The 2024 IEEE AI+ Congress

23rd IEEE International Conference on Trust, Security and Privacy in Computing and Communications

18th IEEE International Conference on Big Data Science and Engineering

27th IEEE International Conference on Computational Science and Engineering

22nd IEEE International Conference on Embedded and Ubiquitous Computing

12th IEEE International Conference on Smart City and Informatization

TrustCom/BigDataSE/CSE/EUC/iSCI-2024

December 17 - 21, 2024, Sanya, Hainan, China

https://ieee-aiplus.org/2024/

Organized by

Sponsored and supported by

IEEE

IEEE COMPUTER SOCIETY

TCSC IEEE

IEEE HI-TC Hyper Intelligence Technical Committee

CPSS Cyber-Physical-Social Systems

TABLE OF CONTENTS

Registration Desk

The Registration Desk will be open on the lobby (Ground Floor) of **HUALUXE Sanya Yalong Bay Resort** to assist you at the following time:

- Monday, December 16, 2024, 14:00 – 20:00
- Tuesday, December 17, 2024, 8:00 – 20:00
- Wednesday, December 18, 2024, 8:00 – 20:00
- Thursday, December 19, 2024, 8:00 – 20:00
- Friday, December 20, 2024, 8:00 – 12:00

Name Badges and Meal Tickets

All delegates, sponsors, and speakers of the IEEE TrustCom/BigDataSE/CSE/EUC/iSCI-2024 will receive a name badge upon registration. This badge must be worn at all times as it serves as your official pass to all technical sessions, as well as morning and afternoon coffee breaks.

Separate meal tickets will be provided for the welcome reception on December 18, the three lunches on December 17, 18, and 20, and the banquet on December 19.

Presentation Guidelines

Conference Date

The conference is to be held from December 17 - 21, 2024. The time for the conference program is based on CST, China Standard Time.

Language

The presentation language of the IEEE TrustCom/BigDataSE/CSE/EUC/iSCI-2024 is English.

For Session Chairs

Session Chairs are requested to join the room at least 10 minutes before their sessions.

For Authors

Authors of **Research Full Papers, Research Papers, and Workshop Papers** are strongly encouraged to attend their respective presentation and Q&A sessions. Please confirm your attendance with the Session Chair at least 10 minutes before the session begins.

Timing

Please refer to the program for the exact timing of your session and the position of your paper within the session.

Authors of **Research Full Papers, Research Papers, and Workshop Papers** are advised to allocate **15 minutes for presentation followed by 5 minutes for questions**. However, the exact presentation time for each paper will be determined by the Session Chairs, depending on the number of presentations in the session. The Session Chairs will ensure that presentations stay within the allocated time.

Proceedings

If you are interested in reading papers during the presentations, here are the proceedings:

https://conferences.computer.org/trustcompub24

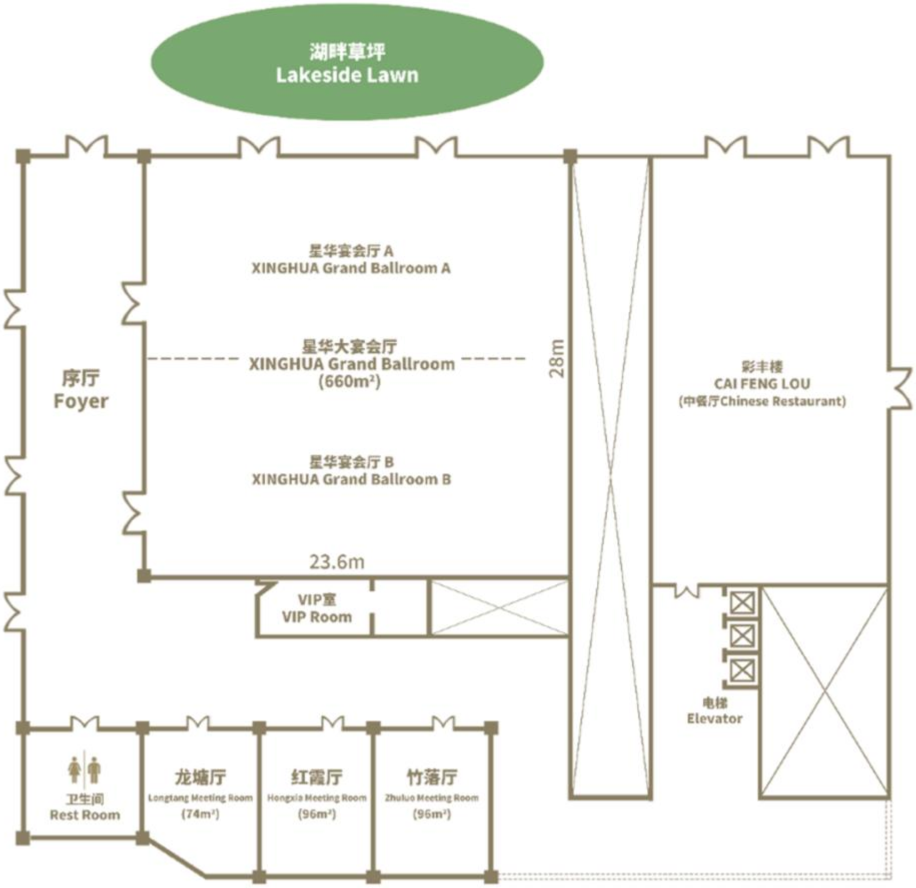
The username and password will be sent to all fully registered participants at the conference, respectively.

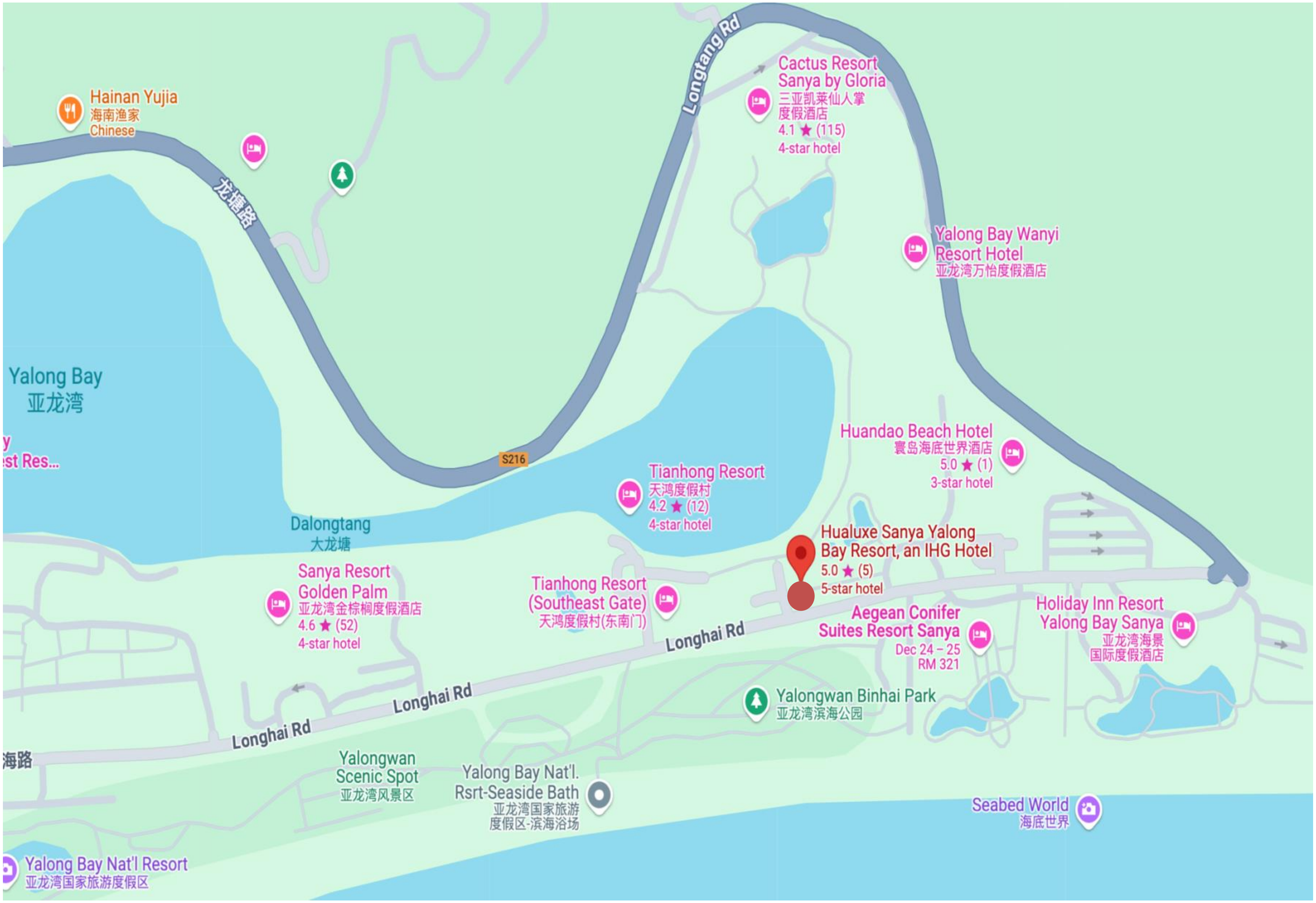
Conference Venue

HUALUXE Sanya Yalong Bay Resort

Locations	Rooms	Activities
Jiari Meeting Room (假日套房酒店会议室)	Room 1	Oral Presentation
Longtang Meeting Room (龙塘厅)	Room 2	Oral Presentation
Hongxia Meeting Room (红霞厅)	Room 3	Oral Presentation
Zhuluo Meeting Room (竹落厅)	Room 4	Oral Presentation
XINGHUA Grand Ballroom A (星华宴会厅 A)	Room 5	Oral Presentation
XINGHUA Grand Ballroom B (星华宴会厅 B)	Room 6	Oral Presentation
XINGHUA Grand Ballroom (星华大宴会厅)	Room 7	Opening/Keynote/Reception/Banquet/Panel

Note: Jiari Meeting Room is on the Ground Floor of the Holiday Inn & Suites, which is the next building.




Hainan Yujia
海南渔家
Chinese
龙塘路
Longtang Rd
Cactus Resort
Sanya by Gloria
三亚凯莱仙人掌
度假酒店
4.1 ★ (115)
4-star hotel
Yalong Bay Wanyi
Resort Hotel
亚龙湾万怡度假酒店
Yalong Bay
亚龙湾
y
est Res...
S216
Huandao Beach Hotel
寰岛海底世界酒店
5.0 ★ (1)
3-star hotel
Tianhong Resort
天鸿度假村
4.2 ★ (12)
4-star hotel
Dalongtang
大龙塘
Hualuxe Sanya Yalong
Bay Resort, an IHG Hotel
5.0 ★ (5)
5-star hotel
Sanya Resort
Golden Palm
亚龙湾金棕榈度假酒店
4.6 ★ (52)
4-star hotel
Tianhong Resort
(Southeast Gate)
天鸿度假村(东南门)
Longhai Rd
Aegean Conifer
Suites Resort Sanya
Dec 24 – 25
RM 321
Holiday Inn Resort
Yalong Bay Sanya
亚龙湾海景
国际度假酒店
Longhai Rd
Yalongwan Binhai Park
亚龙湾滨海公园
Longhai Rd
海路
Yalongwan
Scenic Spot
亚龙湾风景区
Yalong Bay Nat'l.
Rsrt-Seaside Bath
亚龙湾国家旅游
度假区-滨海浴场
Seabed World
海底世界
Yalong Bay Nat'l Resort
亚龙湾国家旅游度假区

Welcome Message from the Congress Steering Chair

Welcome to the 2024 IEEE AI + Congress which includes the 23rd IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom-2024); the 18th IEEE International Conference on Big Data Science and Engineering (BigDataSE-2024); the 27th IEEE International Conference on Computational Science and Engineering (CSE-2024); the 22nd IEEE International Conference on Embedded and Ubiquitous Computing (EUC-2024); the 12th IEEE International Conference on Smart City and Informatization (iSCI-2024).

In an era where artificial intelligence (AI) is increasingly integrated into diverse fields, the 2024 IEEE AI + Congress serves as a dynamic hub for innovation and collaboration at the intersection of AI and emerging technologies. This congress brings together leading researchers, practitioners, and industry experts to explore transformative AI-driven solutions that address critical challenges and drive advancements across a wide range of domains.

Here, we would like to sincerely thank all organizing committee members, program committee members, and reviewers for their hard work and valuable contributions. Without your help, these conferences would not have been possible. We greatly appreciate the sponsorship from IEEE, IEEE Computer Society, IEEE Technical Committee on Scalable Computing, IEEE SC Technical Committee on Hyper-Intelligence, and IEEE CIS Cyber-Physical-Social Systems Task Force. We are very grateful to the keynote speakers for their authoritative speeches. We thank all authors and conference participants for using this forum to communicate their excellent work.

