: Blockchain and Distributed Ledger (Room: Online Room 1)

Session Chair: Jinyao Zhu, Guangzhou University, China

- HyperChain: A Dynamic State Sharding Protocol Supporting Smart Contracts to Achieve Low Cross-Shard and Scalability
  Hengyu Pan, Cheng Qu, Haowen Zhang, Shuo Wang, Jing Li
- Efficient Covert Communication Scheme Based on Ethereum
  Yuanyuan Li, Wei Chen, Xin Huang, Peng Han, Shenhai Zheng, Zhiqin Zhu
- Two-Stage Smart Contract Vulnerability Detection Combining Semantic Features and Graph Features
  Zhenkun Luo, Shuhong Chen, Guojun Wang, Hanjun Li
- TI-DNS: A Trusted and Incentive DNS Resolution Architecture based on Blockchain
  Yufan Fu, Jiuqi Wei, Ying Li, Botao Peng, Xiaodong Li
- Felix: A Model of Detecting Off-chain Abnormal States in Decentralized Applications
  Lianhai Wang, Qihao Huang, Wei Shao, Jinpeng Wang, Xiaoqian Liu, Fansheng Wang
- Opcode Sequences-Based Smart Contract Vulnerabilities Detection Using Deep Learning
  Jinyao Zhu, Xiaofei Xing, Guojun Wang, Peiqiang Li
- A Commitment and Ring Signature based Scheme for Amount and Identity Privacy Protection in Blockchain
  Shiyong Huang, Haocong Li, Ruoting Xiong, Wei Ren, Jie He, Yi Ren
- IHFBF: A High-Performance Blockchain Framework for Improving Hyperledger Fabric Permissioned Chain
  Min Xu, XiaoDing Wang, Hui Lin
- VMR-Tree: Efficient and Verifiable Location-based kNN Queries on Blockchain
  Yiping Teng, Lei Liu, Jiawei Qi, Haochun Pan, Chunlong Fan

13:30-15:45 Session TrustCom-11: Computer and Data Security (I) (Room: Online Room 2)

Session Chair: Zhengxin Yu, University of Lancaster, UK

- Differential Privacy Frequent Closed Itemset Mining over Data Stream
  Xuebin Ma, Shengyi Guan, Yanan Lang
- MPS: A Multiple Poisoned Samples Selection Strategy in Backdoor Attack
  Weihong Zou, Shigeng Zhang, Weiping Wang, Jian Zhang, Xuan Liu
- UFADF: A Unified Feature Analysis and Detection Framework for Malicious Office Documents
  Yang Hu, Jia Chen, Xin Luo
- EAMDM: An Evolved Android Malware Detection Method Using API Clustering
  Hongyu Yang, Youwei Wang, Liang Zhang, Ze Hu, Xiang Cheng, Laiwei Jiang
- SPSW: Database Watermarking Based on Fake Tuples and Sparse Priority Strategy
  Zhiwen Ren, Zehua Ma, Weiming Zhang, Nenghai Yu
- Crowdsensed Data-oriented Distributed and Secure Spatial Query Scheme
  Yuxi Li, Fucai Zhou, Jingjing Chen, Dong Ji
- Flush+Revisit: A Cross-CCX Side-Channel Attack on AMD Processors
  Danping Li, Ziyuan Zhu, Jiao Shen, Yusha Zhang, Gang Shi, Dan Meng
- Self-attention is What You Need to Fool a Speaker Recognition System
  Fangwei Wang, Ruixin Song, Zhiyuan Tan, Qingru Li, Changguang Wang, Yong Yang
- FPHammer: A Device Identification Framework based on DRAM Fingerprinting
  Dawei Li, Di Liu, Yangkun Ren, Ziyi Wang, Yu Sun, Zhenyu Guan, Qianhong Wu, Jianwei Liu

16:00-18:00 Session TrustCom-2: Blockchain and Distributed System (Room: Devonshire A)

Session Chair: Reham Al Tamime, Qatar Computing Research Institute, Qatar

- Rethinking Practical Blockchain-Based Symmetric Searchable Encryption Services
  Jun Zhao, Jiangshan Yu, Xingliang Yuan, Joseph K. Liu, Cong Zuo
- PrivOff: Secure and Privacy-Preserving Data Management for Distributed Off-Chain Networks
  Htet Htet Hlaing, Hitoshi Asaeda
- FL-TIA: Novel Time Inference Attacks on Federated Learning
  Chamara Sandeepa, Bartlomiej Siniarski, Shen Wang, Madhusanka Liyanage
- Parallel Pattern Matching over Brotli Compressed Network Traffic
  Xiuwen Sun, Guangzheng Zhang, Di Wu, Qingying Yu, Jie Cui, Hong Zhong
- DFedXGB: An XGB Vertical Federated Learning Framework with Data Desensitization
  Qing Yang, Youliang Tian, Jinbo Xiong
- Impact of Aggregation Function Randomization against Model Poisoning in Federated Learning
  Seyedsina Nabavirazavi, Rahim Taheri, Mohammad Shojafar, Sundararaja Sitharama Lyengar

16:00-18:45 Session TrustCom-6: Attacks and Anomalies Detection (Room: Online Room 1)

Session Chair: Marios Anagnostopoulos, Aalborg University, Denmark

- Insider Threat Detection Based on Heterogeneous Graph Neural Network
  Tian Tian, Yiru Gong, Bo Jiang, Junrong Liu, Huamin Feng, Zhigang Lu
- Inter-slice Correlation Weighted Fusion for Universal Lesion Detection
  Muwei Jian, Yue Jin, Rui Wang, Xiaoguang Li, Hui Yu
- Anomaly Detection in Dynamic Networks through Edge-Tight Structure Embedding
  Liming Wang, Jiaxing Fan, Fengzhe Zhong, Yan Liu, Jinyang Liu
- A DGA Domain Name Detection Method Based on Two-Stage Feature Reinforcement
  Hongyu Yang, Tao Zhang, Ze Hu, Liang Zhang, Xiang Cheng
- REDA: Malicious Traffic Detection Based on Record Length and Frequency Domain Analysis
  Wanshuang Lin, Chunhe Xia, Tianbo Wang, Chen Chen, Yuan Zhao, Weidong Zhou
- IAD-Net: Multivariate KPIs Interpretable Anomaly Detection with Dual Gated Residual Fusion Networks

Wen Liu, Degang Sun, Haitian Yang, He Zhu, Yan Wang

- FINDER: A Simple and Effective Defender against Unnoticeable Graph Injection Attacks
  Linlin Su, Jinyan Wang, Zeming Gan, Xianxian Li
- MTD-RTPE: A Malicious Traffic Detection Method Based on Relative Time-Delay Positional Encoding
  Jingyu Liu, Chunfang Yang, Ma Zhu, Baojun Qi, Xueyuan Fu, Mengyang Zhou
- High-knowledge shilling attack detection method based on genetic co-forest
  Lingyue Su, Yongli Wang
- LActDet: An automatic network attack activity detection framework for multi-step attacks
  Huiran Yang, Jiaqi Kang, Yueyue Dai, Yan Zhang, Huajun Cui, Can Ma
- A Scalable Pattern Matching Implementation on Hardware using Data Level Parallelism
  Hassan Jalil Hadi, Khurram Shahzad, Naveed Ahmed, Yue Cao, Yasir Javed

16:00-18:45 Session TrustCom-12: Network and System Security (II) (Room: Online Room 2)

Session Chair: Ziqi Li, Beijing University of Posts and Telecommunications, China

- Lightweight Hierarchical Deterministic Wallet Supporting Stealth Address for IoT
  Chenghe Dong, Jianhong Zhang, Zongyi Lv, Ruxuan Zhang
- Investigating Fraud and Misconduct in Legitimate Internet Economy based on Customer Complaints
  Wenrui Ma, Ying Cong, Haitao Xu, Fan Zhang, Zhao Li, Siqi Ren
- Detecting BGP Anomalies based on Spatio-Temporal Feature Representation Model for Autonomous Systems
  Zimian Liu, Han Qiu, Rui Wang, Junhu Zhu, Qingxian Wang
- Do NoT Open (DOT): A Unified Generic and Specialized Models for Detecting Malicious Email Attachments
  Vinay Sachidananda, Sivaanandh Muneeswaran, Yang Liu, Kwok-Yan Lam
- GuiDiv: Mitigating Code-reuse Attack in an IoT Cluster Using Guided Control Flow Diversification.
  Yuanpei Li, Qinglei Zhou, Bin Li, Yan Zhuang
- Enhancing Security in Industrial IoT: A Taxonomy-driven Approach to Risk Assessment
  Muna Al-Hawawreh, Robin Doss
- Push It Real Good: Towards Behavioral Access Control using the Door Handle Push-Down-Phase Only
  Eric Klieme, Ben-Noah Engelhaupt, Vincent Xeno Rahn, Christoph Meinel
- HackMentor: Fine-Tuning Large Language Models for Cybersecurity
  Jie Zhang, Hui Wen, Liting Deng, Mingfeng Xin, Zhi Li, Lun Li, Hongsong Zhu, Limin Sun
- Topology construction method of anti-tracking network based on cross-domain decentralized gravity model
  Zhefeng Nan, Qian Qiang, Tianning Zang, Changbo Tian, Shuyuan Zhao, Shuhe Liu
- Software Vulnerabilities Detection Based on a Pre-trained Language Model
  Wenlin Xu, Tong Li, Jinsong Wang, Haibo Duan, Yahui Tang
- On ECG Signal Classification: An NAS-empowered Semantic Communication System
  Huanlai Xing, Huaming Ma, Zhiwen Xiao, Xinhan Wang, Bowen Zhao, Shouxi Luo, Li Feng, Lexi Xu

2 November 2023 Thursday

13:30-15:30 Session TrustCom-3: Trustworthy and Secure AI (I) (Room: Devonshire A)

Session Chair: Htet Htet Hlaing, National Institute of Information and Communications Technology, Japan

- Advanced Machine-Learning Technologies for Coronary Artery Disease Prediction using Heterogeneous Data
  Malak Alqulaity, Po Yang
- Learning in the Dark: Privacy-Preserving Machine Learning using Function Approximation
  Tanveer Khan, Antonis Michalas
- Towards Trust-Centric Networking: A General Model for Trust Evaluation
  Andrés F. Murillo, Ayoub Messous, Andikan Otung, Motoyoshi Sekiya
- TrustGlass: Human-Computer Trusted Paths with Augmented Reality Smart Glasses
  Hélio Borges, Daniel Andrade, João Nuno Silva, Miguel Correia
- Trustworthiness and Subversion in Large Service-Oriented Multi-Agent Systems under Virtual Anonymity and Blind Provider Selection
  Jerzy Konorski
- HiSec: Towards Cyber Threat Correlation and Discovery Based on Hierarchical Graph Neural Networks
  Liwen Xu, Xiang Lin, Jianhua Li, Min Bai, Liejun Wang
- TouchEnc: a Novel Behavioural Encoding Technique to Enable Computer Vision for Continuous Smartphone User Authentication
  Peter Aaby, Mario Valerio Giuffrida, William Buchanan, Zhiyuan Tan

13:30-15:45 Session TrustCom-7: Privacy and Trust (Room: Online Room 1)

Session Chair: Xiaoding Wang, Fujian Normal University, China

- Decentralized Matrix Factorization with Heterogeneous Differential Privacy
  Wentao Hu, Hui Fang
- Integrating VirtIO and QEMU on seL4 for Enhanced Devices Virtualization Support
  Everton de Matos, Conor Lennon, Eduardo K. Viegas, Markku Ahvenjärvi, Hannu Lyytinen, Ivan Kuznetsov, Joonas Onatsu, Anh Huy Bui
- Multi-Scale Feature Aggregation for Rumor Detection: Unveiling the Truth within Text
  Jianming Wu, Shuhong Chen, Guojun Wang, Hao Wang, Hanjun Li
- A Framework for Privacy Policy Enforcement for Connected Automotive Systems
  Anis Bkakria, Lydia Brika
- Cropping Resilient Secret Image Sharing Scheme with Lossless Recovery
  Shengyang Luo, Yaqi Liu, Xuehu Yan, Chao Huang
- Robustness and Privacy for Green Learning under Noisy Labels
  De Li, Tiange Xia, Qiyu Li, Xianxian Li, Jinyan Wang
- SecGAN: Honest-Majority Maliciously 3PC Framework for Privacy-Preserving Image Synthesis
  Yuting Yang, Lin Liu, Shaojing Fu, Jun-Jie Huang, Yuchuan Luo
- Deanonymize Tor Hidden Services Using Remote Website Fingerprinting
  Meiqi Wang, Muqian Chen, Zeyu Li, Xuebin Wang, Jinqiao Shi, Binxing Fang
- BAA: A Novel Decentralized Authorization System for Privacy-Sensitive Medical Data
  Cong Zha, Yulei Wu, Zexun Jiang, Wenqian Zhao, Hao Yin

13:30-15:45 Session TrustCom-13: Trustworthy and Secure AI (II) (Room: Online Room 2)

Session Chair: Zhe Wang, University of Exeter, UK

- Representation-enhanced APT Detection Using Contrastive Learning
  Fengxi Zhou, Baoming Chang, Yu Wen, Dan Meng
- APM: An Attack Path-based Method for APT Attack Detection on Few-Shot Learning
  Jiacheng Li, Tong Li, Runzi Zhang, Di Wu, Hao Yue, Zhen Yang
- Class-Targeted Poisoning Attacks against DNNs
  Jian Chen, Jingyao Wu, Hao Yin, Qiang Li, Wensheng Zhang, Chen Wang

- EzBoost: Fast And Secure Vertical Federated Tree Boosting Framework via EzPC
  Xinwen Gao, Shaojing Fu, Lin Liu, Yuchuan Luo, Luming Yang
- Neighborhood Matching Entity Alignment Model for Vulnerability Knowledge Graphs
  Qi Yan, Mohan Li, Yanbin Sun
- The Dynamic Paradox: How Layer-skipping DNNs Amplify Cache Side-Channel Leakages
  Jinze She, Wenhao Wang, Zihao Wang
- Reducing Model Memorization to Mitigate Membership Inference Attacks
  Mehrdad Sheikhjaberi, Dima Alhadidi
- Towards Dynamic Backdoor Attacks against LiDAR Semantic Segmentation in Autonomous Driving
  Shuai Li, Yu Wen, Xu Cheng
- BadLiDet: A Simple Backdoor Attack against LiDAR Object Detection in Autonomous Driving
  Shuai Li, Yu Wen, Huiying Wang, Xu Cheng

16:00-18:00 Session TrustCom-4: Computer and Data Security (II) (Room: Devonshire A)

Session Chair: Zhiyuan Tan, Edinburgh Napier University, UK

- GenRex: Leveraging Regular Expressions for Dynamic Malware Detection
  Dominika Regeciova, Dusan Kolar
- "A method like this would be overkill": Developers' Perceived Issues with Privacy-preserving Computation Methods
  Patrick Kuehtreiber, Viktoriya Pak, Delphine Reinhardt
- Achieving Higher Level of Assurance in Privacy Preserving Identity Wallets
  Benjamin Larsen, Nada El Kassem, Thanassis Giannetsos, Ioannis Krontiris, Stefanos Vasileiadis, Liqun Chen
- Robustness Assessment of Biometric Authenticators
  Romain Dagnas, Anis Bkakria, Reda Yaich
- Multi-stage Attack Detection and Prediction Using Graph Neural Networks: An IoT Feasibility Study
  Hamdi Friji, Ioannis Mavromatis, Adrian Sanchez-Mompo, Pietro Carnelli, Alexis Olivereau, Aftab Khan
- SSdetector: Secure and Manageable Host-based IDS with SGX and SMM
  Yoshimichi Koga, Kenichi Kourai
- A First Look at Digital Rights Management Systems for Secure Mobile Content Delivery
  Amir Rafi, Carlton Shepherd, Konstantinos Markantonakis

16:00-18:45 Session TrustCom-8: Trusted Computing (Room: Online Room 1)

Session Chair: Rui Jin, University of Exeter, UK

- Cluster Nodes Integrity Attestation and Monitoring Scheme for Confidential Computing Platform
  Ketong Shang, Fang Lu, Ke Huang, Yu Qin, Wei Li, Wei Feng
- SCATMAN: A Framework for Enhancing Trustworthiness in Digital Supply Chains
  Michael Eckel, Anirban Basu, Satoshi Kai, Hervais Simo Fhom, Sinisa Dukanovic, Henk Birkholz, Shingo Hane, Matthias Lieske
- PLDB: Protecting LSM-based Key-Value Store using Trusted Execution Environment
  Chenkai Shen, Lei Fan
- A Cost-effective Automation Method of Massive Vulnerabilities Analysis and Remediation Based on Cloud Native
  Tian Hu, Shangyuan Zhuang, Jiyan Sun, Yinlong Liu, Wei Ma, Hongchao Wang
- A Multi-Source Cross-Project Fine-Grained Vulnerability Detection System Using Fusion Representation

Gewangzi Du, Liwei Chen, Tongshuai Wu, Chenguang Zhu, Gang Shi

- MemInspect: Memory Forensics for Investigating Fileless Attacks
  Tao Leng, Yuedong Pan, Lixin Zhao, Aimin Yu, Ziyuan Zhu, Lijun Cai, Dan Meng
- Towards Survivable In-Memory Stores with Parity Coded NVRAM
  Zhixuan Wang, Guangping Xu, Hongzhang Yang, Yulei Wu
- Grading and Calculation of Synchronic Distance in Petri Nets for Trustworthy Modeling and analyzing
  Yumeng Cheng, Wangyang Yu, Xiaojun Zhai, Fei Hao, Yuan Liu
- A lightweight and high-precision approach for bulky JavaScript engines fuzzing
  Lianpei Zhou, Xi Xiao, Guangwu Hu, Hao Li, Xiangbo Wu, Tao Zhou
- BiLSTM and VAE Enhanced Multi-Task Neural Network for Trust-Aware E-Commerce Product Analysis
  Shusuke Wani, Xiaokang Zhou, Shohei Shimizu
- CENSOR: Privacy-preserving Obfuscation for Outsourcing SAT formulas
  Tassos Dimitriou, Khazam Alhamdan

16:00-18:30 Session TrustCom-14: Federated Learning (Room: Online Room 2)

Session Chair: Hongtao Lv, Shandong University, China

- Scalable Federated Learning for Fingerprint Recognition Algorithm
  Chenzhuo Wang, Yanrong Lu, Athanasios V. Vasilakos
- FedRSM: Representational-Similarity-Based Secured Model Uploading for Federated Learning
  Gengxiang Chen, Sheng Liu, Xu Yang, Tao Wang, Linlin You, Feng Xia
- Defending against Adversarial Attacks in Federated Learning on Metric Learning Model
  Zhipin Gu, Jiangyong Shi, Yuexiang Yang, Liangzhong He
- Crowdsourcing-based Model Testing in Federated Learning
  Yunpeng Yi, Hongtao Lv, Tie Luo, Junfeng Yang, Lei Liu, Lizhen Cui
- HDFL: Private and Robust Federated Learning using Hyperdimensional Computing
  Harsh Kasyap, Somanath Tripathy, Mauro Conti
- Byzantine-Robust Federated Learning through Dynamic Clustering
  Hanyu Wang, Liming Wang, Hongjia Li
- FedDLM: A Fine-Grained Assessment Scheme for Risk of Sensitive Information Leakage in Federated Learning-Based Android Malware Classifier
  Changnan Jiang, Chunhe Xia, Chen Chen, Huacheng Li, Tianbo Wang, Xiaojian Li
- UNITE: Privacy-Aware Verifiable Quality Assessment via Federated Learning in Blockchain-Empowered Crowdsourcing
  Liangen He, Haiqin Wu, Liang Li, Jucai Yang
- FedJudge: Blockchain-based full-lifecycle trustworthy federated learning incentive mechanism
  Jiuzheng Wang, Ruilin Zhang, Xinyi Li, Hao Yin
- Sym-Fed: Unleashing the Power of Symmetric Encryption in Cross-Silo Federated Learning
  Jinzhao Wang, Wenlong Tian, Ruixuan Li, Junwei Tang, Xuming Ye, Yaping Wan, Zhiyong Xu

3 November 2023 Friday

9:00-10:45 Session TrustCom-9: Cryptography (Room: Online Room 1)

Session Chair: Dominika Regéciová, Brno University of Technology, Czechia

- The Broken Verifying: Inspections at Verification Tools for Windows Code-Signing Signatures
  Guangqi Liu, Qiongxiao Wang, Cunqing Ma, Jingqiang Lin, Yanduo Fu, Bingyu Li, Dingfeng Ye
- A Broadband Subliminal Channel in Signatures Without Sharing the Signing Key
  Qinghua Hu, Chunxiang Xu, Wanpeng Li

- CEIVS: A Scalable and Secure Encrypted Image Retrieval Scheme with Vertical Subspace Clustering
  Ruizhong Du, Jing Cui, Mingyue Li, Yuqing Zhang
- Securing an Efficient Lightweight AES Accelerator
  Ruoyu Huang, Abdullah Aljuffri, Said Hamdioui, Kezheng Ma, Mottaqiallah Taouil
- Enhanced Ticket Transparency (eTT) Framework for Single Sign-On Services with Pseudonyms
  Guangqi Liu, Jingqiang Lin, Dawei Chu, Xiaokun Zhang, Qiongxiao Wang, Cunqing Ma, Fengjun Li, Dingfeng Ye
- SIMD Bootstrapping in FHEW Scheme
  Man Chen, Yuyue Chen, Zoe L. Jiang
- Efficient and Secure Authentication Key Establishment Protocol Using Chaotic Map and PUF in Smart Environments
  Fengling Pang, Chingfang Hsu, Man Ho Au, Lein Harn, Ze Zhang, Li Long