The conferences are planned to be held in December 17 - 21, 2024, Sanya, Hainan, China.

We hope you find the conferences a stimulating and exciting forum.

Laurence T. Yang
FCAE, FEIC, MAE, MRAE, FIEEE, MNAAI
Steering Chair, IEEE CS Technical Committee on Scalable Computing
Chair, IEEE SMC Technical Committee on Cybermatics
Chair, IEEE SC Technical Committee on Hyper-Intelligence
Chair, IEEE CIS Smart World Technical Committee
Academic Vice-president and Dean, Zhengzhou University, China
Congress Steering Chair

Congress Keynotes

Keynote 1: M. Jamal Deen, McMaster University, Canada

Brain-inspired Cognitive Dynamic Systems for Engineering and Health Applications

Keynote 2: Elisa Bertino, Purdue University, USA

Applying Machine Learning to Securing Cellular Networks

Keynote 3: Jinjun Chen, Swinburne University of Technology, Australia

Composite DP-unbias: Bounded and Unbiased Composite Differential Privacy

Keynote 4: Moncef Gabbouj, Tampere University, Finland

The Super Neuron Model - New Generation Machine Learning and Applications

Keynote 5: Nirwan Ansari, New Jersey Institute of Technology, USA

AI-Native Core Network Designs

Keynote 6: C. L. Philip Chen, South China University of Technology, China

An Incremental-Self-Training-Guided Semi-Supervised Broad Learning System for Data Annotation

Keynote 7: Sergei Kuznetsov, HSE University, Russia

Explainable Knowledge Discovery with Interval Pattern Structures

Keynote 8: Liming Chen, Dalian University of Technology, China

Towards a Hybrid Intelligent Framework for Intrusion Responses in IoT Systems

The 2024 IEEE AI+ Congress

Keynote 1: Brain-inspired Cognitive Dynamic Systems for Engineering and Health Applications

***M. Jamal Deen**, McMaster University, Canada*

About the Keynote Speaker

M. Jamal Deen is a Distinguished University Professor at McMaster University. His research interests are nano-/opto-electronics, nanotechnology, data analytics and their applications to health and environmental sciences. His research record includes more than 930 peer-reviewed articles (~20% are invited), two textbooks, 6 awarded patents extensively used in industry, and 26 best paper/poster/presentation awards. As an undergraduate, he was the top-ranked mathematics and physics student and the second ranked student at the university, winning the Chancellor's gold medal and the Irving Adler prize. As a graduate student, he was a Fulbright-Laspau Scholar and an American Vacuum Society Scholar. As an educator, he won the IEEE Canada's Ham Education Medal, the McMaster President's Award for Excellence in Graduate Supervision, and MSU Macademics' Lifetime Achievement Award for his exceptional dedication to teaching. His other awards and honours include the Callinan Award and the Electronics and Photonics Award from the Electrochemical Society (ECS); a Humboldt Research Award; the Eadie Medal from the Royal Society of Canada (RSC); the McNaughton Gold Medal, Fessenden Medal and Gotlieb Medal, all from IEEE Canada. He was awarded five honorary doctorate degrees in recognition of his exceptional research and scholarly accomplishments, exemplary professionalism and valued services. He is elected by his peers to Fellow status in thirteen national academies and professional societies including RSC, IEEE, ECS and the American Physical Society. Recently, he was appointed to the Order of Canada. He served as President of the Academy of Science, RSC, from 2015 to 2017.

Summary: This presentation will introduce and summarize intelligent systems using brain-inspired cognitive dynamic systems (CDS) as an analogy of the human brain, in two important applications. First, an overview of the basic cognition concepts such as the perception–action cycle (PAC), memory, attention, intelligence, and language will be given. Next, we will explain why CDS are necessary and how machine learning methods including supervised learning and reinforcement learning are used. This will be followed by two examples – one in engineering and another in healthcare. In engineering area, we will use CDS as the brain of a software defined optical communications systems (SDOCS) to demonstrate the performance enhancement of ultrahigh-speed optical pulse transmission system upgraded with the preceptor of CDS as the proof-of-concept of SDOCS. Our experimental results show ~1.3 dB enhancement in Q-factor for a 1.28 Tbaud (10 Gbaud ×128 OTDM) fiber optic system with polarization-multiplexed 64 quadrature amplitude modulation (QAM) at 15 Tbit/s data rate over a 150 km long fiber link. Very importantly, the CDS provides good reliability over system disturbances such as clock recovery intolerance. In healthcare, we have developed a CDS-based framework for a smart e-Health system to realize an automatic screening process in the presence of a defective or abnormal dataset that may have poor labeling and/or lack enough training patterns. To mitigate the adverse effect of such a defective dataset, we developed a decision-making system that is inspired by the decision-making processes in humans in case of conflict-of-opinions (CoO). We present a proof-of-concept implementation of this framework to automatically identify people having Arrhythmia from single lead Electrocardiogram (ECG) traces. It is shown that the proposed CDS performs well with low diagnosis errors. Finally, the proposed CDS algorithm can be incorporated in the autonomic computing layer of a smart-e-Health-home platform to achieve a pre-defined degree of screening accuracy in the presence of a defective dataset.

The 2024 IEEE AI+ Congress

Keynote 2: Applying Machine Learning to Securing Cellular Networks

***Elisa Bertino**, Purdue University, USA*

About the Keynote Speaker

Elisa Bertino is a Distinguished Samuel Conte professor of Computer Science at Purdue University. She serves as Director of the Purdue Cyberspace Security Lab (Cyber2Slab). Prior to joining Purdue, she was a professor and department head at the Department of Computer Science and Communication of the University of Milan. She has been a visiting researcher at the IBM Research Laboratory in San Jose (now Almaden), at Rutgers University, at Telcordia Technologies. She has also held visiting professor positions at the Singapore National University and the Singapore Management University. Her recent research focuses on security and privacy of cellular networks and IoT systems, and on edge analytics for cybersecurity. Elisa Bertino is a Fellow member of IEEE, ACM, and AAAS. She received the 2002 IEEE Computer Society Technical Achievement Award for “For outstanding contributions to database systems and database security and advanced data management systems”, the 2005 IEEE Computer Society Tsutomu Kanai Award for “Pioneering and innovative research contributions to secure distributed systems”, the 2019-2020 ACM Athena Lecturer Award, and the 2021 IEEE 2021 Innovation in Societal Infrastructure Award. She received an Honorary Doctorate from Aalborg University in 2021 and an Honorary Research Doctorate in Computer Science from the University of Salerno in 2023. She is currently serving as ACM Vice-president.

Summary: Cellular network security is more critical than ever, given the increased complexity of these networks and the numbers of applications that depend on them, including telehealth, remote education, ubiquitous robotics and autonomous vehicles, smart cities, and Industry 4.0. In order to devise more effective defenses, a recent trend is to leverage machine learning (ML) techniques, which have become applicable because of today advanced capabilities for collecting data as well high-performance computing systems for training of ML models. Recent large language models (LLMs) are also opening new interesting directions for security applications. In this talk, I will first present a comprehensive threat analysis in the context of 5G cellular networks to give a concrete example of the magnitude of the problem of cellular network security. Then, I will present two specific applications of ML techniques for the security of cellular networks. The first application focuses on the use of natural language processing techniques to the problem of detecting inconsistencies in the "natural language specifications" of cellular network protocols. The second application addresses the design of an anomaly detection system able to detect the presence of malicious base stations and determine the type of attack. Then I'll conclude with a discussion on research directions.

The 2024 IEEE AI+ Congress

Keynote 3: Composite DP-unbias: Bounded and Unbiased Composite Differential Privacy

***Jinjun Chen**, Swinburne University of Technology, Australia*

About the Keynote Speaker

Jinjun Chen is a Professor from Swinburne University of Technology, Australia. He holds a PhD in Information Technology from Swinburne University of Technology, Australia. His research interests include data privacy and security, cloud computing, scalable data processing, data systems and related various research topics. His research results have been published in more than 300 papers in international journals and conferences. He received various awards such as IEEE TCSC Award for Excellence in Scalable Computing and Australia's Top Researchers. He has served as an Associate Editor for various journals such as ACM Computing Surveys, IEEE TC, TCC and TSUSC. He is a MAE (Academia Europea) and IEEE Fellow (IEEE Computer Society). He is Chair for IEEE TCSC (Technical Community for Scalable Computing).

Summary: The most kind of traditional DP (Differential Privacy) mechanisms (e.g. Laplace, Gaussian, etc.) have unlimited output range. In real scenarios, most datasets have bounded output range. Users would then need to use post-processing or truncated mechanisms to forcibly bound output distribution. However, these mechanisms would incur bias problem which has been a long-known DP challenge, resulting in various unfairness issues in subsequent applications. A tremendous amount of research has been done on analyzing this bias problem and its consequences, but no solutions can solve it fully.

As the world first solution to solve this long-known DP bias problem, this talk will present a new innovative DP mechanism named Composite DP-unbias. It will first illustrate this long-known bias problem, and then detail the rational of the new mechanism and its example noise functions as well as their implementation algorithms. All source codes are publicly available on Github for any deployment or verification.

The 2024 IEEE AI+ Congress

Keynote 4: The Super Neuron Model - New Generation Machine Learning and Applications

Moncef Gabbouj, *Tampere University, Finland*

About the Keynote Speaker

Moncef Gabbouj received his BS degree in 1985 from Oklahoma State University, and his MS and PhD degrees from Purdue University, in 1986 and 1989, respectively, all in electrical engineering. Dr. Gabbouj is a Professor of Information Technology at the Department of Computing Sciences, Tampere University, Tampere, Finland. He was Academy of Finland Professor during 2011-2015. His research interests include Big Data analytics, artificial intelligence, machine learning, pattern recognition, and video processing and coding. Dr. Gabbouj is a Fellow of the IEEE and member of the Academia Europaea and the Finnish Academy of Science and Letters. He is the past Chairman of the IEEE CAS TC on DSP and committee member of the IEEE Fourier Award for Signal Processing. He served as associate editor and guest editor of many IEEE, and international journals and Distinguished Lecturer for the IEEE CASS. Dr. Gabbouj served as General Chair of IEEE ICIP 2024, ISCAS 2019, ICIP 2020, and ICME 2021. Gabbouj is Finland Site Director of the USA NSF IUCRC funded Center for Big Learning and led the Artificial Intelligence Research Task Force of Finland’s Ministry of Economic Affairs and Employment funded Research Alliance on Autonomous Systems (RAAS).

Summary: Deep Learning is great as it has outperformed many traditional approaches in numerous fields. However, DL comes at a price of high computational cost and follows mostly a Blackbox approach. Striving towards Green Learning, we will propose and discuss Operational Neural Networks (ONNs) as more efficient alternatives to conventional Convolutional Neural Networks (CNNs). ONNs can perform any linear or non-linear transformation with a proper combination of “nodal” and “pool” operators. This is a great leap towards expanding the neuron’s learning capacity in CNNs, which thus far required the use of a single nodal operator for all synaptic connections for each neuron. This restriction has recently been lifted by introducing a superior neuron called the “generative neuron” where each nodal operator can be customized during the training to maximize learning. As a result, the network can self-organize the nodal operators of its neurons’ connections. Self-Organized ONNs (Self-ONNs) equipped with superior generative neurons can achieve diversity even with a compact configuration. A novel approach to enforce diversity in ANN will also be discussed. We shall explore several applications of neural network models equipped with the generative and the superior neuron.

The 2024 IEEE AI+ Congress

Keynote 5: AI-Native Core Network Designs

***Nirwan Ansari**, New Jersey Institute of Technology, USA*

About the Keynote Speaker

Nirwan Ansari is a Distinguished Professor of Electrical and Computer Engineering at the New Jersey Institute of Technology (NJIT), holds a Ph.D. from Purdue University, an MSEE from the University of Michigan, and a BSEE (summa cum laude with a perfect GPA) from NJIT. He is a Fellow of the Institute of Electrical and Electronics Engineers (IEEE) as well as the National Academy of Inventors (NAI).

He authored Green Mobile Networks: A Networking Perspective (Wiley-IEEE, 2017) with T. Han, and co-authored two other books. He has also (co-)authored over 700 technical publications, with more than half of them published in widely cited journals and magazines. He has served as a guest editor for numerous special issues on various emerging topics in communications and networking. Currently, he serves as the Editor-in-Chief of IEEE Wireless Communications and has been on the editorial/advisory board of over ten journals. His current research focuses on green communications and networking, edge computing, drone-assisted networking, and various aspects of broadband networks.