9:00-10:45 Session TrustCom-15: Trustworthy and Secure AI (III) (Room: Online Room 2)

Session Chair: Feihao, Shaanxi Normal University, China

- Safety or Not? A Comparative Study for Deep Learning Apps on Smartphones
  Jin Au-yeung, Shanshan Wang, Yuchen Liu, Zhenxiang Chen
- Big Data Assisted Object Detection with Privacy Protection
  JianLin Zhang, XiaoDing Wang, Hui Lin
- FlowBERT: An Encrypted Traffic Classification Model Based on Transformers Using Flow Sequence
  Quanbo Pan, Yang Yu, Hanbing Yan, Maoli Wang, Bingzhi Qi
- Fooling Object Detectors in the Physical World with Natural Adversarial Camouflage
  Dandan Li, Yufeng Li, Guiqi Zhang, Ke Sun, Jiangtao Li
- Too Noisy, or Not Too Noisy? A Private Training in Machine Learning
  Lukasz Krzywiecki, Grzegorz Zaborowski, Marcin Zawada
- FineCTI: A Framework for Mining Fine-grained Cyber Threat Information from Twitter Using NER Model
  Chunyan Ma, Jun Jiang, Kai Zhang, Zhengwei Jiang, Peian Yang, Xuren Wang, Huamin Feng
- Secure Synchronized Spatio-Temporal Trajectory Similarity Search
  Yiping Teng, Jiawei Qi, Lei Liu, Shiqing Wang, Li Xu, Chunlong Fan

9:00-10:45 Session TrustCom-17 & EUC-3: Network and System Security (III) (Room: Online Room 6)

Session Chair: Jie Gao, University of Exeter, UK

- Measuring DNS-over-Encryption Performance Over IPv6
  Liang Jiao, Yujia Zhu, Baiyang Li, Qingyun Liu
- SRBR: Anti-selfish Routing Based on Social Similarity and Reputation Using Fuzzy Logic
  Haoxiang Wang, Yu'ang Zhang, Yujie Song, Yue Cao, Chee Yen Leow, Shihan Bao
- Reinforcement Learning Based Neighbour Selection for VANET with Adaptive Trust Management
  Orvila Sarker, Hong Shen, M. Ali Babar
- SharpEye: Identify mKCP Camouflage Traffic through Feature Optimization
  Yuwei Xu, Zizhi Zhu, Yunpeng Bai, Lilanyi Wu, Kehui Song, Guang Cheng
- Network based Intrusion Detection using Time aware LSTM Autoencoder
  Ritesh Ratti, Sanasam Ranbir Singh, Sukumar Nandi
- Cerberus: Efficient OSPS Traffic Identification through Multi-Task Learning
  Yuwei Xu, Xiaotian Fang, Jie Cao, Rou Yu, Kehui Song, Guang Cheng
- Temporal-aware Lightweight Visual Tracking Method for Dynamic Traffic Scenes
  Xuming Cen, Nan Hu, Haozhe Wang, Shiyi Liu

11:00-13:45 Session TrustCom-10 & ITCCN-13: Computer and Data Security (III) (Room: Online Room 1)

Session Chair: Dominika Regéciová, Brno University of Technology, Czechia

- SATBA: An Invisible Backdoor Attack Based on Spatial Attention
  Huasong Zhou, Xiaowei Xu, Xiaodong Wang, Leon Bevan Bullock
- Sparsity Aware of TF-IDF Matrix to Accelerate Oblivious Document Ranking and Retrieval
  Zeshi Zhang, Guangping Xu, Hongzhang Yang, Yulei Wu
- SQL injection attack sample generation based on IE-GAN
  Mingdi Xu, Bo Xie, Feng Cui, Chaoyang Jin, Yu Wang
- Dynamic Security Parameters for Multichannel Secret Sharing Protocols
  David Pineda Reyes, Josiah Hsu, Claire Wagner, Devin Pohly
- Static-RWArmor: A Static Analysis Approach for Prevention of Cryptographic Windows Ransomware
  Md. Ahsan Ayub, Ambareen Siraj, Bobby Filar, Maanak Gupta
- LPA: A Lightweight PUF-based Authentication Protocol for IoT System
  Vikash Kumar Rai, Somanath Tripathy, Jimson Mathew
- Privacy-Preserving Detection Method for Transmission Line Based on Edge Collaboration
  Quan Shi, Kaiyuan Deng
- PANGA: Attention-based Principal Neighborhood Aggregation for Forecasting Future Cyber Attacks
  Alok Kumar Trivedi, Priyanka Bagade
- Unified Identification of Anomalies on the Edge: A Hybrid Sequential PGM Approach
  Javad Forough, Monowar Bhuyan, Erik Elmroth
- Random Chunks Generation Attack Resistant Cross-User Deduplication for Cloud Storage
  Xin Tang, Yiteng Zhou, Yudan Zhu, Mingjun Fu, Luchao Jin
- Undermining License Plate Recognition: A Data Poisoning Attack
  Bo Song, Yunpeng Yi, Ting Zhou, Junfeng Yang, Lei Liu

11:00-13:15 Session TrustCom-16: Emerging Technologies (Room: Online Room 2)

Session Chair: Songyuan Li, University of Exeter, UK

- MENDER: Multi-level Feature Fusion Discovery Framework for Exposed ICS Remote Management Devices in the Wild
  Liuxing Su, Zhenzhen Li, Gaopeng Gou, Zhen Li, Gang Xiong, Chengshang Hou
- Fine-Grained Task Scheduling Combining DDPG and Path Selection in LEO Satellite Networks
  Gaowei Zhang, Xu Zhou, Xiaobo Zhang
- Affinity-Based Resource and Task Allocation in Edge Computing Systems
  Wenbing Zou, Xiulei Liu, Shoulu Hou, Ye Zhang, Lin Miao, Yi Gong, Ning Li
- Distributed Dependent Task Offloading in CPU-GPU Heterogenous MEC: A Federated Reinforcement Learning Approach
  Hualong Huang, Zhekai Duan, Wenhan Zhan, Yichen Liu, Zhi Wang, Zitian Zhao
- LWVN:A Lightweight Virtual Network View Method to Defend Lateral Movement
  Degang Sun, Guokun Xu, Weijie Wang, Yan Wang, Qiujian Lv, Xinxing Zhou, Zhiqi Li
- Fuzz Testing for Rust Library Functions
  Yongjian Guo, Xi Xiao, Yuanyi Lin, Hao Li, Xiangbo Wu, Tao Zhou
- FlexAuth: A Decentralized Authorization System with Flexible Delegation
  Ziyu Fei, Ying Li, Jiuqi Wei, Yufan Fu, Botao Peng, Xiaodong Li
- RUE: Realising Unlearning from the Perspective of Economics
  Mingjian Tang, Weiqi Wang, Chenhan Zhang, Shui Yu
- Look Closer to Touch Behavior-enabled Android Pattern Locks: A Study in the Wild

Gergely Tuskó, Weizhi Meng, Brooke Lampe

ITCCN-2023 TECHNICAL SESSIONS

1 November 2023 Wednesday

13:30-15:30 Session ITCCN-1: Privacy and Trust (Room: Devonshire B)

Session Chair: Kalam Khadka, University of Canberra, Australia

- Understanding Privacy Concerns in Mobile Health Applications: A Scenario-based Online Survey
  Reham Al Tamime, Ali Farooq, Joni Salminen, Vincent Marmion, Wendy Hall
- Trustworthy Execution in Untrustworthy Autonomous Systems
  David Halasz, Suyash Shandilya, Barbora Buhnova
- Survey on Recognition of Privacy Risk from Responding on Twitter
  Toru Nakamura, Yukiko Sawaya, Takamasa Isohara
- Membership Inference Attacks against GNN-based Hardware Trojan Detection
  Kento Hasegawa, Kazuki Yamashita, Seira Hidano, Kazuhide Fukushima, Kazuo Hashimoto, Nozomu Togawa
- Analysing Utility Loss in Federated Learning with Differential Privacy
  Anastasia Pustozerova, Jan Baumbach, Rudolf Mayer
- Ripple20 Vulnerabilities Detection using a Featureless Deep Learning Model
  Sarah Bin hulayyil, Shancang Li
- EPPVChain: An Efficient Privacy-Preserving Verifiable Query Scheme for Blockchain Databases
  Jingxian Cheng, Saiyu Qi, Yong Qi, Jianfeng Wang, Qin Jiang, Di Wu

13:30-15:45 Session ITCCN-6: Network and System Security (I) (Room: Online Room 3)

Session Chair: Xiaoding Wang, Fujian Normal University, China

- The Impact of EMI on Security Access Control in Datacenter Data Halls
  Shahriar Saadat
- Physical Layer Secure Communication based on MIMO Channel Constellation Flipping
  Tong Gao, Xianhui Lu
- Channel-Robust Radio Frequency Fingerprint Identification for LTE Devices with Hybrid Feature
  Haichuan Peng, Linning Peng, Hua Fu, Lingnan Xie, Junxian Shi, Wentao Jing
- Zero Trust Score-based Network-level Access Control in Enterprise Networks
  Leonard Bradatsch, Oleksandr Miroshkin, Nataša Trkulja, Frank Kargl
- Enhancing IoT Security: Novel Mechanisms for Malware Detection using HPCs and Neural Networks
  Shashwat Adhikari, Hafizul Asad, Kevin Jones
- Guardians of DNS Integrity: A Remote Method for Identifying DNSSEC Validators Across the Internet
  Yevheniya Nosyk, Maciej Korczynski, Andrzej Duda
- A Novel Approach for Trajectory Partition Privacy in Location-Based Services
  Chundong Wang, Yongxin Zhao
- Don't Get Hijacked: Prevalence, Mitigation, and Impact of Non-Secure DNS Dynamic Updates
  Yevheniya Nosyk, Maciej Korczynski, Carlos Hernandez Gañán, Michał Król , Qasim Lone, Andrzej Duda
- Network Attack Identification and Analysis Based on Graph Convolutional Neural Network
  Xingyu Wang, Kun Wen, Yingdan Zhang

16:00-18:00 Session ITCCN-2: Computer and Data Security (I) (Room: Devonshire B)

Session Chair: Kalam Khadka, University of Canberra, Australia

- Survey of Malware Analysis through Control Flow Graph using Machine Learning
  Shaswata Mitra, Stephen A. Torri, Sudip Mital
- Secure Traversable Event logging for Responsible Identification of Vertically Partitioned Health Data
  Sunanda Bose, Dusica Marijan
- Apt Detection of Ransomware - An Approach to Detect Advanced Persistent Threats Using System Call Information
  Rudra Prasad Baksi, Vishwas Nalka, Shambhu Upadhyaya
- A Survey on Principles of Persuasion as a Social Engineering Strategy in Phishing
  Kalam Khadka, Abu Barkat Ullah, Wanli Ma, Elisa Martinez Marroquin, Yibe Alem
- WiDeS: Wiping Detection using System-calls - An Anti-Forensic Resistant Approach
  Pranitha Sanda, Digambar Pawar, Radha Vedala
- Model-Driven Security Analysis of Self-Sovereign Identity Systems
  Yepeng Ding, Hiroyuki Sato
- ECC Implementation and Performance Evaluation for Securing OPC UA Communication
  Alexandra Tidrea, Adrian Korodi
- Dynamic Scheduling of AES Cores for Aperiodic Tasks on Multi-tenant Cloud FPGAs
  Stephen Donchez, Xiaofang Wang

16:00-18:15 Session ITCCN-7: Trustworthy and Secure AI (Room: Online Room 3)

Session Chair: Songyuan Li, University of Exeter, UK

- ConFunc: Enhanced Binary Function-Level Representation through Contrastive Learning
  Longfei Li, Xiaokang Yin, Xiao Li, Xiaoya Zhu, Shengli Liu
- TGCN-DA: A Temporal Graph Convolutional Network with Data Augmentation for High Accuracy Insider Threat Detection
  Ximing Li, Linghui Li, Xiaoyong Li, Binsi Cai, Bingyu Li
- EFwork: An Efficient Framework for Constructing a Malware Knowledge Graph
  Chen Chen, Chunhe Xia, Tianbo Wang, Wanshuang Lin, Yuan Zhao, Yang Li
- Temporal-Gated Graph Neural Network with Graph Sampling for Multi-step Attack Detection
  Shuyu chen, Dawei Lin, Zhenping Xie, Hongbo Wang
- GBTrust: Leveraging Edge Attention in Graph Neural Networks for Trust Management in P2P Networks
  Badr BELAJ, Aafaf OUADDAH, Abdelattif Mezrioui, Noel Crespi, Emmanuel BERTIN
- On-graph Machine Learning-based Fraud Detection in Ethereum Cryptocurrency Transactions
  Helen Milner, Redowan Mahmud, Mahbuba Afrin, Sashowta G. Siddhartha, Sajib Mistry, Aneesh Krishna
- CWGAN-GP: Fuzzing Testcase Generation Method based on Conditional Generative Adversarial Network
  Zhongyuan Qin, Jiarong Fan, Zeru Li, Xujian Liu, Xin Sun
- Malware Detection Using Contrastive Learning Based on Multi-Feature Fusion
  Kailu Guo, Yang Xin, Tianxiang Yu
- A Trustworthiness Evaluation Mechanism Based on Beta Distribution Under Selected Condition
  Kewei Guo, Xuefei Li

2 November 2023 Thursday

13:30-15:30 Session ITCCN-3: Internet-of-Things (Room: Devonshire B)

Session Chair: Rudra Prasad Baksi, Illinois State University, USA

- UAV Bluetooth Communication Link Assessment for Emergency Response Applications
  Brendan Black, Joseph Rafferty, Jose Santos, Andrew Ennis
- IoT Device Lifecycle Management
  Nektarios Georgalas, Andrew Ennis, Cathryn Peoples, Joseph Rafferty, Philip Perry, Claudia Cristina, Brendan Black, Adrian Moore, Tom Bowman, Bryan Scotney, Andrew Reeves
- Actionable Contextual Explanations for Cyber-Physical Systems
  Sanjiv Subodhnarayan Jha, Simon Mayer, Kimberly Garcia
- Proactive Device Management for the Internet of Things
  Tom Bowman, Nektarios Georgalas, Andrew Reeves, Andrew Ennis, Cathryn Peoples, Brendan Black, Fadi El-Moussa, Adrian Moore
- A Dynamic Network-based Intrusion Detection Model for Industrial Control Systems
  PPaulo R. de Oliveira, Altair O. Santin, Pedro Horchulhack, Eduardo K. Viegas, Everton de Matos
- An Interactive Web Portal for Customised Telerehabilitation in Neurological Care
  M A Hannan Bin Azhar, Zoltán Mészáros, Tasmina Islam, Soumya Kanti Manna
- Matrix Platform: Empowering Smart Ports with Advanced Video Analytics for Enhanced Security, Safety, and Efficiency
  Brendan Black, Philip Perry, Joseph Rafferty, Claudia Cristina, Tom Bowman, Cathryn Peoples, Andrew Ennis, Andrew Reeves, Nektarios Georgalas, Adrian Moore, Bryan Scotney
- A Comparative Analysis of Federated Learning Techniques on On-Demand Platforms in Supporting Modern Web Browser Applications
  Muhammad Senoyodha Brennaf, Po Yang, Vitaveska Lanfranchi

13:30-15:45 Session ITCCN-8: Computer and Data Security (II) (Room: Online Room 3)

Session Chair: Yuhong Jiang, University of Exeter, UK

- CamPass: a Secure Camera-based Password Manager for Kiosk Browsing
  Rui Zhao
- Generating Optimized Universal Adversarial Watermark for Preventing Face Deepfake
  Kaiqi Lv, Weiguo Lin, Junfeng Xu, Wanshan Xu, Shuren Chen, Shengwei Yi
- Keyword Spotting in the Homomorphic Encrypted Domain Using Convolution Decomposition
  Chenyu Dong, Peijia Zheng, Weiqi Luo
- Semantic-Driven Focused Crawling Using LASER and FAISS: A Novel Approach for Threat Detection and Improved Information Retrieval
  Prasasthy Balasubramanian, Justin Seby, Panos Kostakos
- Code Execution Capability as a Metric for Machine Learning-Assisted Software Vulnerability Detection Models
  Daniel Grahn, Lingwei Chen, Junjie Zhang
- A Fine-Grained Access Control Mechanism Based on Search Trees
  Xianxia Zou, Cenyu Zheng, Haodong Lin, Like Du, Weiwu Xu, Chong He
- Challenges and Considerations in Data Recovery from Solid State Media: A Comparative Analysis with Traditional Devices
  Aidan Spalding, Zhiyuan Tan, Kehinde O. Babaagba
- Dynamic Searchable Scheme with Forward Privacy for Encrypted Document Similarity
  Mustafa A. Al Sibahee, Chengwen Luo, Jin Zhang, Yijing Huang, Zaid Ameen Abduljabbar
- LiPI: Lightweight Privacy-Preserving Data Aggregation in IoT
  Himanshu Goyal, Krishna Kodali, Sudipta Saha

16:00-18:00 Session ITCCN-4: Network and System Security (II) (Room: Devonshire B)

Session Chair: Xiaohua Feng, University of Bedfordshire, UK

- Access Control based on CRDTs for Collaborative Distributed Applications

Pierre-Antoine Rault, Claudia-Lavinia Ignat, Olivier Perrin

- Putting a Padlock on Lambda - Integrating vTPMs into AWS Firecracker
  Melker Veltman, Alexandra Parkegren, Victor Morel
- Phish and Chips: Language-agnostic classification of unsolicited emails
  Carlos H. Ganan, Siôn Lloyd, Samaneh Tajalizadehkhoob
- Evaluation of Decision Tree-Based Rule Derivation for Intrusion Detection in Automotive Ethernet
  Felix Gail, Roland Rieke, Florian Fenzl, Christoph Krauß
- A Contextual Derivation Algorithm for Cybersecurity in IoT Environments
  Abdul Qadir Khan, Nouredine Tamani, Saad El Jaouhari, Lina Mroueh
- Generating Synthetic Tabular Data for DDoS Detection Using Generative Models
  Samed Saka, Ali Al-Ataby, Valerio Selis
- TorKameleon: Improving Tor's Censorship Resistance with K-anonymization and Media-based Covert Channels
  Afonso Vilalonga, João S. Resende, Henrique Domingos
- Attacks Against Mobility Prediction in 5G Networks
  Syafiq Al Atiiq, Yachao Yuan, Christian Gehrmann, Jakob Sternby, Luis Barriga

16:00-18:45 Session ITCCN-9: Emerging Technologies (Room: Online Room 3)

Session Chair: Yuhong Jiang, University of Exeter, UK

- CGPNet: Enhancing Medical Image Classification through Channel Grouping and Partial Convolution Network
  Kairen Chen, Shuhong Chen, Guojun Wang, Chenchen Wang
- DOPS: A Practical Dual Offline Payment Scheme of CBDC for Mobile Devices
  Bo Yang, Yanchao Zhang, Dong Tong
- Android Malicious Application Detection Based on Improved Mayfly Algorithm
  Yin Zhen Wei, Shuo Lu
- Game Theory-Based Trade-Off Analysis for Privacy and Openness in Decision Making by Controlling Quantity of Information
  Mohd Anuaruddin Bin Ahmadon, Shingo Yamaguchi, Alireza Jolfaei
- Leveraging Hardware Performance Counters for Efficient Classification of Binary Packers
  Erika Leal, Binlin Cheng, TuQuynh Nguyen, Alfredo Gutierrez Garcia, Nathan Cabero, Jiang Ming
- Python Subset to Digital Logic Dataflow Compiler for Robots and IoT
  Kristaps Jurkans, Charles Fox
- I2Map: IoT Device Attestation Using Integrity Map
  Imran Makhdoom, Mehran Abolhasan, Justin Lipman, Daniel Franklin, Massimo Piccardi
- A Near-Field EM Sensor Implemented in FPGA Configurable Fabric
  Can Aknesil, Elena Dubrova, Niklas Lindskog, Håkan Englund
- Trust Assessment of a Darknet Marketplace
  Florian Platzer, York Yannikos
- Automatic Scam-Baiting Using ChatGPT
  Piyush Bajaj, Matthew Edwards
- A Comprehensive Machine Learning Methodology for Embedded Systems PHM
  Juliano Pimentel, Alistair A. McEwan, Hong Qing Yu

3 November 2023 Friday

9:00-10:30 Session ITCCN-5&IUCC-2: Reliable Distributed System (Room: Burlington)

Session Chair: Chai Luo, China University of Petrolem, China

- Pooling Under the Sun: A Mining Pool Centralized Revisit and Solution
  Kundu Chen, Jie Luo
- A Practical and Privacy-Preserving Vehicular Data Sharing Framework by Using Blockchain
  Xu Yang, Ao Wang, Qiuhao Wang, Saiyu Qi, Yong Qi
- Enhancing Tunnel Safety for Dangerous Goods Vehicles through Blockchain-Based Time-Stamping
  Karolina Bak, Hannes Salin, Karol Niczyj, Lukasz Krzywiecki
- A reliable edge server placement strategy based on DDPG in the Internet of Vehicles
  Zhou Zhou, Yonggui Han, Mohammad Shojafar, Zhongsheng Wang, Jemal Abawajy
- Tabular Generative Adversarial Networks with an Enhanced Sampling Approach for High-Quality Cardiovascular Disease Dataset Generation
  Malak Alqulaity, Po Yang
- A Deep Learning Model for Mobility Change Prediction Based on National Prevention and Control Policy
  Shifeng Li, Ruoling Peng, Po Yang, Yun Yang