He was elected to serve on the IEEE Communications Society (ComSoc) Board of Governors as a member-at-large. He has served as the Director of ComSoc Educational Services Board, chaired various technical and steering committees within ComSoc, and served on many committees such as the IEEE Fellow Committee. He has actively participated in organizing numerous IEEE International Conferences/Symposia/Workshops. Among his many recognitions are several excellence in teaching awards, multiple best paper awards, the NCE Excellence in Research Award, several ComSoc TC technical recognition awards, the NJ Inventors Hall of Fame Inventor of the Year Award, the Thomas Alva Edison Patent Award, the Purdue University Outstanding Electrical and Computer Engineering Award, the NCE 100 Medal, the NJIT Excellence in Research Prize and Medal, and designation as a COMSOC Distinguished Lecturer. He has also been granted more than 40 U.S. patents.

Summary: 3GPP is paving the way for a transformative leap towards AI-Native operations in the upcoming 6G core networks (CNs). Unlike the fragmented and non-standardized applications of artificial intelligence (AI) in 5G CNs, the 6G era promises a revolutionary overhaul. AI will become the central driving force behind all network functions, marking a significant evolution known as AI-Native. This presentation will delve into this paradigm shift, exploring how AI will fundamentally reshape network architectures. Attendees will gain insights into the pivotal role of AI in enhancing efficiency, adaptability, and intelligence across network operations, heralding a new epoch in telecommunications.

The 2024 IEEE AI+ Congress

Keynote 6: An Incremental-Self-Training-Guided Semi-Supervised Broad Learning System for Data Annotation

***C. L. Philip Chen**, South China University of Technology, China*

About the Keynote Speaker

C. L. Philip Chen is the Chair Professor and Dean of the School of Computer Science and Engineering, South China University of Technology. Prior to this position he worked in US in two different universities as a tenured professor, department chair and associate dean, and in University of Macao as the dean. He is a Fellow of IEEE, AAAS, IAPR, CAA, CAAI, and HKIE; a member of Academia Europaea (AE), a member of European Academy of Sciences and Arts (EASA), and a Full Foreign Member of Russia Academy of Engineering (FFM-RAE). He received the IEEE Norbert Wiener Award in 2018, for his contribution in systems and cybernetics, and machine learnings, the IEEE Joseph G. Wohl Outstanding Career award, Wu WenJun Outstanding Contribution award from Chinese AI Association, and 2016 Outstanding Electrical and Computer Engineers Award from his alma mater, Purdue University.

He is a highly cited researcher by Clarivate Analytics from 2018-2023. His current research interests include cybernetics, systems, and computational intelligence. For his contribution in these research areas, he received two times best transactions paper award from IEEE Transactions on Neural Networks and Learning Systems for his papers in 2014 and 2018 and received three-time Macau natural science award. In professional service, he was the Editor-in-Chief of the IEEE Transactions on Cybernetics, the Editor-in-Chief of the IEEE Transactions on Systems, Man, and Cybernetics: Systems, the President of IEEE Systems, Man, and Cybernetics Society. Currently, he is the director of two Guangdong Key Labs, the director of a research lab funded by the Ministry of Education, a Vice President of Chinese Association of Automation, and Co-President of Guangdong AI Industrial Association.

Summary: The Broad Learning System (BLS) has been proved to be effective and efficient lately and has recently been applied in numerous fields. It is mainly a supervised learning system and thus not suitable for specific practical applications with a mixture of labeled and unlabeled data. This talk first presents the necessity and various kinds of data annotation followed by the presentation of an incremental-self-training-guided semi-supervised BLS (ISTSS-BLS). Distinctive to traditional self-training, where all unlabeled data are labeled simultaneously, incremental self-training (IST) obtains unlabeled data incrementally from an established sorted list based on the distance between the data and their cluster center. During iterative learning, a small portion of labeled data is first used to train BLS. The system recursively self-updates its structure and meta-parameters using: 1) the double-restricted mechanism and 2) the dynamic neuron-incremental mechanism. Taking the advantages of incremental learning from the BLS, these strategies guarantee a parsimonious model during the update. In addition, ISTSS-BLS is compared with different state-of-the-art alternatives, and all results indicate that it possesses significant advantages in performance.

The 2024 IEEE AI+ Congress

Keynote 7: Explainable Knowledge Discovery with Interval Pattern Structures

Sergei Kuznetsov, *HSE University, Russia*

About the Keynote Speaker

Sergei O. Kuznetsov graduated from Moscow Institute for Physics and Technology and defended Doctor of Science thesis on Machine Learning Models Based on Concept Lattices in 2002 at the Computing Center of Russian Academy of Science. He is now full professor at the HSE University in Moscow, being the head of School for Data Analysis and Artificial Intelligence, the head of the International Laboratory for Intelligent Systems, and the academic supervisor of the Data Science master program. His main research interests are in the Formal Concept Analysis, Explainable AI (XAI) and Knowledge Discovery.

Summary: Interval pattern structures allow for direct processing of numerical data by constructing clusters, taxonomies of objects, implicational dependencies, biclusters of similar values while avoiding binarization. Models and applications related to interval pattern structures will be discussed. We show that interval pattern structures propose explainable methods of knowledge discovery in numerical data, allowing for better interpretability of the classical ML approaches like k-NN algorithm.

The 2024 IEEE AI+ Congress

Keynote 8: Towards a Hybrid Intelligent Framework for Intrusion Responses in IoT Systems

***Liming Chen**, Dalian University of Technology, China*

About the Keynote Speaker

Liming Chen is a Chair Professor at Dalian University of Technology (DUT), China. He leads the Intelligent Cyber-Physical System Research Lab. Prior to joining DUT, he was the Research Director for the School of Computing at Ulster University, UK. His current research interests include data analytics, pervasive computing, artificial intelligence, intelligent cyber-physical systems and their applications in smart healthcare and cybersecurity. His research has been funded by external grants from the UK research councils, European Research Programmes such as FP7, AAL and Horizon 2020, and industrial collaborators like SAP, British Telecommunication and PwC. Liming was the coordinator for the EU Horizon 2020 Excellence Research programme MSCA ITN ACROSSING project, the General Chair for IEEE DigitalTwin2024, IEEE WoWMoM2022, IEEE Smart World Congress 2019 and IEEE UIC2017. He is an IET Fellow and has served as an expert for research funding assessment for UKRI, EU Horizon2020, Canada, Chile, Netherlands and Denmark.

Summary: The rapid expansion of the Internet of Things and the emergence of edge computing-based applications has led to a new wave of cyber-attacks, with intensity and complexity that has never been seen before. Most research has currently focused on Intrusion Detection Systems (IDS). Due to the volume and speed of this new generation of cyber-attacks it is no longer sufficient to solely detect attacks and leave the response to security analysts. As a result, research into Intrusion Response Systems (IRS) has attracted growing attention. Though substantial progress has been made, resilient automatic IRSs have not been seen yet. In this talk, the speaker will first introduce a data- and knowledge-driven hybrid framework which streamlines the lifecycle from data-driven intrusion detection to the knowledge-driven intrusion responses by combining data analytics and knowledge representation and reasoning. He will then describe the methods and mechanisms for automatic and human-in-the-loop intrusion response, covering cost and effect analysis, action prioritisation, ranking and selection. Following this he will present an initial implementation of the framework in a dashboard prototype. Finally, the speaker will discuss research challenges and future directions to stimulate new ideas and approaches in this promising research area.

Panel on AI Trust, Security and Privacy

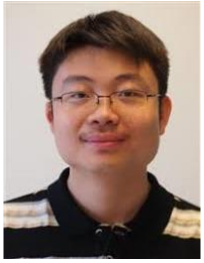
With the rapid development of artificial intelligence technology, the contradiction between the complexity of data security and the limitations of traditional network security governance has become increasingly prominent. Empowering security operations through AI is seen as a key link in developing new quality productivity. These remain a question on how to strengthen AI governance, effectively prevent and resolve various security risks brought about by the development of AI, and continuously improve the institutionalization of AI security supervision.
This panel involves world-wide research experts related to AI and aims to discuss the future trend of AI in Trust, Security and privacy.

Each panelist first has around 5min to talk about their own work related to AI, then we spend 20min for a panel discussion and the last 15min answering the questions from the audience.

Panel Schedule

Panel Date: 17:30 – 18:30, December 18, 2024
Panel Venue: XINGHUA Grand Ballroom

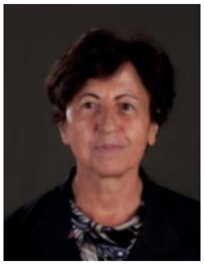
Moderator



Weizhi Meng is a Full Professor in the School of Computing and Communications, Lancaster University, United Kingdom, and an adjunct faculty in the Department of Applied Mathematics and Computer Science, Technical University of Denmark, Denmark. He obtained his Ph.D. degree in Computer Science from the City University of Hong Kong. He was a recipient of the Hong Kong Institution of Engineers (HKIE) Outstanding Paper Award for Young Engineers/Researchers in both 2014 and 2017. He also received the IEEE ComSoc Best Young Researcher Award for Europe, Middle East, & Africa Region (EMEA) in 2020. His primary research interests are blockchain technology, cyber security and artificial intelligence in security including intrusion detection, blockchain applications, smartphone security, biometric authentication, and IoT security. He serves as associate editors / editorial board members for many reputed journals such as IEEE TDSC and IEEE TIFS, as well as general chair for various international conferences such as ACM CCS 2023 and ESORICS 2022. He is an ACM Distinguished Speaker.

Panelists

Nirwan Ansari, Distinguished Professor of Electrical and Computer Engineering at the New Jersey Institute of Technology (NJIT), holds a Ph.D. from Purdue University, an MSEE from the University of Michigan, and a BSEE (summa cum laude with a perfect GPA) from NJIT. He is a Fellow of the Institute of Electrical and Electronics Engineers (IEEE) as well as the National Academy of Inventors (NAI). He was elected to serve on the IEEE Communications Society (ComSoc) Board of Governors as a member-at-large. He has served as the Director of ComSoc Educational Services Board, chaired various technical and steering committees within ComSoc, and served on many committees such as the IEEE Fellow Committee. He has actively participated in organizing numerous IEEE International Conferences/Symposia/Workshops. Among his many recognitions are several excellence in teaching awards, multiple best paper awards, the NCE Excellence in Research Award, several ComSoc TC technical recognition awards, the NJ Inventors Hall of Fame Inventor of the Year Award, the Thomas Alva Edison Patent Award, the Purdue University Outstanding Electrical and Computer Engineering Award, the NCE 100 Medal, the NJIT Excellence in Research Prize and Medal, and designation as a COMSOC Distinguished Lecturer. He has also been granted more than 40 U.S. patents.



Elisa Bertino is a Distinguished Samuel Conte professor of Computer Science at Purdue University. She serves as Director of the Purdue Cyberspace Security Lab (Cyber2Slab). Prior to joining Purdue, she was a professor and department head at the Department of Computer Science and Communication of the University of Milan. She has been a visiting researcher at the IBM Research Laboratory in San Jose (now Almaden), at Rutgers University, at Telcordia Technologies. She has also held visiting professor positions at the Singapore National University and the Singapore Management University. Her recent research focuses on security and privacy of cellular networks and IoT systems, and on edge analytics for cybersecurity. Elisa Bertino is a Fellow member of IEEE, ACM, and AAAS. She received the 2002 IEEE Computer Society Technical Achievement Award for “For outstanding contributions to database systems and database security and advanced data management systems”, the 2005 IEEE Computer Society Tsutomu Kanai Award for “Pioneering and innovative research contributions to secure distributed systems”, the 2019-2020 ACM Athena Lecturer Award, and the 2021 IEEE 2021 Innovation in Societal Infrastructure Award. She received an Honorary Doctorate from Aalborg University in 2021 and an Honorary Research Doctorate in Computer Science from the University of Salerno in 2023. She is currently serving as ACM Vice-president.

Liqun Chen is a Professor in Secure Systems at the University of Surrey. Before taking up this position in 2016, she was a principal research scientist at Hewlett-Packard Laboratories, Bristol, UK. She developed several cryptographic schemes that were adopted by International Standards bodies, such as ISO/IEC, IEEE and TCG (Trusted Computing Group). Notably, she designed several cryptographic algorithms, including direct anonymous attestation, which are used in the Trusted Platform Module (TPM). She was the technical leader and principal investigator in the EU H2020 FutureTPM project, which identified and developed algorithms for a TPM that would be secure against quantum computer attacks. Additionally, she has served as a principal investigator in six other EU Horizon projects, which make use of post-quantum cryptography, trusted computing and distributed ledger technologies to achieve security, privacy and trust in real-world applications. She has acted as an editor or co-editor for 11 ISO/IEC documents and assisted with TCG's TPM specifications. Her current research interests include applied cryptography, trusted computing, and security standardisation.