9:00-10:45 Session ITCCN-10: Network and System Security (III) (Room: Online Room 3)

Session Chair: Tong Ding, Shandong University, China

- Be like a Chameleon: Protect Traffic Privacy with Mimicry
  Zexiao Zou, Yan Zhang, Jin Chen, Jianyi Zhang, Zhiqiang Wang, Lei Ju, Ri Xu
- Analysis and Comparison of Delay Tolerant Network Security Issues and Solutions
  Jingwen Su, Xiangyu Bai, Kexin Zhou
- Securing Zero Trust Networks: the Decentralized Host-to-Host Authentication Policy Enforcement
  Adam Spanier, Rui Zhao, Pei-Chi Huang
- Protocol Aware Unsupervised Network Intrusion Detection System
  Ritesh Ratti, Sanasam Ranbir Singh, Sukumar Nandi
- A Public Key Infrastructure for 5G Service-Based Architecture
  Ayush Kumar, Vrizlynn L.L. Thing
- Access control for interoperable energy management systems using Verifiable Credentials
  Nikos Fotiou, Spiros Chadoulos, Iordanis Koutsopoulos, Vasilios A. Siris, George C. Polyzos
- HF-Mid: A Hybrid Framework of Network Intrusion Detection for Multi-type and Imbalanced Data
  Weidong Zhou, Tianbo Wang, Guotao Huang, Xiaopeng Liang, Chunhe Xia, Xiaojian Li

11:00-13:30 Session ITCCN-11: Blockchain and Cryptography (Room: Online Room 3)

Session Chair: Ayush Kumar, ST Engineering, Singapore

- Referable NFT-based Revenue Allocation Mechanism in Data Marketplace
  Hui Zhao, Xiaodong Zhang, Jinshan Shi, Ru LI
- A Secure Blockchain-based Authentication and Key Agreement Protocol for 5G Roaming
  Awaneesh Kumar Yadav, Manoj Misra, An Braeken, Madhusanka Liyanage
- Chrisimos: A useful Proof-of-Work for finding Minimal Dominating Set of a graph
  Diptendu Chatterjee, Prabal Banerjee, Subhra Mazumdar
- Blockchain-based and Privacy-Preserving Data Collection for Vehicular Crowdsensing
  Xionghe Yu, Xiaolan Tang, Wenlong Chen
- BC-FL k-means: A Blockchain-based Framework for Federated Clustering
  Mina Alishahi, Wouter Leeuw, Nicola Zannone
- Secure Decentralized Identity Management using Blockchain
  Sandeep Srivastava, Deepshikha Agarwal, Brijesh Chaurasia
- A Novel Blockchain-based Decentralized Multi-party Certificate Management Framework

Shalitha Wijethilaka, Awaneesh Kumar Yadav, An Braeken, Madhusanka Liyanage

- Practical Privacy-Preserving Ride Sharing Protocol with Symmetric Key
  Sara Ramezanian, Christian Gehrmann
- ChainPass: A Privacy-preserving Complete Cross-chain Authentication for Consortium Blockchains
  Yuwei Xu, Ying Zhang, Haonan Shi, Jie Cao
- Inj-Kyber: Enhancing CRYSTALS-Kyber with Information Injection within a Bio-KEM Framework
  Junwei Yu, Yepeng Ding, Yuheng Guo, Kentaro Kotani, Hiroyuki Sato

ACE-2023 TECHNICAL SESSION

1 November 2023 Wednesday

16:00-18:00 Session ACE-1: Applications of AI, Cyber Security and Economics Data Analytics (Room: Burlington)

Session Chair: Xiaohua Feng, University of Bedfordshire, UK

- Keynote: Cyberstalking: Reflections on the evolution of fixated online intrusions
  Dr Emma Short, London Metropolitan University
- Detecting Masquerading Traitors from Process Visualization of Computer Usage
  Martin Macakl, Radek Oslejsek, Barbora Buhnova
- *A Computing Education Challenge on Information Retrieval Impact and Pedagogic Research*
  Xiaohua Feng
- Cybersecurity Human Factors
  Xiaohua Feng, E. Dawam

BDRA-2023 TECHNICAL SESSIONS

1 November 2023 Wednesday

13:30-16:00 Session BDRA-1: Big Data Application (Room: Online Room 4)

Session Chair: Lexi Xu, China Unicom, China

- Multi-Granularity Cross-Attention Network for Visual Question Answering
  Yue Wang, Wei Gao, Xinzhou Cheng, Xin Wang, Huiying Zhao, Zhipu Xie, Lexi Xu
- An Analysis Strategy of Abnormal Subscriber Warning Based on Federated Learning Technology
  Jie Gao, Tianyi Wang, Yuhui Han, Lixia Liu, Xingwei Zhang, Lexi Xu, Yang Wu, Zijing Yang, Chen Cheng
- Medical Image Recognition Technology Based On Fusion Of Faster-RCNN And SSD
  Yuwen Huo, Song Wu, Mingde Huo
- Vulnerability Name Prediction Based on Enhanced Multi-Source Domain Adaptation
  Ying Xing, Mengci Zhao, Bin Yang, Yuwei Zhang, Wenjin Li, Jiawei Gu, Jun Yuan, Lexi Xu
- An AI-driven Dockerized Lightweight Framework for Smart Home Service Orchestration
  Zhaoning Wang, Jiajia Zhu, Bo Cheng, Xinzhou Cheng, Feibi Lyu, Guoping Xu, Jinjian Qiao, Lu Zhi, Tian Xiao
- Proactive Operation and Maintenance for 5G Networks Based on Complaint Prediction
  Feibi Lyu, Ning Meng, Yuhui Han, Jinjian Qiao, Zhipu Xie, Xinzhou Cheng, Lexi Xu, Zhaoning Wang, Guoping Xu
- Automatic Intelligent Chronic Kidney Disease Detection in Healthcare 5.0
  Geng Tian, Amir Rehman, Huanlai Xing, Li Feng, Nighat Gulzar, Abid Hussain

- TrustedBench: An efficient and user-friendly distributed performance testing tool for blockchain system
  Yang Cheng, Kai Wei, Yihui Zhang, Chunyu Jiang, Weiwei Pang, Qi Zhang, Bin Liu, Lifeng Zhang, Tingting Liu, Yinqian Wu
- Assessing the Value of Data Assets: An Exploratory Study of Valuation Methods
  Bohuan Ai, Yufei Li, Wenda Ma, Mengyuan Qiu, Miao Liu
- A Cooperative Lane Change Method for Connected and Automated Vehicles Based on Reinforcement Learning
  Fanqiang Meng, Jian Wang, Boxiong Li

16:00-18:30 Session BDRA-2: Big Data Research (Room: Online Room 4)

Session Chair: Zhe Wang, University of Exeter, UK

- Research on Enterprises Growth for Industries in Post-Epidemic Era
  Heng Zhang, Bing Yan, Yunpeng Li, Lexi Xu, Xinzhou Cheng, Lijuan Cao, Kun Chao, Wei Xia, Qinqin Yu
- Research on Data Security for Vehicle-Infrastructure-Cloud Integration
  Yunlu Yang, Miaoqiong Wang, Yuming Ge, Rundong Yu
- Research on DataOps Capability - Practice and Development
  Zheng Yin, Shengwen Zhou, Jingjing Zhou, Minghui Tian, Musen Lin
- Research on Operation Evolution of 5G Non-Public Network
  Kun Chao, Zhen Xing, Xinzhou Cheng, Jian Guan, Lexi Xu, Xiqing Liu, Yuwei Jia, Lijuan Cao
- Research on Diagnosis System of 5G Data Service Latency Problem
  Jinjian Qiao, Guoping Xu, Ning Meng, Feibi Lyu, Xinzhou Cheng, Jiajia Zhu, Lexi Xu, Liang Liu
- Research on Assessment System for Blockchain
  Weiwei Pang, Kai Wei, Yihui Zhang, Chunyu Jiang, Yang Cheng, Qi Zhang, Bin Liu, Lifeng Zhang, Tingting Liu, Yinqian Wu
- Development Situation and Suggestions of Data Elements in China
  Shu Yan, Sirui Zhang, Ailin Lv, Bo Yuan, Kai Wei
- Research on Technology and Industry Situation of Lakehouse
  Yanmei Liu, Pengwei Ma, Jiafeng Tian
- Research on Technologies in Data Fabric
  Qingyuan Hu, Zheng Yin, Tao Tao, Jibin Wang, Zhuo Chen, Bohuan Ai, Yu Liu, Chongzhou Liu
- Research On Development of Data disaster Recovery System
  Jiafeng Tian, Pengwei Ma, Chaolun Wang, Zhuo Wang

AINet-2023 TECHNICAL SESSION

2 November 2023 Thursday

13:30-16:00 Session AINet-1: AI-driven Network (Room: Online Room 4)

Session Chair: Lexi Xu, China Unicom, China

- Design and Implementation of Digital Consulting Capability Platform based on Knowledge Sharing
  Zhen Guo, Pengzhou Zhang, Lexi Xu, Peng Liang, Shuwei Yao
- RedCap In-depth Research and Market Development Prospect
  Jinhu Shen, Rui Wang, Mingjie Yang, Liang Cui, Ao Shen, Bao Guo, Jiayu Li, Yuan Fang, Pengcheng Liu, Jimin Ling
- Research on Interpretable Customer Churn Prediction Based on Attention Mechanism

Bin Yang, Jing Liang, Yubin Chen, Ying Xing, Wei Gao, Yue Wang, Lexi Xu, Xinzhou Cheng

- Method for Dual-path Upgrade in a Leaked Signal Indoor Distribution System in 5G Network
  Bao Guo, Lufei Zhang, Jinge Guo, Jinhu Shen, Shumin Jiang, Pengcheng Liu
- SSF-EDZL Scheduling Algorithm On Heterogeneous Multiprocessors
  Peng Wu, Chengzhuo Han, Tao Yan, Lu Chen, Tianhao Guo, Zhi Li
- Evaluation of Distributed Collaborative Learning Approach For 5G Network Data Analytics Function
  Shoufeng Wang, Hua-Min Chen, Ye Ouyang, Fan Li, Xuan Chen, Limeng Ma, Zhanwu Li, Sen Bian, Zhidong Ren
- Research on Cross-Layer Alarm Association in 5G Core Network
  Dongyue Zhang, Sai Han, Zelin Wang, Jingwei Wang, Guangquan Wang, Jieyan Yang
- The Research and Implementation of Optical Cable Fault Location Method Based on Navigation
  Ao Li, Sai Han, Zelin Wang, Guangquan Wang, Zhi Qiao, Songtao Ni
- User Relationship Discovery Based on Telecom Data
  Yue Wang, Wei Gao, Xinzhou Cheng, Xin Wang, Lexi Xu, Siwei Wang, Yuanguang Wang, Fanyu Meng, Kunyan Li
- A Bigdata Sharing Architecture Based on Federal Learning in State Grid
  Liu Na, Rui Yang, Zhicheng Zang, Yu Wang, Chao Wu, Xiaofei Li, Zhendong Li, Meng Li

MLSys-2023 TECHNICAL SESSION

2 November 2023 Thursday

16:00-18:30 Session MLSys-1: Machine Learning assisted Smart System (Room: Online Room 4)

Session Chair: Jinming Wang, University of Exeter, UK

- Leveraging Oversampling Techniques in Machine Learning Models for Multi-class Malware Detection in Smart Home Applications
  Abdullahi Chowdhury, Mohammad Manzurul Islam, Shahriar Kaisar, Mahbub E Khoda, Ranesh Naha, Mohammad Ali Khoshkholghi, Mahdi Aiash
- EasyOrchestrator: A Dynamic QoS-Aware Service Orchestration Platform for 6G network
  Yi Yue, Zhiyan Zhang, Chang Cao, Xiongyan Tang, Wencong Yang, Feile Li
- A Novel Algorithm and System of Customer Value Evaluation based on Telecom Operator Big Data
  Chen Cheng, Xinzhou Cheng, Jinyou Dai, Xu Xia, Bin Yang, Feibi Lyu, Jie Gao, Wei Zhang, Tian Xiao, Tianyi Wang
- 5G/5G-A Private Network: Construction, Operation and Applications
  Lexi Xu, Junsheng Zhao, Hong Zhu, Mingde Huo, Xinzhou Cheng, Kun Chao, Jie Li, Jian Guan, Xiqing Liu, Jie Gao
- Elastic Digital Twin Network Modeling toward Restraining Resource Occupation
  Shoufeng Wang, Hua-Min Chen, Ye Ouyang, Fan Li, Xuan Chen, Jianchao Guo, Yun Li, Sen Bian, Xidong Wang, You Lu
- An Improved Lightweight Linear K-value Transformer
  Anyan Xiao, Zhuo Yan, Zheng Li, Huangxin Xu, Huixuan Zheng, Yujie Ai, Xiaocong Zhang, Qixuan Sun, Changyu Zhao
- FedQuant: Stock Prediction with Muti-Party Technical Indicators using Federated Learning Method in Quantitative Trading
  Zijing Yang, Lexi Xu, Jie Gao, Jie Li, Yang Wu, Xinzhou Cheng
- Design and Implementation of Mask Detection System Based on Improved YOLOv5s

Changyu Zhao, Zhuo Yan, Huangxin Xu, Xueliang Chen, Zheng Li, Xinyu Zhong, Cuiwei Liu, Anyan Xiao, Xingyan Lv

- Address Localization Method Based on Data Fusion of Core Network and Radio Access Network
  Tianyi Wang, Yuhui Han, Wei Zhang, Xinzhou Cheng, Jie Gao, Qijiao Yang, Fengqiang Chen, Chen Cheng
- FLEvaluate: Robust Federated Learning Based on Trust Evaluate
  Chao Guo, Buxin Guo, Tingting Zhu, Peihe Liu, Cheng Gong

SAGIINAT-2023 TECHNICAL SESSIONS

3 November 2023 Thursday

9:00-10:45 Session SAGIINAT-1: Advanced Technology for Space-Air-Ground Integrated Information Networks (Room: Online Room 4)

Session Chair: Cheng Wang, Beijing University of Posts and Telecommunications, China

- Deep Reinforcement Learning Based Interference Avoidance Beam-Hopping Allocation Algorithm in Multi-beam Satellite Systems
  Haonan Wang, Lixiang Liu, Xin Zhou, Lexi Xu, Guangyang Wu, Shuaijun Liu
- A low complexity and efficient algorithm for LEO satellite routing
  Hao Wang, Yun Liu, Zhiqun Song, Bing Hu, Zikai Wang, Ruiliang Song, Pei Xiao
- Multiple Chord Distance Regression Algorithm to Judge Constellations Without Prior Information
  Wenli Yan, Shuaijun Liu, Lixiang Liu
- Simulation of Space-borne Digital Phased Array Anntenna
  Jifeng Liu, Yao Zhou, Cheng Wang, Yingnan Liu, Fuchang Li
- Optimization Method for LEO Constellation Frequency Compatibility Simulation Parameters
  Gao Xiang, Fu Jiangyin, Yao Xiujuan, Yan Yi
- Coexistence Analysis Between the Large-scale IMT systems and LEO Satellite communication systems
  Yuqian Cai, Cheng Wang, Xiaoqian Wang, Xiaoyan Zhao, Weidong Wang
- Coexistence Analysis of 10-10.5 GHz IMT and EESS (passive) Systems
  Xiaoqian Wang, Cheng Wang, Yuqian Cai, Xiaoyan Zhao, Weidong Wang

11:00-13:00 Session SAGIINAT-2 & AINet-2 & MLSys-2: Heterogenouse Network and Machine Learning System (Room: Online Room 4)

Session Chair: Cheng Wang, Beijing University of Posts and Telecommunications, China

- Constellation Autonomy Modeling for Agile on-Orbit Communication and Computing
  Shoufeng Wang, Hua-Min Chen, Ye Ouyang, Fan Li, Xuan Chen, Jianchao Guo, Yun Li, Sen Bian, Xidong Wang, Zhidong Ren
- Service-Driven Shared QoS Orchestration for Satellite-Ground Integrated Networks
  Lin Lin, Bin Zhu, ZeLin Wang, Guangquan Wang, Kaichu Xing
- Analyzing Land Cover and Land Use Changes Using Remote Sensing Techniques: A Temporal Analysis of Climate Change Detection with Google Earth Engine
  Mozina Afzal, Kamran Ali, Mumraiz Khan Kasi, Masood Ur Rehman, Mohammad Ali Khoshkholghi, Bushra Haq, Syed Ahmed Shah
- Application Scenarios of Confidential Computing in Satellite Internet
  Jie Ren, Lin Lin, Miao Xue, Zelin Wang
- Research on the Construction of Information System Stability Guarantee Capability
  Pengwei Ma, Chaolun Wang

- Research on Distributed Database Stability Testing Platform based on Chaos Engineering
  Chaolun Wang, Jiaxing Yang, Xiaolu Han, Jianrui Ma, Siyuan Liu, Pengwei Ma
- A Novel Uplink Coverage and Capacity Enhancement Scheme in NR TDD Network
  Bao Guo, Jinge Guo, Lufei Zhang, Yuan Fang, Yingtao Meng, Jiayu Li
- Smart Campus Construction based on Telecom Operators Big Data
  Runsha Dong, Xiaodong Cao, Chao Wang, Zhaoyang Sun, Lexi Xu, Xin He, Yang Wu

CAI-2023 TECHNICAL SESSION

3 November 2023 Friday

11:00-12:30 Session CAI-1 & ACE-2 & CSE-4: Secure and Intelligent Systems (Room: Burlington)

Session Chair: Haozhe Wang, University of Exeter, UK

- Stealthy Rootkits vs Low-Power IoT Devices: A Process-level Colonel Blotto Game
  Talal Halabi
- MOFP: Multi-Objective Filter Pruning for Deep Learning Models
  Jen-Chieh Yang, Hung-I Lin, Lin-Jing Kuo, Sheng-De Wang
- Literature Study on Bias & Fairness in ML Learning Systems
  Qaizar Bamboat, Hong Qing Yu
- A Hybrid Filter Pruning Method Based on Linear Region Analysis
  Chang-Hsuan Hsieh, Jen-Chieh Yang, Hung-Yi Lin, Lin-Jing Kuo, Sheng-De Wang
- Increasing user seduction in e-commerce community interaction using the participation continuum
  Jonathan Bishop, Ashu M.G. Solo
- Soft Hybrid Filter Pruning using a Dual Ranking Approach
  Peng-Yu Chen, Jen-Chieh Yang, Sheng-De Wang

CSE & BigDataSE & iSCI-2023 TECHNICAL SESSIONS

1 November 2023 Wednesday

13:30-15:30 Session CSE-1 & BigDataSE: Computational Science (I) (Room: Burlington)

Session Chair: Chase Wu, New Jersey Institute of Technology, USA

- Control Overhead Reduction using Length-based Same Destination Aggregation for Large Scale Software Defined Networks in Next Generation Internet of Things
  Mohammad Shahzad, Lu Liu, Nacer Belkout
- Optimizing Quantum Reversible Circuits Using Reinforcement Learning
  Sheng Yang, Guan-Ju Peng
- KrNER: A Novel Named Entity Recognition Method Based on Knowledge Enhancement and Remote Supervision
  Jinhua Du, Hao Yin
- Comparison of the Barriers to BIM Adoption and Digital Transformation within the Construction Industry of Pakistan and Ireland
  Adhban Farea, Moaaz Munir, Rahat Ullah, Michal Otreba, Sean Carroll, Joe Harrington
- Quantum Inspired Binary Atom Search Optimization Algorithm for Charging Station Placement Problem
  Madathodika Asna, Hussain Shareef, Achikkulath Prasanthi
- KLDP: A Data Profiling Technique Based on Knowledge Graph and Large Language Modeling

Jinhua Du, Hao Yin

- Ensemble Learning Models for Large-Scale Time Series Forecasting in Supply Chain
  Minjuan Zhang, Chase Wu, Aiqin Hou
- Fast Fluid Antenna Multiple Access with Path Loss Consideration and Different Antenna Architecture
  Halvin Yang, Xiao Lin, Kai-Kit Wong, Yizhe Zhao

3 November 2023 Friday

9:00-10:45 Session CSE-2 & iSCI: Computational Engineering (Room: Online Room 5)

Session Chair: Adhban Farea, Munster Technological University, Ireland

- Towards Reliable Collaborative Data Processing Ecosystems: Survey on Data Quality Criteria
  Louis Sahi, Romain Laborde, Mohamed-Ali Kandi, Michelle Sibilla, Giorgia Macilotti, Benzekr Abdelmaleki, Afonso Ferreira
- Railway Traffic Signal Recognition System based on Spatio-Temporal Features
  Haohan Zhu, Andrea Staino, Biswajit Basu
- A Large-scale Non-standard English Database and Transformer-based Translation System
  Arghya Kundu, Uyen Trang Nguyen
- Clupiter: a Raspberry Pi mini-supercomputer for educational purposes
  Alonso Rodríguez-Iglesias, María J. Martín, Juan Touriño
- Transparent network acceleration for big data computing in Java
  Fabian Ruhland, Filip Krakowski, Michael Schöttner
- Towards a Context-based Mobility Prediction in Smart Cities: First Experimentations
  Boukhedouma Hocine, Meziane Abdelkrim, Hammoudi Slimane, Benna Amel, Hadjali Allel
- Ax-to-Grind Urdu: Benchmark Dataset for Urdu Fake News Detection
  Sheetal Harris, Jinshuo Liu, Hassan Jalil Hadi, Yue Cao