Jinjun Chen is a Professor from Swinburne University of Technology, Australia. He holds a PhD in Information Technology from Swinburne University of Technology, Australia. His research interests include data privacy and security, cloud computing, scalable data processing, data systems and related various research topics. His research results have been published in more than 300 papers in international journals and conferences. He received various awards such as IEEE TCSC Award for Excellence in Scalable Computing and Australia’s Top Researchers. He has served as an Associate Editor for various journals such as ACM Computing Surveys, IEEE TC, TCC and TSUSC. He is a MAE (Academia Europea) and IEEE Fellow (IEEE Computer Society). He is Chair for IEEE TCSC (Technical Community for Scalable Computing).

Moncef Gabbouj received his BS degree in 1985 from Oklahoma State University, and his MS and PhD degrees from Purdue University, in 1986 and 1989, respectively, all in electrical engineering. Dr. Gabbouj is a Professor of Information Technology at the Department of Computing Sciences, Tampere University, Tampere, Finland. He was Academy of Finland Professor during 2011-2015. His research interests include Big Data analytics, artificial intelligence, machine learning, pattern recognition, and video processing and coding. Dr. Gabbouj is a Fellow of the IEEE and member of the Academia Europaea and the Finnish Academy of Science and Letters. He is the past Chairman of the IEEE CAS TC on DSP and committee member of the IEEE Fourier Award for Signal Processing. He served as associate editor and guest editor of many IEEE, and international journals and Distinguished Lecturer for the IEEE CASS. Dr. Gabbouj served as General Chair of IEEE ICIP 2024, ISCAS 2019, ICIP 2020, and ICME 2021. Gabbouj is Finland Site Director of the USA NSF IUCRC funded Center for Big Learning and led the Artificial Intelligence Research Task Force of Finland’s Ministry of Economic Affairs and Employment funded Research Alliance on Autonomous Systems (RAAS).

The 2024 IEEE AI+ Congress Program

IEEE TrustCom/BigDataSE/CSE/EUC/iSCI-2024

Tuesday, December 17, 2024 (China Standard Time CST, UTC+8)

Room	Room 1 (Jiari)	Room 2 (Longtang)	Room 3 (Hongxia)	Room 4 (Zhuluo)	Room 5 (XINGHUA A)	Room 6 (XINGHUA B)
8:00-10:00	TrustCom-31: Emerging Tech (IV)	TrustCom-35: AI Trust (VI)	TrustCom-39: Security (XVI)	TrustCom-43: Security (XX)	TrustCom-47: Forensics and Analytics (II)	TrustCom-51: AI Trust (X)
10:00-10:20	**Coffee Break**					
10:20-12:20	TrustCom-32: Emerging Tech (V)	TrustCom-36: AI Trust (VII)	TrustCom-40: Security (XVII)	TrustCom-44: Privacy (VII)	TrustCom-48: Emerging Tech (VII)	TrustCom-52: Security and Privacy
12:20-14:00	**Lunch**					
14:00-16:00	TrustCom-33: Emerging Tech (VI)	TrustCom-37: Trust (III)	TrustCom-41: Security (XVIII)	TrustCom-45: Privacy (VIII)	TrustCom-49: AI Trust (VIII)	TrustCom-53: Data Security and Privacy
16:00-16:20	**Coffee Break**					
16:20-18:20	TrustCom-34: AI Trust (V)	TrustCom-38: Security (XV)	TrustCom-42: Security (XIX)	TrustCom-46: Privacy (IX)	TrustCom-50: AI Trust (IX)	TrustCom-54: Trustworthy Crowd Computing

Wednesday, December 18, 2024 (Room 7, China Standard Time CST, UTC+8)

Zoom Link, Room: 829 8865 5295**, Password:** 332063

08:30-9:30	**Opening Ceremony**
9:30-10:10	**Keynote 1:** Brain-inspired Cognitive Dynamic Systems for Engineering and Health Applications **M. Jamal Deen**, McMaster University, Canada **Chaired by:** C. L. Philip Chen, South China University of Technology, China
10:10-10:50	**Keynote 2:** Applying Machine Learning to Securing Cellular Networks **Elisa Bertino**, Purdue University, USA **Chaired by:** Xiaofeng Chen, Xidian University, China
10:50-11:10	**Coffee Break**
11:10-11:50	**Keynote 3:** Composite DP-unbias: Bounded and Unbiased Composite Differential Privacy **Jinjun Chen**, Swinburne University of Technology, Australia **Chaired by:** Mianxiong Dong, Muroran Institute of Technology, Japan
11:50-12:30	**Keynote 4:** The Super Neuron Model - New Generation Machine Learning and Applications **Moncef Gabbouj**, Tampere University, Finland **Chaired by:** Zheng Yan, Xidian University, China
12:30-14:30	**Lunch**
14:30-15:10	**Keynote 5:** AI-Native Core Network Designs **Nirwan Ansari**, New Jersey Institute of Technology, USA **Chaired by:** Weizhi Meng, Lancaster University, UK
15:10-15:50	**Keynote 6:** An Incremental-Self-Training-Guided Semi-Supervised Broad Learning System for Data Annotation **C. L. Philip Chen**, South China University of Technology, China **Chaired by:** Liming Chen, Dalian University of Technology, China
15:50-16:10	**Coffee Break**
16:10-16:50	**Keynote 7:** Explainable Knowledge Discovery with Interval Pattern Structures **Sergei Kuznetsov**, HSE University, Russia **Chaired by:** Yaliang Zhao, Henan University, China
16:50-17:30	**Keynote 8:** Towards a Hybrid Intelligent Framework for Intrusion Responses in IoT Systems **Liming Chen**, Dalian University of Technology, China **Chaired by:** Xiaokang Zhou, Kansai University, Japan
17:30-18:30	**Panel: AI Trust, Security and Privacy**
19:30-20:30	**Reception**

Thursday, December 19, 2024 (China Standard Time CST, UTC+8)						
Room	**Room 1 (Jiari)**	**Room 2 (Longtang)**	**Room 3 (Hongxia)**	**Room 4 (Zhuluo)**	**Room 5 (XINGHUA A)**	**Room 6 (XINGHUA B)**
8:00-10:00	TrustCom-1: Trust (I)	TrustCom-3: Security (II)	BigDataSE-1: Data Analytics and Processing	CSE-1: Computational Intelligence Analysis	TrustCom-5: Security (IV)	TrustCom-7: Security (VI)
10:00-10:20	**Coffee Break**					
10:20-12:20	TrustCom-2: Security (I)	TrustCom-4: Security (III)	EUC-1: Embedded and Ubiquitous Computing	iSCI-1: Smart City and Informatization	TrustCom-6: Security (V)	TrustCom-8: Security (VII)
14:00-18:00	**Outreach Academic Activities**					
19:00-21:00	**Banquet (**XINGHUA Grand Ballroom**)**					

Friday, December 20, 2024 (China Standard Time CST, UTC+8)

Room	Room 1 (Jiari)	Room 2 (Longtang)	Room 3 (Hongxia)	Room 4 (Zhuluo)	Room 5 (XINGHUA A)	Room 6 (XINGHUA B)
8:00-10:00	TrustCom-9: Privacy (I)	TrustCom-13: Emerging Tech (II)	TrustCom-17: AI Trust (III)	TrustCom-21: Security (IX)	TrustCom-25: Security (XIII)	TrustCom-29: Privacy (VI)
10:00-10:20	**Coffee Break**					
10:20-12:20	TrustCom-10: Privacy (II)	TrustCom-14: Emerging Tech (III)	TrustCom-18: AI Trust (IV)	TrustCom-22: Security (X)	TrustCom-26: Security (XIV)	TrustCom-30: Forensics and Analytics (I)
12:20-14:00	**Lunch**					
14:00-16:00	TrustCom-11: Privacy (III)	TrustCom-15: AI Trust (I)	TrustCom-19: Trust (II)	TrustCom-23: Security (XI)	TrustCom-27: Privacy (IV)	NSFC Project Meeting (I)
16:00-16:20	**Coffee Break**					
16:20-18:20	TrustCom-12: Emerging Tech (I)	TrustCom-16: AI Trust (II)	TrustCom-20: Security (VIII)	TrustCom-24: Security (XII)	TrustCom-28: Privacy (V)	NSFC Project Meeting (II)

The TrustCom-2024 Presentation Program

TrustCom-1: Trust (I)
Session Chair: Qiujie Lv (lvqiujie@zzu.edu.cn), Zhengzhou University

MAXPoWR: Memory Attestation and Export in Process-based Trusted Execution Environments
Hendrik Meyer zum Felde; Andrei Cosmin Aprodu

Trusted Networking for Drones: Reputation-Based Security Mechanisms for Node Access and Information Synchronization
Ruizhong Du; Jiajia Kang; Jin Tian

Enhancing Consistency in Container Migration via TEE: A Secure Architecture
Qingyu Gao; Liantao Song; Yan Lei; Feng Wang; Lei Wang; Shize Zong; Yan Ding

A Semi-Fragile Reversible Watermarking for 3D Models Based on IQIM with Dual-Strategy Partition Modulation
Fei Peng; Yousheng Liang; Min Long

MSMP: A Centralized Shared-memory Management for Building Efficient and Reliable File Systems on Microkernels
Feng He; Shijun Zhao; Dan Meng; Rui Hou

Blind Signature Based Anonymous Authentication on Trust for Decentralized Mobile Crowdsourcing
Wei Feng; Dongyuan Wei; Qianqian Wang

TrustCom-2: Security (I)
Session Chair: Qiujie Lv (lvqiujie@zzu.edu.cn), Zhengzhou University

CTWF: Website Fingerprinting Attack based on Compact Convolutional Transformer
Guangfa Lyu; Jian Kong; Yinglong Chen; Fengyu Wang

LSTM-Diff: A Data Generation Method for Imbalanced Insider Threat Detection
Tian Tian; Yan Zhu; Ning An; Bo Jiang; Huamin Feng; Zhigang Lu

SeChannel: A Secure and Lightweight Channel Protection Approach for TEE Systems
Nan Jiang; Yuanbo Zhao; Qihang Zhou; Xiaoqi Jia; Jing Tang

Hardware Assisted Security Gateway System: Combined with FPGA Shielding Protection
Jihong Liu; Chenyang Tu; Yifei Zhang

xIDS-EnsembleGuard: An Explainable Ensemble Learning-based Intrusion Detection System
Muhammad Adil; Mian Ahmad Jan; Safayat Bin Hakim; Houbing H Song; Zhanpeng Jin

DMA: A Persistent Threat to Embedded Systems Isolation
Jean de Bonfils Lavernelle; Pierre-Francois Bonnefoi; Benoît Gonzalvo; Damien Sauveron

TrustCom-3: Security (II)
Session Chair: Zhicai Zhang (zzcai@hainanu.edu.cn), Hainan University

StegaFDS: Generative Steganography Based on First-Order DPM-Solver
Chengyu Li; Weihai Li; Zikai Xu; Nenghai Yu

Red Team Redemption: A Structured Comparison of Open-Source Tools for Adversary Emulation
Max Landauer; Klaus Mayer; Florian Skopik; Markus Wurzenberger; Manuel Kern

VisualAuth: Secure Transaction Authentication and Trusted UI on COTS Android Devices
Mykolai Protsenko; Albert Stark; Andreas Papon; Sandra Kostic

From Data to Action: CTI Analysis and ATT&CK Technique Correlation
Duy Khanh Nguyen; Hsiching Chu; Viet Quoc Nguyen; Min-Te Sun; Kazuya Sakai; Wei-Shinn Ku

A Revocable Pairing-Free Certificateless Signature Scheme Based on RSA Accumulator
Zhuowei Shen; Xiao Kou; Taiyao Yang; Haoqin Xu; Dongbin Wang; Shaobo Niu

Face Anti-Spoofing Based on Multi-Modal Dual-Stream Anomaly Detection
Jiuyao Jing; Yu Zheng; Qi He; Chunlei Peng

TrustCom-4: Security (III)
Session Chair: Zhicai Zhang (zzcai@hainanu.edu.cn), Hainan University

Behavior Speaks Louder: Rethinking Malware Analysis Beyond Family Classification
Zhang Fei; Xiaohong Li; Sen Chen; Ruitao Feng

Vulnerabilities are Collaborating to Compromise Your System: A Network Risk Assessment Method Based on Cooperative Game and Attack Graph
Xin Deng; Rui Wang; Weihong Han; Zhihong Tian

StegoFL: Using Steganography and Federated Learning to Transmit Malware
Rong Wang; Junchuan Liang; Haiting Jiang; Chaosheng Feng; Chinchen Chang

Correcting the Bound Estimation of Mohawk
Mingjie Yu; Wei Jin; Fenghua Li; Yunchuan Guo; Zheng Yan; Xiao Wang; Nenghai Yu

OFLGI: An Optimization-based Feature-Level Gradient Inversion Attack
Yongwei Lu; Xiaoyan Liang; Ruizhong Du; Junfeng Tian