11:00-13:45 Session CSE-3 & ITCCN-14: Computational Science and Secure Systems (II) (Room: Online Room 5)

Session Chair: Yuhong Jiang, University of Exeter, UK

- Fast Text Classification using Lean Gradient Descent Feed Forward Neural Network for Category Feature Augmentation
  Joseph Attieh, Joe Tekli
- Hybrid Multi-Objective Relinked GRASP for the constrained Next Release Problem
  Víctor Pérez-Piqueras, Pablo Bermejo, José A. Gámez
- Stabilized Finite Element Approximation for The Transient Darcy-Brinkman-Forchheimer Model
  Rafael Cabral de Moura, Lucia Catabriga
- Histopathological Image Classification and Vulnerability Analysis using Federated Learning
  Sankalp Vyas, Amar Nath Patra, Raj Mani Shukla
- High-Performance Object Serialization based on Ahead-of-Time Schema Generation
  Filip Krakowski, Fabian Ruhland, Michael Schöttner
- MD-SCS: A Dynamic Behavioral Approach for Early Malware Detection with Sonification of System Call Sequences
  Raghav Bhardwaj, Morteza Noferesti, Madeline Janecek, Naser Ezzati-Jivan
- On the Adoption of Homomorphic Encryption by Financial Institutions
  Michela Iezzi, Carsten Maple, Danilo A. Giannone
- Anomaly based malware threat detection on Linux Systems
  Jayanthi Ramamoorthy, Narasimha K. Shashidhar, Bing Zhou
- A novel network flow feature scaling method based on cloud-edge collaboration

Zeyi Li, Ze Zhang, Mengyi Fu, Pan Wang

- Quantifying Nematodes through Images: Datasets, Models, and Baselines of Deep Learning
  Zhipeng Yuan, Nasamu Musa, Katarzyna Dybal, Matthew Back, Daniel Leybourne, Po Yang
- Give and Take: Federated Transfer Learning for Industrial IoT Network Intrusion Detection
  Lochana Telugu Rajesh, Tapadhir Das, Raj Mani Shukla, Shamik Sengupta

EUC-2023 TECHNICAL SESSIONS

3 November 2023 Friday

9:00-10:30 Session EUC-1: Ubiquitous Computing and Systems (Room: Chartsworth)

Session Chair: Hannan Azhar, Canterbury Christ Church University, UK

- HMAS: enabling seamless collaboration between drones, quadruped robots, and human operators with efficient spatial awareness
  Amaury Saint-Jore, Ye-Qiong Song, Laurent Ciarletta
- Dynamic Split Computing-Aware Mixed-Precision Quantization for Efficient Deep Edge Intelligence
  Naoki Nagamatsu, Yuko Hara-Azumi
- A Mobile-First Disconnected Data Distribution Network
  Shashank Hegde, Deepak Munagala, Aditya Singhania, Ben Reed
- Trustworthy Insights: A Novel Multi-Tier Explainable Framework for Ambient Assisted Living
  Merlin Kasirajan, M A Hannan Bin Azhar, Scott Turner

11:00-12:30 Session EUC-2 : Embedded Computing and Systems (Room: Chartsworth)

Session Chair: Zi Wang, University of Exeter, UK

- Model-based Development for ROS 2-based Autonomous-driving Software
  Takumi Onozawa, Hiroshi Fujimoto, Takuya Azumi
- Simulation for Trade-off between Interference and Performance in a Bluetooth Low Energy Network
  Bozheng Pang, Tim Claeys, Kristof T'Jonck, Jens Vankeirsbilck, Hans Hallez, Jeroen Boydens
- Experimental Validation of Common Assumptions in Bluetooth Low Energy Interference Studie
  Bozheng Pang, Jens Vankeirsbilck, Hans Hallez, Jeroen Boydens
- Performance Evaluation Framework for Arbitrary Nodes of Autonomous-driving Systems
  Yuta Tajima, Tatsuya Miki, Takuya Azumi

Part II: TECHNICAL SESSIONS OF IUCC/CIT/DSCI/SmartCNS-2023

IUCC-2023 TECHNICAL SESSION

3 November 2023 Friday

11:00-13:45 Session IUCC-1 & ITCCN-12: Ubiquitous Systems and Trustworthy Computing (Room: Online Room 6)

Session Chair: Jie Gao, University of Exeter, UK

- Pollutant Concentration Prediction Based on the Optimization of Long-Short Distance in Space
  Muyao Peng, Kun Wang, Yueli Wen
- Design and Implementation of Intelligent Pet Feeding System
  Qi Li, Xinqi Shen, Zhongkai Cheng, Yu Liu
- Software defined networking flow admission and routing under minimal security constraints

Jorge López, Charalampos Chatzinakis, Marc Cartigny, Claude Poletti

- DTrap: A cyberattack-defense confrontation technique based on Moving Target Defense
  Zheng Yang, Degang Sun, Yan Wang, Xinbo Han, Chen Meng, Weiqing Huang
- Addressing a Malicious Tampering Attack on the Default Isolation Level in DBMS
  Abdullah Alhajri, Arshad Jhumka
- MATH - Finding and Fixing Exploits in Algorand
  Peter Ince, Xiapu Luo, Jiangshan Yu, Joseph K. Liu, Xiaoning Du
- Personalized Privacy-Preserving Semi-Centralized Recommendation System in a Trust-based Agent Network
  Qi Wen, Carson K. Leung, Adam G.M. Pazdor
- A New Design for Self-Encryption
  Roland Kromes, João Rodrigues, Duarte Nascimento, Gonçalo Cadete, François Verdier, Kaitai Liang
- Construction of Artificial Intelligence Generated Content in Digital Film Production
  Jinning wang, Xinyuan Huang, Zichu Yang, Weiran Zhao
- A Big Data Science and Engineering Solution for Transit Performance Analytics
  Nhu Minh Ngoc Pham, Yixi Wu, Carson K. Leung, Mohammadafaz V. Munshi, Vrushil Kiritkumar Patel, Connor C.J. Hryhoruk
- SmartLLM: A New Oracle System for Smart Contracts Calling Large Language Models
  Zhenan Xu, Jiuzheng Wang, Cong Zha, Xinyi Li, Hao Yin

CIT-2023 TECHNICAL SESSION

2 November 2023 Thursday

13:30-16:00 Session CIT: Computer and Information Technology (Room: Online Room 5)

Session Chair: Zhiwei Zhao, University of Electronic Science and Technology of China, China

- Lung Cancer Detection Using Machine Learning Approach
  Md Abrar Hamim, F.M. Tanmoy, Umme Fatema Tuj Asha, Md Nazmul Haq, Maruf Alam, Bijoy Ghosh
- Rethinking Evaluation Metric for Probability Estimation Models Using Esports Data
  Euihyeon Choi, Jooyoung Kim, Wonkyung Lee
- Communication Efficient Federated Learning Based on Combination of Structural Sparsification and Hybrid Quantization Sensing
  Tingting Wu, Wei Yu, Manxue Guo, Wenjing Nie, Zimeng Jia, Lun Xin
- COVID-19 Detection System: A Comparative Analysis of System Performance Based on Acoustic Features of Cough Audio Signals
  Asmaa Shati, Ghulam Mubashar Hassan, Amitava Datta
- R-SACE: RIS-Enabled Sensing-Aided Communication Enhancement in ISAC Systems
  Xiaohui Li, Yunpei Chen, Hong Wang, Shuran Sheng
- Deep learning for graph analysis: application to online human activity recognition
  Nassim Mokhtari, Mohamed Outlouhou, Alexis Nédélec, Pierre De Loor
- Total Cost of Ownership Applied to the Migration of Legacy Systems to Cloud Computing Environment
  Anilton Maia, Mario Meireles, Carlos Salles
- Personal Data Privacy in Software Development Processes: A Practitioner's Point of View
  Vinícius C. Andrade, Sheila Reinehr, Cinthia O. A. Freitas, Andreia Malucelli
- DEU-Net: Dual Encoder U-Net for 3D Medical Image Segmentation
  Yuxiang Zhou, Xin Kang, Fuji Ren, Satoshi Nakagawa, Xiao Shan

- 1-D CNN-Based Online Signature Verification with Federated Learning
  Lingfeng Zhang, Yuheng Guo, Yepeng Ding, Hiroyuki Sato

DSCI & SmartCNS-2023 TECHNICAL SESSION

2 November 2023 Thursday

16:00-18:00 Session DSCI & SmartCNS: Computational Intelligence and Smart Networking (Room: Online Room 5)

Session Chair: Tong Ding, Shandong University, China

- An Instruction Inference Graph Optimal Transport Network Model For Biomedical Commonsense Question Answering
  Luyue Kong, Shu Zhang, Jinbao Li, Song Liu
- Ergonomic Design of Precise Percutaneous Robot for Substantial Organs Based on JACK Simulation
  Bowen Sun, Xin Peng, SaiSai Li, Jiaxin Sun, Haochuan Tian
- Performance Evaluation of Flight Energy Consumption of UAVs in IRS-assisted UAV Systems
  Xiuyi Luo, Chongrui Lu, Siyi Ouyang, Siyu Xia
- Research on UAV Obstacle Avoidance Method Based on Virtual-real Combination Technology
  Wanying Song, Ying Lu, Jin Liu, Zilu Qin, Xiaodan Wang, Yanfang Fu
- A residual attention-based privacy-preserving biometrics model of transcriptome prediction from genome
  Cheng Tian, Song Liu, Jinbao Li, Guangchen Wang, Luyue Kong
- Designing and Implementing Communication-efficient Model of Distributed System for Real-time Electromagnetic Transient Simulation
  Qi Guo, Binjiang Hu, Zeqi Hong, Yanjun Zhao, Shuyong Li, Liang Tu
- DP-ProtoNet:An interpretable dual path prototype network for medical image diagnosis
  Luyue Kong, Ling Gong, Guangchen Wang, Song Liu
- A novel semantic dependency and aspect interaction graph convolutional network for aspect-level sentiment analysis
  Yihong Zhu, Xiaoliang Chen, Junsen Fu, Yajun Du

Part III: TECHNICAL SESSIONS OF UbiSec-2023 and Associated Symposia

UbiSec & ColTrust & SPIoT-2023 TECHNICAL SESSIONS

1 November 2023 Wednesday

13:30-15:45 Session UbiSec-3 & ColTrust: Emerging Techniques in Security and Trustworthiness (Room: Online Room 5)