Front-running Attacks in Hash-Based Transaction Sharding Blockchains
Yusen Wang; Jiong Lou; Zihan Wang; Jie Li

TrustCom-5: Security (IV)
Session Chair: Lijun Gao (wgljsuccess@163.com), Xidian University

Multi-Authority Ciphertext-Policy Attribute-based Encryption with Hidden Policy for Securing Internet-of-Vehicles
Jie Cui; Jing Zhang; Lu Wei; Minghui Zhu; Hong Zhong; Geyong Min

WASHADOW: Effectively Protecting WebAssembly Memory Through Virtual Machine-Aware Shadow Memory
Zhuochen Jiang; Baojian Hua

Attacking High-Performance SBCs: A Generic Preprocessing Framework for EMA
Debao Wang; Yiwen Gao; Jingdian Ming; Yongbin Zhou; Xian Huang

CPCED: A Container Escape Detection System Based on CNI Plugin
Yu Hao; Xu Zhang; Dongbin Wang

Path Generation Method of Anti-Tracking Network based on Dynamic Asymmetric Hierarchical Architecture
Zhefeng Nan; Qi Wang; Changbo Tian; Yijing Wang; Tianning Zang; Dongwei Zhu

TOScorr: Transformer-based Flow Correlation Attack on Tor Onion Service
Yilin Zhu; Guang Cheng; Shunyu Zheng; Hantao Mei

TrustCom-6: Security (V)
Session Chair: Mengshuai Ma (202212083900010@hainnu.edu.cn), Hainan University

M-ETC: Improving Multi-task Encrypted Traffic Classification by Reducing Inter-task Interference
Yuwei Xu; Xiaotian Fang; Zhengxin Xu; Kehui Song; Yali Yuan; Guang Cheng

Lattice-based Multi-Stage Secret Sharing 3D Secure Encryption Scheme
Xu Li; Yinghao Wu; Yang Liu; Baosheng Wang; Bei Wang; Yijun Cui

Efficiently Detecting DDoS in Heterogeneous Networks: A Parameter-Compressed Vertical Federated Learning Approach
Cao Chen; Fenghua Li; Yunchuan Guo; Zifu Li; Wenlong Kou

Attack-Defense Graph Generation: Instantiating Incident Response Actions on Attack Graphs
Kéren A Saint-Hilaire; Christopher Neal; Frédéric Cuppens; Nora Cuppens-Boulahia; Francesca Bassi

SCENE: Shape-based Clustering for Enhanced Noise-resilient Encrypted Traffic Classification
Meijie Du; Mingqi Hu; Shu Li; Zhao Li; Qingyun Liu

GraySniffer: A Cliques Discovering Method for Illegal SIM Card Vendor Based on Multi-Source Data
Tao Leng; Chang You; Shuangchun Luo; Junyi Liu; Yutong Zeng; Cheng Huang

TrustCom-7: Security (VI)
Session Chair: Mingjun Wang (mjwang@xidian.edu.cn), Xidian University

JASFREE: Grammar-free Program Analysis for JavaScript Bytecode
Hao Jiang; Baojian Hua; Haiwei Lai; Si Wu

SyntaxBridge: Protocol Description Transformer for Enhanced Formal Analysis of Security Protocols
Liujia Cai; Tong Yu; Yumeng Li; Siqi Lu; Hanjie Dong; Guangying Cai; Guangsong Li; Yongjuan Wang

STGCN-Based Link Flooding Attack Detection and Mitigation in Software-Defined Network
Yue Li; Runcheng Fang; Qipeng Song; Xilei Yang

LayyerX: Unveiling the Hidden Layers of DoH Server via Differential Fingerprinting
Yunyang Qin; Yujia Zhu; Linkang Zhang; Baiyang Li; Yong Ding; Qingyun Liu

WCDGA: BERT-Based and Character-Transforming Adversarial DGA with High Anti-Detection Ability
Zhujie Guan; Mengmeng Tian; Yuwei Xu; Kehui Song; Guang Cheng

Towards High-Quality Electromagnetic Leakage Acquisition in Side-Channel Analysis
Xiaoran Huang; Yiwen Gao; Wei Cheng; Yuejun Liu; Jingdian Ming; Yongbin Zhou; Jian Weng

TrustCom-8: Security (VII)
Session Chair: Weizhi Meng (weme@dtu.dk), Lancaster University

Cyber Risk Analysis on Electric Vehicle Systems via NIST CSF
Spyridon Sourmelis; Weizhi Meng

EUREKHA: Enhancing User Representation for Key Hackers Identification in Underground Forums
Abdoul Nasser Hassan Amadou; Anas Motii; Saida Elouardi; EL Houcine Bergou

Few-shot Encrypted Malicious Traffic Classification via Hierarchical Semantics and Adaptive Prototype Learning
Yuan Zhao; Chunhe Xia; Tianbo Wang; Mengyao Liu; Yang Li

AIDE: Attack Inference Based on Heterogeneous Dependency Graphs with MITRE ATT&CK
Weidong Zhou; Chunhe Xia; Feng Nan; Xinyi Pan; Tianbo Wang; Xiaojian Li

From Scarcity to Clarity: Few-Shot Learning for DoH Tunnel Detection Through Prototypical Network
Beibei Feng; Qi Wang; Yijing Wang; Xiaolin Xu; Tianning Zang; Jingrun Ma

SBOM Generation Tools in the Python Ecosystem: An In-Detail Analysis
Serena Cofano; Giacomo Benedetti; Matteo Dell'Amico

Shapley-value-based Explanations for Cryptocurrency Blacklist Detection
Feixue Yan

TrustCom-9: Privacy (I)
Session Chair: Zhao Zhang (zhangzhaozm@163.com), University of Electronic Science Technology of China

Controllable Quantum Computing Privacy via Inherent Noises and Quantum Error Mitigation
Keyi Ju; Hui Zhong; Xinyue Zhang; Xiaoqi Qin; Miao Pan

Scalable Client-side Encrypted Deduplication beyond Secret Sharing of the Master Key
Yuchen Chen; Guanxiong Ha; Xuan Shan; Chunfu Jia; Qiaowen Jia

Machine Learning-based Optimal Data Trading Mechanism with Randomized Privacy Protection Scheme
Xiaohong Wu; Yujun Lin; Jie Tao; Yonggen Gu

You Are as You Type: Investigating the Influence of Timestamp Accuracy on the Robustness of Keystroke Biometrics
Florian Dehling; Luigi Lo Iacono; Sebastian Koch; Hannes Federrath

Towards Privacy-aware IoT Communications: Delegable, Revocable, and Efficient
Pengfei Wu; Jianfei Sun; Guoming Yang; Robert Deng

TrustNotify: A Lightweight Framework for Complete and Trustworthy Data Deletion Notification Distribution
Qipeng Song; Ruiyun Wang; Yue Li; Yiheng Yan; Xingyue Zhu; Hui Li

TrustCom-10: Privacy (II)
Session Chair: Qi Xia (xiaqi@uestc.edu.cn), University of Electronic Science and Technology of China

Budget-Feasible Double Auction Mechanisms for Model Training Services in Federated Learning Market
Ting Zhou; Hongtao Lv; Ning Liu; Lei Liu

VCaDID: Verifiable Credentials with Anonymous Decentralized Identities
Yalan Wang; Liqun Chen; Long Meng; Christopher J.P. Newton

A Framework for Detecting Hidden Partners in App Collusion
Qinchen Guan; Shaoyong Du; Kerong Wang; Chunfang Yang; Xiangyang Luo

Enhancing Privacy-Preserving Multi-Authority Attribute-Based Encryption: Addressing Rogue-Key Attacks Under Adaptive Corruption of Authorities
Jingchi Zhang; Anwitaman Datta

VDPSRQ: Achieving Verifiable and Dynamic Private Spatial Range Queries over Outsourced Database
Haoyang Wang; Kai Fan; Yue Quan; Fenghua Li; Hui Li

DPFCIL: Differentially Private Federated Class-Incremental Learning on non-IID Data
Fuyao Zhang; Dan Wang; Chuyang Liang

TrustCom-11: Privacy (III)
Session Chair: Jinke Wang (wangjk@henu.edu.cn), Henan University

Secure Federated Learning Schemes Based on Multi-Key Homomorphic Encryption
Wenxiu Ding; Hongjiang Guo; Zheng Yan; Mingjun Wang

TriViewNet: Achieve Accurate Tor Hidden Service Classification by Multi-view Feature Extraction and Fusion
Yuwei Xu; Jianfeng Li; Yujie Hou; Xinxu Huang; Yali Yuan; Guang Cheng

SP2-RD2D: Secure and Privacy-Preserving Authentication and Key Agreement Protocol for D2D Relay Communication
Mingjun Wang; Yixuan Liu; Wenxiu Ding

Enhanced Privacy Policy Comprehension via Pre-trained and Retrieval-Augmented Models
Xin Zhang; Bingbing Zhang; Chi Zhang; Lingbo Wei

MIND: A Privacy-Preserving Model Inference Framework via End-Cloud Collaboration
Siyuan Guan; Ziheng Hu; Guotao Xu; Yao Zhu; Bowen Zhao

Analyzing Relationship Consistency in Digital Forensic Knowledge Graphs with Graph Learning
Ruoyao Xiao; Yu Luo; Frank Xu; Harshmeet Lamba; Dianxiang Xu

TrustCom-12: Emerging Tech (I)
Session Chair: Yuheng Zhang (zyuhang@e.gzhu.edu.cn), Guangzhou University

TransFront: Bi-path Feature Fusion for Detecting Front-running Attack in Decentralized Finance
Yuheng Zhang; Guojun Wang; Peiqiang Li; Xubin Li; Wanyi Gu; Mingfei Chen; Houji Chen

RAG-based Cyber Threat Tracing Graph Modeling Method
Jonghee Jeon; Jahoon Koo; Young-Gab Kim

AdaptFL: Adaptive Client Task Allocation-Based Synchronous Federated Learning
Xiaoshuang Li; Mingjun Wang; Yilong Guo; Wenxiu Ding

TierFlow: A Pipelined Layered BFT Consensus Protocol for Large-Scale Blockchain
Yongkang Yu; Jinchun He; Xinwei Xu; Qinnan Zhang; Wangjie Qiu; Hongwei Zheng; Binghui Guo; Jin Dong

ClusterX: Adaptive Collaborative Scheduling of Layered User-Proxy Mapping to Enhance DDoS Defense in Distributed Clusters
Jianbo Lin; Lin Yan; Zhi Lin; Zan Zhou; Shujie Yang

New Compact Construction of FHE from Cyclic Algebra LWE
Yuan Liu; Licheng Wang; Yongbin Zhou

TrustCom-13: Emerging Tech (II)
Session Chair: Rui Zhang (zhangrui03@xidian.edu.cn), Xidian University

Rethinking Mutation Strategies in Fuzzing Smart Contracts
Jingzhang Cao; Meng Wang; Shenao Lin

Towards a Robust Medical Record System: Integrating Logical Reasoning for Trustworthy Data Management
Hanning Zhang; Guansheng Wang; Junwei Feng; Lei Feng; Quan Gan; Long Ji

CVchain: A Cross-Voting-based Low Latency Parallel Chain System
Jianrong Wang; Yacong Ren; Dengcheng Hu; Qi Li; Sen Li; Xuewei Li; Xiulong Liu

A Novel Time Series Approach to Anomaly Detection and Correction for Complex Blockchain Transaction Networks
Qi Xia; Ansu Badjie; Jianbin Gao; Grace Mupoyi; Hu Xia; Isaac Obiri

A Sustainable Storage Compensation Method for Consortium Blockchain-based Computing Power Trading
Guangzhuo Zhu; Qian Wang; Bei Gong

A High-Accuracy Multi-View Unknown Traffic Identification Method Based on Contrastive Learning
Yuwei Xu; Zizhi Zhu; Chufan Zhang; Kehui Song; Guang Cheng

TrustCom-14: Emerging Tech (III)
Session Chair: Rui Zhang (zhangrui03@xidian.edu.cn), Xidian University

Attacking High-order Masked Cryptosystem via Deep Learning-based Side-Channel Analysis
Zelong Zhang; Wei Cheng; Yongbin Zhou; Zehua Qiao; Yuhan Zhao; Jian Weng

Efficient and Accurate Min-entropy Estimation Based on Decision Tree for Random Number Generators
Yuan Ma; Maosen Sun; Wei Wang; Tianyu Chen; Na Lv; Dongchi Han

User Authentication Based on the Integration of Musical Signals and Ear Canal Acoustics
Tongxi Chen; Weizhi Meng; Wenjuan Li

Multiplicative Masked M&M: An Attempt at Combined Countermeasures with Reduced Randomness
Kaiyuan Li; Haruka Hirata; Daiki Miyahara; Kazuo Sakiyama; Yuko Hara-Azumi; Yang Li