Session Chair: Yuheng Zhang, Guangzhou University, China

- FRAD: Front-Running Attacks Detection on Ethereum using Ternary Classification Model
  Yuheng Zhang, Pin Liu, Guojun Wang, Peiqiang Li, Wanyi Gu, Houji Chen, Xuelei Liu, Jinyao Zhu
- Honey-Gauge: Enabling User-Centric HoneypotClassification
  Vinay Sachidananda, Berwyn Chai, Florian Gondesen, Kwok-Yan Lam, Yang Liu
- SCORD: Shuffling Column-Oriented Relational Database to Enhance Security
  Tieming Geng, Chin-Tser Huang, Csilla Farkas
- TruFaaS - Trust Verification Framework for FaaS

Avishka Shamendra, Binoy Peries, Gayangi Seneviratne, Sunimal Rathnayake

- Impact of Library Code in Binary Similarity Systems
  Andrei Vasile Mihalca, Ciprian Pavel Oprisa
- Privacy-Preserving Fall Detection in Elderly People Using Deep Learning
  Faseeh Iftikhar, Muhammad Faizan Khan, Guojun Wang, Fazli Wahid
- Research on Authorization Model of Attribute Access Control Based on Knowledge Graph
  Li Ma, Qidi Lao, Wenyin Yang, Zexian Yang, Dong Yuan, Zhaoxiong Bu
- Physically Unclonable Function Using Schmitt Triggers
  Rishab Goyal, Ritu Gupta
- Hydamc: A Hybrid Detection Approach for Misuse of Cryptographic Algorithms in Closed-Source Software
  Haoling Fan, Fanfyu Zheng, Jingqiang Lin, Lingjia Meng, Mingyu Wang, Qiang Wang, Shijie Jia, Yuan Ma

16:00-18:30 Session UbiSec-4 & SPIoT & CAI-2: Advanced Techniques in Data Privacy and Predictive Analytics (Room: Online Room 5)

Session Chair: Michael Mireku Kwakye, Fort Hays State University, USA

- Bilateral Personalized Information Fusion in Mobile Crowdsensing
  Zheqi Feng, Tao Peng, Guojun Wang, Kejian Guan
- A Probability Mapping-Based Privacy Preservation Method for Social Networks
  Qingru Li, Yahong Wang, Fangwei Wang, Zhiyuan Tan, Changguang Wang
- Channel Spatio-temporal Convolutional Network for Pedestrian Trajectory Prediction
  Zhonghao Lu, Lina Xu, Ying Hu, Liping Sun, Yonglong Luo
- Detection of Cyberbullying in Social Media Texts Using Explainable Artificial Intelligence
  Mohammad Rafsun Islam, Ahmed Saleh Bataineh, Mohammad Zulkernine
- Automatically Inferring Image Base Addresses of ARM32 Binaries Using Architecture Features
  Daniel Chong, Junjie Zhang, Nathaniel Boland, Lingwei Chen
- Machine Learning-based BGP Traffic Prediction
  Talaya Farasat, Muhammad Ahmad Rathore, Akmal Khan, JongWon Kim, Joachim *Posegga*
- SmartBuoy: A Machine Learning-based Detection Method for Interest Flooding Attacks in VNDN
  Yuwei Xu, Tiantian Zhang, Junyu Zeng, Rongrong Wang, Kehui Song, Jingdong Xu
- Simulation of Mixmining Reward Parameters for NymMixnet
  Harry Halpin
- Loft: An architecture for lifetime management of privacy data in service cooperation
  Cong Zha, Ju Xing, Zenan Xu, Hao Yin
- Multi-step Prediction of LTE-R Communication Quality based on CA-TCN and Differential Evolution
  Jiantao Qu, Chunyu Qi, Gaoyun An, He Meng

2 November 2023 Thursday

13:30-15:30 Session UbiSec-1: Emerging Frontiers in Cyberspace Security (Room: Burlington)

Session Chair: Michael Mireku Kwakye, Fort Hays State University, USA

- BiBERT-AV: Enhancing Authorship Verification through Siamese Networks with Pre-trainedBERT and Bi-LSTM
  Amirah Almutairi, BooJoong Kang, Nawfal Fadhel
- How does post-quantum cryptography affect Central Bank Digital Currency?

Lars Hupel, Makan Rafiee

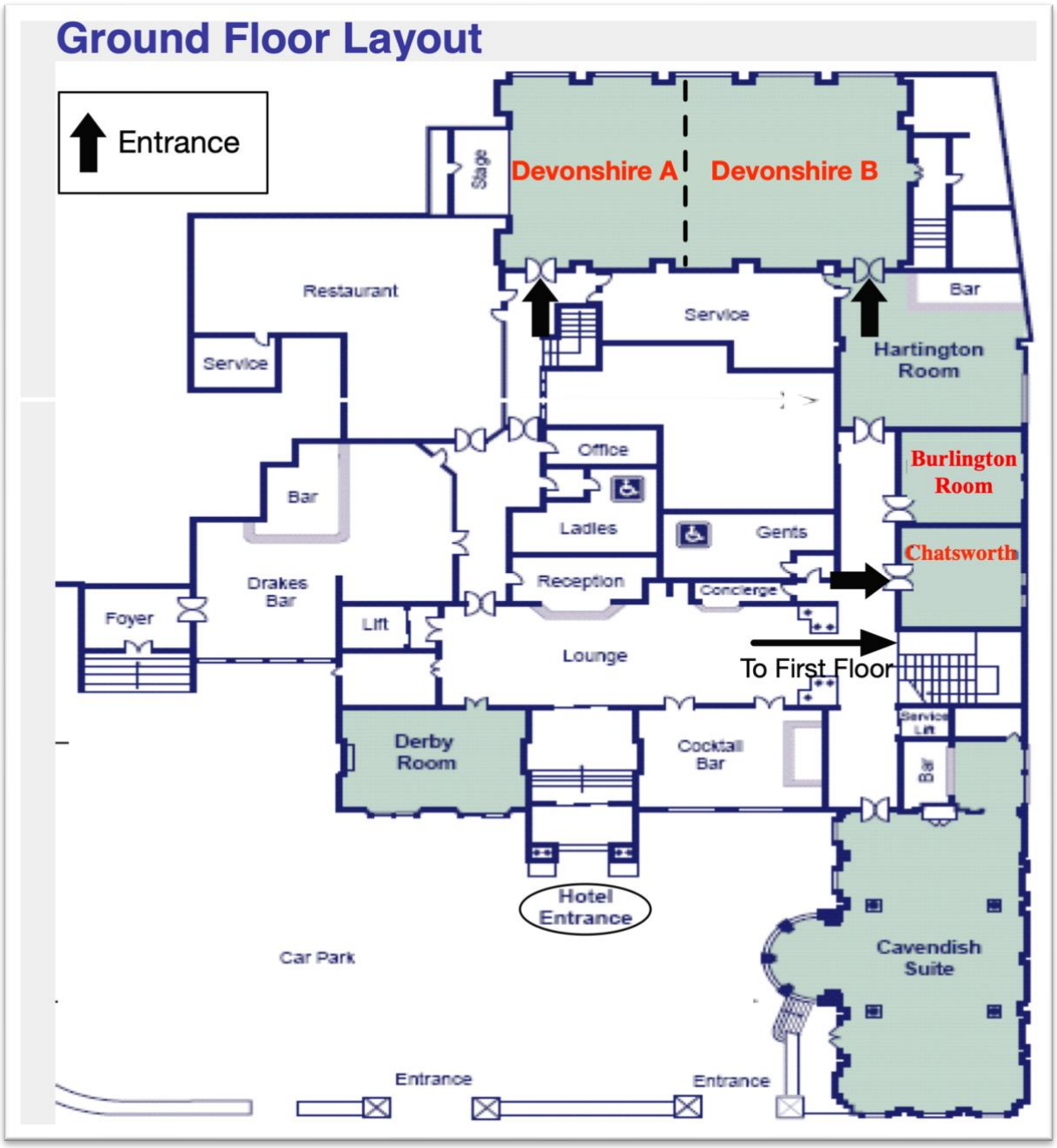
- A Comprehensive Survey of Attack Techniques, Implementation, and Mitigation Strategies in Large Language Models
  Aysan Esmradi, Daniel Wankit Yip, Chun Fai Chan
- Process Mining with Programmable Logic ControllerMemory States
  Chun Fai Chan, Kam Pui Chow
- Deploying Post-Quantum Algorithms in Existing Applications and Embedded Devices
  Petr Muzikant, Jan Willemson
- A SLAHP in the face of DLL Search Order Hijacking
  Antonin Verdier, Romain Laborde, Mohamed-Ali Kandi, Abdelmalek Benzekri
- Improving DNS Data Ex-filtration Detection through Temporal Analysis
  Georgios Spathoulas, Marios Anagnostopoulos, Konstantinos Papageorgiou, Georgios Kavallieratos, Georgios Theodoridis

16:00-18:00 Session UbiSec-2: Cyberspace Privacy and Blockchain Innovations (Room: Burlington)

Session Chair: Amirah Almutairi, University of Southampton, UK

- Blockchain-based Privacy-Preservation Platform for Data Storage and Query Processing
  Michael Mireku Kwakye, Ken Barker
- Is it Really You Who Forgot the Password? When Account Recovery Meets Risk-Based Authentication
  Andre Büttner, Andreas Thue Pedersen, Stephan Wiefling, Nils Gruschka, Luigi Lo Iacono
- Poison Egg: Scrambling Federated Learning with Delayed Backdoor Attack
  Masayoshi Tsutsui, Tatsuya Kaneko, Shinya Takamaeda-Yamazaki
- A Unified Knowledge Graph to Permit Interoperability of Heterogeneous Digital Evidence
  Ali Alshumrani, Nathan Clarke, Bogdan Ghita
- SMARPchain: A Smart Marker Based Reputational Probabilistic Blockchain for Multi-Agent Systems
  Chin-Tser Huang, Laurent Njilla, Matthew Sharp, Tieming Geng
- Multi-NetDroid: Multi-layer Perceptron Neural Network for Android Malware Detection
  Andri Rai, Eul Gyu Im
- Privacy-preserving Blockchain-based Traceability System with Decentralized Ciphertext-Policy Attribute-based Encryption
  Tsz Ho Pun, Yijun He, Siu Ming Yiu
- A Secure Contactless Payment System with Bidirectional Blockchain and Blake Hash Function
  Bhaskar Rongali, Satyajit Mohapatra, Sanjeet Kumar Nayak

Floor Plan


Ground Floor Layout
Entrance
Stage
Devonshire A
Devonshire B
Restaurant
Service
Service
Bar
Hartington Room
Office
Burlington Room
Bar
Ladies
Gents
Chatsworth
Drakes Bar
Reception
Concierge
Foyer
Lift
Lounge
To First Floor
Service Lift
Derby Room
Cocktail Bar
Bar
Hotel Entrance
Car Park
Cavendish Suite
Entrance
Entrance