Multi-Channel Leakage Detection Based on Chi-square Test of Independence
Xiaoyong Kou; Gongxuan Zhang

MVSS: Blockchain Cross-shard Account Migration Based on Multi-version State Synchronization
Weihan Wang; Xiulong Liu; Liyuan Ma; Hao Xu; Gaowei Shi; Juncheng Ma; Keqiu Li

TrustCom-15: AI Trust (I)
Session Chair: Ruiying Lu (luruiying@xidian.edu.cn), Xidian University

Enhancing Adversarial Robustness through Self-Supervised Confidence-Based Denoising
Yongkang Chen; Tong Wang; Wei Kong; Taotao Gu; Guiling Cao; Xiaohui Kuang

A Knowledge Graph Completion Method Based on Gated Adaptive Fusion and Conditional Generative Adversarial Networks
Zhixuan Zhang; Yanhui Zhu; Yuezhong Wu; Fangteng Man; Hao Chen; Xujian Ying

MARS: Robustness Certification for Deep Network Intrusion Detectors via Multi-Order Adaptive Randomized Smoothing
Mengdie Huang; Yingjun Lin; Xiaofeng Chen; Elisa Bertino

GTree: GPU-Friendly Privacy-preserving Decision Tree Training and Inference
Qifan Wang; Shujie Cui; Lei Zhou; Ye Dong; Jianli Bai; Yun Sing Koh; Giovanni Russello

RTS: A Training-time Backdoor Defense Strategy Based on Weight Residual Tendency
Fan Xiang; Xueyang Li; Guozhu Meng

Trustworthiness and Path Regularity Based Contrastive Learning for Noisy Knowledge Graph Error Assertion Detection
Zhuohan Ao; Yi Wang; Ying Wang; Yu Zhan

TrustCom-16: AI Trust (II)
Session Chair: Jinke Wang (wangjk@henu.edu.cn), Henan University

RPG-Diff: Precise Adversarial Defense Based on Regional Positioning Guidance
Haotian Wang; Jing Liu

Toward Privacy-Preserving and Verifiable XGBoost Training for Horizontal Federated Learning
Wei Xu; Hui Zhu; Chang Xiao; Fengwei Wang; Dengguo Feng; Hui Li

Local Drift Correction and Attention Aggregation for Self-Organized Federated Learning
Haiying Liu; Ruichun Gu; Jingyu Wang; Xiaolin Zhang; Bolin Zhang; Xuebao Li

Boosting Transferability of Adversarial Examples by Joint Training and Dual Feature Mixup
Mengmeng Tang; Shuhong Chen; Guojun Wang; Hanjun Li; Zhuyi Yao; Sheng Wen

Federated Unlearning for Samples Based on Adaptive Gradient Ascent of Angles
Ying Hua; Hui Xia; Shuo Xu

Membership Inference Attacks via Dynamic Adversarial Perturbations Reduction
Zehua Ding; Youliang Tian; Guorong Wang; Jinbo Xiong; Jianfeng Ma

TrustCom-17: AI Trust (III)
Session Chair: Yu Zheng (yzheng@xidian.edu.cn), Xidian University

Defending Against Backdoor Attacks through Causality-Augmented Diffusion Models for Dataset Purification
Yuefeng Lai; Lizhao Wu; Lin Hui

LLM4MDG: Leveraging Large Language Model to Construct Microservices Dependency Graph
Jiekang Hu; Yakai Li; Zhaoxi Xiang; Luping Ma; Xiaoqi Jia; Qingjia Huang

StrucTrans: Zero-Query Structural Adversarial Attack Transferred from Masked Autoencoders to Image Classifiers
Yi Ji; Isao Echizen

A GPU-Based Privacy-Preserving Machine Learning Acceleration Scheme
Jie Hou; Zengrui Huang; Zhiyong Zhang; Wei Zhang; Lei Ju

A Low-cost Black-box Jailbreak Based on Custom Mapping Dictionary with Multi-round Induction
Feng Wu; Weiqi Wang; Youyang Qu; Shui Yu

TTFL: Towards Trustworthy Federated Learning with Arm Confidential Computing
Lizhi Sun; Jingzhou Zhu; Boyu Chang; Yixin Xu; Bo Yang; Hao Wu; Fengyuan Xu; Sheng Zhong

TrustCom-18: AI Trust (IV)
Session Chair: Xuyang Jing (jingxuyang@xidian.edu.cn), Xidian University

Topic-Aware Sensitive Information Detection in Chinese Large Language Model
Yalin Sun; Ruiying Lu; Kang Li; Yu Zheng

UNIRE: Secure Trajectory-User Linking Model Aggregation with Knowledge Transfer
Jiezhen Tang; Hui Zhu; Yandong Zheng; Junpeng Zhang; Fengwei Wang; Jiaqi Zhao; Hui Li

Zephyr: A High-Performance Framework for Graph Attention Networks on Heterogeneous Data
Wenxiu Ding; Muzhi Liu; Yuxuan Cai; Mingxing Chen; Zheng Yan; Mingjun Wang

AS-FIBA: Adaptive Selective Frequency-Injection for Backdoor Attack on Deep Face Restoration
Zhenbo Song; Wenhao Gao; Zhenyuan Zhang; Jianfeng Lu

CertRob: Detecting PDF Malware with Certified Adversarial Robustness via Randomization Smoothing
Lijun Gao; Zheng Yan

Paa-Tee: A Practical Adversarial Attack on Thermal Infrared Detectors with Temperature and Pose Adaptability
Zhangchi Zhao; Jianyi Zhang; Liqun Shan; Ziyin Zhou; Kaiying Han; Xiali Hei

TrustCom-19: Trust (II)
Session Chair: Raphael Antonius Frick (Raphael.frick@sit.fraunhofer.de), Fraunhofer SIT, ATHENE Center

T-ABE: A practical ABE scheme to provide trustworthy key hosting on untrustworthy cloud
Shuaishuai Chang; Yuzhe Li; Bo Li; Jinchao Zhang

Three-Body Problem: An Empirical Study on Smartphone-based TEEs, TEE-based Apps, and their Interactions
Xianghui Dong; Yin Liu; Xuejun Yu

A Trust Model with Fitness-Based Clustering Scheme in FANETs
Junqiao Gao; Chaklam Cheong; Mansi Zhang; Yue Cao; Tao Peng; Shahbaz Pervez

TWCF: Trust Weighted Collaborative Filtering based on Quantitative Modeling of Trust
Wenting Song; K. Suzanne Barber

Analyzing the Effectiveness of Image Preprocessing Defenses Under Runtime Constraints
Niklas Bunzel; Gerrit Klause

FedSGProx: Mitigating Data Heterogeneity and Isolated Nodes in Graph Federated Learning
Xutao Meng; Qingming Li; Yong Li; Li Zhou; Xiaoran Yan

TrustCom-20: Security (VIII)
Session Chair: Mingshuai Sheng (mingshuai@hainanu.edu.cn), Hainan University

Designing Secret Embedding Scheme Based on Bitcoin Transactions Pattern Controlling
Zheng Feng; Chunyu Xing; Chen Liang

Perturbing Vulnerable Bytes in Packets to Generate Adversarial Samples Resisting DNN-Based Traffic Monitoring
Jie Cao; Zhengxin Xu; Yunpeng Bai; Yuwei Xu; Qiao Xiang; Guang Cheng

Enabling Robust Android Malicious Packet Capturing and Detection via Android Kernel
Mingyang Li; Weina Niu; Xinglong Chen; Jiacheng Gong; Kegang Hao; Xiaosong Zhang

Signcryption based on Elliptic Curve CL-PKC for Low Earth Orbit Satellite Security Networking
Meiling Chen; Yuanyuan Yang; Sixu Guo; Jin Cao; Haitao Du; Li Su

A Multi-hop Reasoning Framework for Cyber Threat Intelligence Knowledge Graph
Kai Zhou; Yong Xie; Xin Liu

LSD Attack: Exploiting Inconsistencies between Design and Implementation of Ethereum Protocols
Chenyu Li; Xiu Zhang; Xueping Liang; Xiaorui Gong

TrustCom-21: Security (IX)
Session Chair: Mingshuai Sheng (mingshuai@hainanu.edu.cn), Hainan University

Lightweight Leakage-Resilient Authenticated Key Exchange for Industrial Internet of Things
Wenxin Jia; Zheng Yang; Zhiqiang Ma

ConfigKG: Identify Routing Security Issues from Configurations based on Knowledge Graph
Pengfei Li; Yujing Liu; Jinshu Su; Bo Yu

CaptchaSAM: Segment Anything in Text-based Captchas
Yijun Wang; Ziyi Zhou; Weiqi Bai; Ruijie Zhao; Xianwen Deng

Tibetan microblogging user data analysis and topic identification
Guixian Xu; Wenhui Gao

Security Enhancement of UAV Swarm Empowered Downlink Transmission with Integrated Sensing and Communication
Runze Dong; Buhong Wang; Jiang Weng; Kunrui Cao; Jiwei Tian; Tianhao Cheng

SimLog: System Log Anomaly Detection Method Based on Simhash
Weiping Wang; Huijuan Wang; Yulu Hong; Chenyu Wang; Hong Song; Shigeng Zhang

TrustCom-22: Security (X)
Session Chair: Panpan Han (823518295@qq.com), Xidian University

FREDet: Fine-Grained Malicious Traffic Detection Based on Frequency Domain Features
Zekai Song; Yunpeng Li; Jian Qin; Changzhi Zhao; Dongxu Han; Yuling Liu

Android Malware Detection Technology Based on SC-ViT and Multi-Feature Fusion
Qiulong Yu; Zhiqiang Wang; Lei Ju; Sicheng Yuan; Ying Zhang

SBCM: Semantic-Driven Reverse Engineering Framework for Binary Code Modularization
Shuang Duan; Hui Shu; Zihan Sha; Yuyao Huang

A Multi-Blockchain Based Anonymous Cross-Domain Authentication Scheme for Industrial Internet of Things
Chengqi Hou; Wei Yang; Yu Wang; Zhiming Zhang; Shaolong Chen; Beibei Li

Deep Learning-based DDoS Attack. Detection Using Adversarial Optimization
Dahai Yu; Jianming Cui; Yungang Jia; Peiguo Fu; Ming Liu

Security Assessment of Customizations in Android Smartwatch Firmware
Yifan Yu; Ruoyan Lin; Shuang Li; Qinsheng Hou; Peng Tang; Wenrui Diao

TrustCom-23: Security (XI)
Session Chair: Bo Liu (liubo@zzu.edu.cn), Zhengzhou University

Sec-Reduce: Secure Reduction of Redundant and Similar Data for Cloud Storage based on Zero-Knowledge Proof
Zhihuan Yang; Wenlong Tian; Emma Zhang; Zhiyong Xu

Private Data Aggregation Enabling Verifiable Multisubset Dynamic Billing in Smart Grids
Qian Yang; Chen Wang; Jian Shen; Yi Li; Dengzhi Liu

Custom Permission Misconfigurations in Android: A Large-Scale Security Analysis
Rui Li; Wenrui Diao; Debin Gao

Orchestrating Security Protection Resource for Space-Ground Integrated Networks
Dongbin Chen; Yunchuan Guo; Xiao Wang; Fenghua Li; Zifu Li

Phase Shift Matrix Optimization and Channel Quantization Alternating in RIS-Assisted Physical Layer Key Generation
Liquan Chen; Yufan Song; Wanting Ma; Tianyu Lu; Peng Zhang

BWG: An IOC Identification Method for Imbalanced Threat Intelligence Datasets
Juncheng Lu; Yiyang Zhao; Wang Yan; Jiyuan Cui; Sanfeng Zhang

TrustCom-24: Security (XII)
Session Chair: Bo Liu (liubo@zzu.edu.cn), Zhengzhou University

Network Traffic Anomaly Detection Method Based on CTA-BiLSTM
Wenlong Liu; Bin Wen; Mengshuai Ma; Wanrong Du

Decentralized and Lightweight Cross-Chain Transaction Scheme based on Proxy Re-signature
Huiying Zou; Jia Duan; Xi Liu; Wei Ren; Tao Li; Xianghan Zheng; Kim-Kwang Raymond Raymond Choo

LLMUZZ: LLM-based Seed Optimization for Black-box Device Fuzzing
Guangming Gao; Shuitao Gan; Xiaofeng Wang; Shengkai Zhu

FCSec: An Open-source Testbed for Security Evaluation on UAV Communications
Indu Chandran; Mukesh Narayana Gadde; Vipin Kizheppatt

Active Defense Research: A New Perspective Integrating Traps and Vulnerabilities
Quan Hong; Yang Yu; Lvyang Zhang; Lidong Zhai

Enhancing Graph-Based Vulnerability Detection through Standardized Deep Learning Pipelines
Jiashun Hao; Young-Woo Kwon

TrustCom-25: Security (XIII)
Session Chair: Shufan Fei (shufanfei@gmail.com), Xidian University

OSN Bots Traffic Transformer: MAE-Based Multimodal Social Bots Behavior Pattern Mining
Haonan Zhai; Ruiqi Liang; Zhenzhen Li; Zhen Li; Wei Xia; Bingxu Wang; Qingya Yang

Enhancing Higher-Order Masking: A Faster and Secure Implementation to Mitigate Bit Interaction Leakage
Jiahao Zhang; Yuejun Liu; Jingdian Ming; Yiwen Gao; Yongbin Zhou; Debao Wang

Towards Securing ASCON Implementation by Inner Product Masking
Yuming Liu; Wei Cheng; Jihao Fan; Yongbin Zhou

A Novel zk-SNARKs Method for Cross-chain Transactions in Multi-chain System
Pengcheng Xia; Jingyu Wu; Yiyang Ni; Jun Li

LAPAID: A Lightweight, Adaptive and Perspicacious Active Intrusion Detection Method on Network Traffic Streams
Bin Li; Li Cheng; Zhongshan Zhang; Yu Pan; Feng Yao; Renjie He

WhisperMQTT: Lightweight Secure Communication Scheme for Subscription-Heavy MQTT Network
Youbin Kim; Man-Ki Yoon

TrustCom-26: Security (XIV)
Session Chair: Shufan Fei (shufanfei@gmail.com), Xidian University

A Reliable Encrypted Traffic Classification Method Based on Attention Mechanisms
Zhijun Wu; Shanhe Niu; Meng Yue

USB Catcher: Detection of Controlled Emissions via Conducted Compromising Emanations
Yixin Zhang; Fuqiang Du; Xinge Chi; Zhiqiang Lv

Improving Security in Internet of Medical Things through Hierarchical Cyberattacks Classification
Hong-Hanh Nguyen-Le; Nhien-An Le-Khac; Vince Noort

Privacy-Preserving Secure Neighbor Discovery for Wireless Networks
Ahmed Mohamed Hussain; Panagiotis Papadimitratos

D3IR: Securing Multi-Domain Networks via Extending Depth-in-Defense Strategies Across Nested Management Domains
Yaobing Xu; Yunchuan Guo; Wenlong Kou; Junhai Yang; Ziyan Zhou; Fenghua Li

BGAS: Blockchain and Group Decentralized Identifiers Assisted Authentication Scheme for UAV Networks
TingYu Wang; Qiang Cao; Shihong Zou; Yueming Lu

TrustCom-27: Privacy (IV)
Session Chair: Xuemei Fu (15931012973@163.com), Hainan University

Sparse Silhouette Jump: Adversarial Attack Targeted at Binary Image for Gait Privacy Protection
Jiayi Li; Ke Xu; Xinghao Jiang; Tanfeng Sun

Real-time Private Data Aggregation over Distributed Spatial-temporal Infinite Streams with Local Differential Privacy
Xingxing Xiong; Shubo Liu; Xiping Liu; Xiaoguang Niu; Wenyu You

Enhancing IoT Privacy: Why DNS-over-HTTPS Alone Falls Short?
Samuel Pélissier; Gianluca Anselmi; Abhishek Kumar Mishra; Anna Maria Mandalari; Mathieu Cunche

Efficient FSS-based Private Statistics for Traffic Monitoring
Zhichao Wang; Qi Feng; Min Luo; Xiaolin Yang; Zizhong Wei

Efficient and Practical Multi-party Private Set Intersection Cardinality Protocol
Shengzhe Meng; Xiaodong Wang; Zijie Lu; Bei Liang

An Efficient and Privacy-Preserving Participant Selection Scheme based on Location in Mobile Crowdsensing
Yudan Cheng; Tao Feng; Zhiquan Liu; Guo Xian; Lulu Han; Jianfeng Ma

TrustCom-28: Privacy (V)
Session Chair: Xuemei Fu (15931012973@163.com), Hainan University

NAGG: Noised Graph Node Feature Aggregations for Preserving Privacy
Yinghao Song; Long Yan; Yang Li; Mingjian Ni; Shengzhong Tan; Dazhong Li; Huiting Zhao; Yulun Song

EffiTaint: Boosting Sensitive Data Tracking with Accurate Taint Behavior Modeling and Efficient Access Path Optimization
Haocheng Li

A Quiet Place: An In-Depth Study of Mobile Public-to-Private Attacks
Yin Liu

Single-sign-on Authentication with Anonymous Token and Restricted Covert Channel
Zhao Zhang; ChunXiang Xu; Man Ho Au

DMASP: Dynamic Multi-keyword Searchable Encryption for Protected Access and Search Patterns with Differencial Privacy
Yue Quan; Kai Fan; Haoyang Wang; Hui Li; Yintang Yang

Research on Intelligent Joint Detection Technology for Application Privacy Behavior Compliance
Ruoding Zhang; Tao Liu; Qifeng Shi; Yan Zhang; Xinrui Geng; Xiaoyi Song

TrustCom-29: Privacy (VI)
Session Chair: Fang Fu (fufang0621@hainanu.edu.cn), Hainan University

Multi-Dimensional Data Collection Under Personalized Local Differential Privacy
Kunpeng Song; Mingzhang Sun; Kui Zhou; Peng Tang; Ning Wang; Shanqing Guo

Interactive Verifiable Local Differential Privacy Protocols for Mean Estimation
Liang Wang; Li Liu; Pei Zhan; Peng Tang; Puwen Wei; Shanqing Guo

CFE: Secure Filtered Words in End-to-End Encrypted Messaging System
Tran Viet Xuan Phuong; Albert Baker; Jan P Springer; Philip Huff; Tho Thi Ngoc Le

Privacy-Preserving Multi-Soft Biometrics through Generative Adversarial Networks with Chaotic Encryption
Hongying Zheng; Hongdie Li; Di Xiao; Maolan Zhang

Data Privacy-Preserving and Communication Efficient Federated Multilinear Compressed Learning
Di Xiao; Zhuyan Yang; Maolan Zhang; Lvjun Chen

Secure Join and Compute in Encrypted Database
Tanusree Parbat; Ayantika Chatterjee

TrustCom-30: Forensics and Analytics (I)
Session Chair: Fang Fu (fufang0621@hainanu.edu.cn), Hainan University

Dycom: A Dynamic Community Partitioning Technique for System Audit Logs
Zhaoyang Wang; Yu Wen; Yanfei Hu; Boyang Zhang; Shuailou Li; Wenbo Wang; Lisong Zhang; Dan Meng

Who Owns the Cloud Data? Exploring a non-interactive way for secure proof of ownership
Zhihuan Yang; Wenlong Tian; Ruixuan Li; Xuming Ye; Zhiyong Xu

Peering Through the Veil: A Segment-Based Approach for VPN Encapsulated Video Title Identification
Zhenyu Xu; Xurui Ren; Yi Zhang; Guang Cheng; Hua Wu

SecureNet-AWMI: Safeguarding Network with Optimal Feature Selection Algorithm
Ming Zhou; Zhijian Zheng; Peng Zhang; Sixue Lu; Yamin Xie; Zhongfeng Jin

Enhancing Information Gathering: An Extensible Framework for Automated Metadata Extraction
Arcangelo Castiglione; Raffaele Pizzolante; Francesco Palmieri

Towards Understanding and Detecting File Types in Encrypted Files for Law Enforcement Applications
Adam Hooker; Wenjian Huang; Shalini Kurumathu; Nishant Vishwamitra; Kim-Kwang Raymond Raymond Choo

TrustCom-31: Emerging Tech (IV)
Session Chair: Yijia Liu (liuyijia42@foxmail.com), Xidian University

Broader but More Efficient: Broad Learning in Power Side-channel Attacks
Yilin Yang; Changhai Ou; Yongzhuang Wei; Wei Li; Yifan Fan; Xuan Shen

BedIDS: An Effective Network Anomaly Detection Method by Fusing Behavior Evolution characteristics
Zhen Liu; Changzhen Hu; Chun Shan; Junkai Yi

Leveraging Large Language Models for Challenge Solving in Capture-the-Flag
Yuwen Zou; Yang Hong; Jingyi Xu; Lekun Liu; Wenjun Fan

Efficient and Verifiable Dynamic Skyline Queries in Blockchain Networks
Bo Yin; Hang Chen; Binyao Xu; Mariam Suleiman Silima; Ke Gu

Enhancing Security and Privacy in Connected and Autonomous Vehicles: A Post-Quantum Revocable Ring Signature Approach
Qingmei Yang; Pincan Zhao; Yuchuan Fu; F. Richard Yu

Leveraging Semi-supervised Learning for Enhancing Anomaly-based IDS in Automotive Ethernet
Jia Liu; Wenjun Fan; Yifan Dai; Eng Gee Lim; Zhoujin Pan; Alexei Lisitsa

TrustCom-32: Emerging Tech (V)
Session Chair: Jieming Yang (yjmlaile@gmail.com), Zhengzhou University

Robust Hardware Trojan Detection: Conventional Machine Learning vs. Graph Learning Approaches
Liang Hong; Xingguo Guo; Zeyar Aung; Wei Hu

UniTTP: A Unified Framework for Tactics, Techniques, and Procedures Mapping in Cyber Threats
Jie Zhang; Hui Wen; Lun Li; Hongsong Zhu

HTV: Measuring Circuit Vulnerability to Hardware Trojan Insertion Based on Node Co-activation Analysis
Shuiliang Chai; Zhanhui Shi; Yanjiao Gao; Yuhao Huang; Aizhu Liu; Jie Xiao

An Intelligent Affinity Strategy for Dynamic Task Scheduling in Cloud-Edge-End Collaboration
Jingsen Zhang; Shoulu Hou; Yi Gong; Tao Wang; Changyuan Lan; Xiulei Liu

Hierarchical Graph Feature Extraction Based on Multi-Information Contract Graph for Enhanced Smart Contract Vulnerability Detection
Tao Fang; Hou Zhihao; Jiahao He; Junjie Zhou; Zhao Gansen

LightRL-AD: A Lightweight Online Reinforcement Learning Approach for Autonomous Defense against Network Attacks
Fengyuan Shi; Zhou Zhou; Jiang Guo; Renjie Li; Zhongyi Zhang; Shu Li; Qingyun Liu; Xiuguo Bao

TrustCom-33: Emerging Tech (VI)
Session Chair: Qixian Ren (qxren307@gmail.com), Xidian University

SPDID: A Secure and Privacy-Preserving Decentralized Identity utilizing Blockchain and PUF
Yueyue He; Wenxuan Fan; Koji Inoue

Enhancing Security and Efficiency in Vehicle-to-Sensor Authentication: A Multi-Factor Approach with Cloud Assistance
Xinrui Zhang; Pincan Zhao; Jason Jaskolka

AdvPurRec: Strengthening Network Intrusion Detection with Diffusion Model Reconstruction Against Adversarial Attacks
Nour Alhussien; Ahmed AlEroud

Privacy Leak Detection in LLM Interactions with a User-Centric Approach
Tan Su; Bingbing Zhang; Chi Zhang; Lingbo Wei

HFI: High-Frequency Component Injection based Invisible Image Backdoor Attack
Huanlai Xing; Xuxu Li; Jing Song; Lexi Xu; Jincheng Peng; Bowen Zhao; Li Feng

From Liberty to 1984: A Methodology for Systematically Deteriorating LLM Outputs through Habituation Tendencies
Dong Zhang

TrustCom-34: AI Trust (V)
Session Chair: Lijun Gao (wgljsuccess@163.com), Xidian University

Attack Data is Not Solely Paramount: A Universal Model Extraction Enhancement Method
Chuang Liang; Jie Huang

Active Source Inference Attack Based on Label-Flipping in Federated Learning
Lening Zhang; Hui Xia

A Universally Composable Key Management System Using Trusted Hardware
Zhenghao Lu; Ding Ma; Lei Fan; Xiuzhen Chen; Yongshuai Duan; Jia Zhang

Achieving Trusted GPU Allocation: An Empirical Study on Efficiency Changes of Deep Learning Training Tasks
Ziheng Zhang; Lei Liu; Zhongmin Yan

THEF: A Privacy-Preserving Framework for Transformer Inference leveraging HE and TEE
Zehao Li; Jiachun Liao; Jinhao Yu; Lei Zhang

DMPA: A Compact and Effective Pipeline for Detecting Multiple Phishing Attacks
Xiaodong Huang; Gangliang Li; Chengfeng Chen; Shouqiang Liu

TrustCom-35: AI Trust (VI)
Session Chair: Jiahe Lan (jiahelan@foxmail.com), Xidian University

Learning Robust and Repeatable Physical Camouflage for Aerial Object Detectors
Zilong He; Hua Zhang

FedNIFW: Non-Interfering Fragmented Watermarking for Federated Deep Neural Network
Haiyu Deng; Xiaocui Dang; Yanna Jiang; Xu Wang; Guangsheng Yu; Wei Ni; Renping Liu

An Effective Adversarial Text Attack through a Block-Sparse Approach with Hamiltonian Insights
Xiang Sun; Zhang Yaling; Yichuan Wang; Chen Zhao; Dongtai Tang

End-to-End Speaker Anonymization Based on Location-Variable Convolution and Multi-Head Self-Attention
Feiyu Zhao; Jianguo Wei; Wenhuan Lu; Yongwei Li

DUDPA-TATD: A Lightweight Privacy-Preserving Anomaly Traffic Detection Method for Edge Computing Scenarios
Guanghan Li; Wenzhong Yang; Xiaodan Tian; Jiaren Peng

Defending Against Model Poisoning Attacks in Federated Learning via Client-guided Trust
Xiangxiang Wang; Hui Xia; Yingqi Zhang

TrustCom-36: AI Trust (VII)
Session Chair: Jiahe Lan (jiahelan@foxmail.com), Xidian University

Abstraction-Based Training for Robust Classification Models via Image Pixelation
Yang Chen; Min Zhang; Min Wu

FusTP-FL: Enhancing Differential Federated Learning through Personalized Layers and Data Transformation
Xiong Yan; Kedong Yan; Chanying Huang; Dan Yin; Shan Xiao

Large Language Model and Behaviour Tree Based Real-world Test Scenario Generation for Autonomous Vehicles
Yuliang Li; Zhonglin Hou; Hong Liu

Robust Purification Defense for Transfer Attacks Based on Probabilistic Scheduling Algorithm of Pre-trained Models: A Model Difference Perspective
Xinlei Liu; Jichao Xie; Tao Hu; Hailong Ma; Baolin Li; Yi Peng; Zhen Zhang

Individual Fair Density-peaks Clustering Based on Local Similar Center Graph and Similar Decision Matrix
Yiding Tang; Zhijing Yang; Yufan Peng; Hui Zhang

D^2FL: Dimensional Disaster-oriented Backdoor Attack Defense of Federated Learning
Yilong Li; Jianyi Zhang; Ziyin Zhou; Zezheng Sun; Xu Ji; Zeping Li; Jiameng Han; Zhangchi Zhao

TrustCom-37: Trust (III)
Session Chair: Yijia Liu (liuyijia42@foxmail.com), Xidian University

Improved Rectangle and Linear Attacks on Lightweight Block Cipher WARP
Yaxin Cui; Hong Xu; Zhichao Xu

SAMOC: Enabling Atomic Invocations for Cross-chain Crowdsourcing Testing DApps in Industrial Control Through Trusted Smart Community and Lock Mechanism
Weiguo Huang; Yong Ding; Jun Li; Yujue Wang; Hai Liang; Changsong Yang

Trustworthy Analysis of Drain3-based Cold Storage Behavior in Judicial Depository Scenarios
Xiangyu Meng; Xuejun Yu

FCADD: Robust Watermarking Resisting JPEG Compression with Frequency Channel Attention and Distortion De-gradient
Dong Yang; Weihai Li; Zikai Xu; Zhiling Zhang; Yiling Chen

ASK-LTL Checker: A Tailored Model Checker for Linear Temporal Logic of CPN State Space
Jing Li; Tao Sun; Wenjie Zhong

Sustainable and Trusted Vehicular Energy Trading Enabled by Scalable Blockchains
Qingmei Yang; Lijun Sun; Xiao Chen; Lingling Wang

TrustCom-38: Security (XV)
Session Chair: Jie Wang (jiewang_xidian@163.com), Xidian University

DyGCN: Dynamic Graph Convolution Network-based Anomaly Network Traffic Detection
Yonghao Gu; Xiaoqing Zhang; Hao Xu

ROSE^+: A Robustness-Optimized Security Scheme Against Cascading Failures in Multipath TCP under LDDoS Attack Streams
Jinquan Nie; Lejun Ji; Yirui Jiang; Yong Ma; Yuanlong Cao

A Novel Approach to Network Traffic Analysis: the HERA Tool
Daniela Pinto; Ivone Amorim; Eva Maia; Isabel Praça

Machine Learning-Based Power Allocation Optimization Algorithm for Enhanced CR-NOMA Network
Yu Fu; Bingcai Chen; Qian Ning; Kai Lin

A Self-Adaptive Framework for Responding to Uncertainty in Access Control Process with Deep Neural Networks
Jihoon Park; Giluk Kang; Young-Gab Kim

Efficient DDoS Detection and Mitigation in Cloud Data Centers Using eBPF and XDP
Ziyue Chen; He Kong; Ding Shuai; Quanfeng Lv; Wei Guo

TrustCom-39: Security (XVI)
Session Chair: Ruonan Zhao (rn_zhao@zzu.edu.cn), Zhengzhou University

A LLM-based Agent for the Automatic Generation and Generalization of IDS Rules
Xiaowei Hu; Haoning Chen; Huaifeng Bao; Wen Wang; Feng Liu

A Self-Supervised Targeted Process Anomaly Detection Method Based on the Minimum Set of Observed Events
Haojun Xia; Limin Sun; Wenliang Liu; Jingyi Xie; Zhanwei Song; Bibo Tu

GeMuFuzz: Integrating Generative and Mutational Fuzzing with Deep Learning
Yuqi Zhai; Rui Ma; Zheng Zhang; Yuche Yang; Siqi Zhao; Hongming Chen

A Cross-Site Scripting Attack Protection Framework Based on Managed Proxy
Cheng Tang; Guozhen Cheng; Hao Liang; Jianhua Peng; Meiyue Yang; Wenyan Liu; Ming Liu; Lei Sha; Qingfeng Wang

IoT Device Fingerprinting from Periodic Traffic Using Locality-Sensitive Hashing
Jianhui Ming; Weiping Wang; Linlin Zhang; Yingjie Hu; Shigeng Zhang

SGCML: Detecting Hacker Community Hidden in Chat Group
Tao Leng; Junyi Liu; Yang Zhen; Chang You; Yutong Zeng; Cheng Huang

TrustCom-40: Security (XVII)
Session Chair: Ruonan Zhao (rn_zhao@zzu.edu.cn), Zhengzhou University

DA-CPVD: Vulnerability Detection Method Based on Dual Attention Composite Pooling
Mengxuan Shi; Jinfu Chen; Saihua Cai; Ziyan Liu; Jiapeng Zhou

Cyber Resilience Framework for Web Server
Wanqiu Zhou; Zheng Zhang; Yuan Yao; Jiang Wang; Jiaxin Ma; Hui Liu

Improved Packet-Level Synthetic Network Traffic Generation
Jacob Soper; Yue Xu; Ernest Foo; Zahra Jadidi; Kien N Thanh

Exploring Permission Control Flaws in Mini-apps
Jun Li; Yuting Zhang; Wu Zhou; Shenzhi Zhang

Maldet: An Automated Malicious npm Package Detector Based on Behavior Characteristics and Attack Vectors
Yu Zhang; Haipeng Qu; Lingyun Ying; Linghui Wang

An Adaptive Reputation Update Mechanism for Primary Nodes in PBFT
Limin Yu; Yongdong Wu; Tong LI; Jiao Lu

TrustCom-41: Security (XVIII)
Session Chair: Chaoming Shi (cmshi_xd@163.com), Xidian University

Rabbit: Secure Encrypted Property Graph Search Scheme Supporting Data and Key Updates
Yingying Wu; Jiabei Wang; Dandan Xu; Yongbin Zhou; Yang Wang

Malware Traffic Classification Based on Multidimensional Features Learning
Yijie Huang; Wei Ding; Mian Huang

ADIoT: An Anomaly Detection Model for IoT Devices Based on Behavioral Feature Analysis
Liang Wang; Zhipeng Wang; Meng Wang

Detection of Sensitive Information Based on Transient Data in Store Buffer and Cache
Yan Chang; Yaqin Wu; Jianwu Rui; Ming Cao; Yawei Yue; Yu Feng; Tingting He; Haihui Gao; Zhen Lv

Unsupervised Evaluation Method of Relative Coordination Degree from Group Perspective
Chenghan Zhang; Yan Liu; Daofu Gong; Ling Wang

DTAME: A Interpretable and Efficient Approach for ABAC Policy Mining and Evaluation Using Decision Trees
Zejun Lan; Jianfeng Guan; Xianming Gao; Tao Feng; Kexian Liu; Jianbang Chen

TrustCom-42: Security (XIX)
Session Chair: Ziyang He (zyhe@zzu.edu.cn), Zhengzhou University

A Vulnerability Detection Method for Intermediate Code Based on a Relational Dependency Graph
Chongjun Tang; Bing Xia; Shihao Chu; Yu Dong; Wenbo Liu

SSC-IDS: A Robust In-vehicle Intrusion Detection System Based on Self-Supervised Contrastive Learning
Zhuoqun Xia; Yongbin Yu; Jingjing Tan; Kejun Long

NLP and Neural Networks for Insider Threat Detection
Neda Baghalizadeh Moghadam; Christopher Neal; Frédéric Cuppens; Nora Cuppens-Boulahia

Two-Stage Federated Learning Strategy for Fairness and Security in Vehicular Networks
Xin Zhang; Chao Guo; Buxin Guo

5G-PPDE: A Novel Adaptive Scaling Framework for Enhancing the Resilience of the 5G Cloud Core Network
Xinyu Huang; Xingxing Liao; Jie Yang; Wei You; Xinsheng Ji; Wenhao Wu; Shiru Min

Contextual Transformer-based Node Embedding for Vulnerability Detection Using Graph Learning
Joseph Gear; Yue Xu; Ernest Foo; Praveen Gauravaram; Zahra Jadidi; Leonie R Simpson

TrustCom-43: Security (XX)
Session Chair: Debin Liu (debinliuhust@gmail.com), Zhengzhou University

CVALLM: A Cloud Platform Security Assessment Framework Based on Large Language Models
Wangyuan Jing; Chi Zhang; Bingbing Zhang; Lingbo Wei

Smart Contract-Based Auditing of Edge Data for Vehicular Networks
Yu Zhao; Yangguang Tian; Chunbo Wang; Xiaoqiang Di; Hui Qi

FD-WF: A Multi-tab Website Fingerprinting Attack Based on Fixed Dimensions for Tor Network
Ruizhe Zhang; Shangnan Yin; Jinfu Chen

Modelling GDPR-compliance based on Defeasible Logic Reasoning: Insights from Time Complexity Perspective
Naila Azam; Alex Chak; Lito Michala; Shuja Ansari; Nguyen B. Truong

A Blockchain-based PHR Sharing Scheme with Attribute Privacy Protection
Chaohe Lu; Zhongyuan Yu; Guijuan Wang; Anming Dong; Xiang Tian

Secure Microwave QR Code Communication Using Pseudo-Random Constellation Rotation
Chunpeng Guo; Beiyuan Liu; Zeyang Sun; Chen Chen; Sai Xu

TrustCom-44: Privacy (VII)
Session Chair: Debin Liu (debinliuhust@gmail.com), Zhengzhou University

Federated Knowledge-enhanced Graph Attention Network for Privacy-preserving Social Recommendation
Xiaofei Hao; Liyuan Liu; Yimeng Wang; Fengyu Li; Wanqing Wu

Federated Learning Greedy Aggregation Optimization for Non-Independently Identically Distributed Data
Bosong Zhang; Qian Sun; Hai Wang; Linna Zhang; Danyang Li

Efficient Multi-subset Fine-grained Authorization PSI over Outsourced Encrypted Datasets
Jinlong Zheng; Jianan Liu; Minhua Su; Dingcheng Li; Kai He; Xueqiao Liu

A Federated Learning Scheme with Adaptive Hierarchical Protection and Multiple Aggregation
Zhiqiang Wang; Ziqing Tian; Xinyue Yu

A Dual Defense Design Against Data Poisoning Attacks in Deep Learning-Based Recommendation Systems
Xiaocui Dang; Priyadarsi Nanda; Manoranjan Mohanty; Haiyu Deng

scE(match): Privacy-Preserving Cluster Matching of Single-Cell Data
Johannes Lohmöller; Jannis Scheiber; Rafael Kramann; Klaus Wehrle; Sikander Hayat; Jan Pennekamp

TrustCom-45: Privacy (VIII)
Session Chair: Ziyang He (zyhe@zzu.edu.cn), Zhengzhou University

Block-Feature Fusion for Privacy-Protected Iris Recognition
Wiraj Udara Wickramaarachchi; Dongdong Zhao; Junwei Zhou; Jianwen Xiang

CFB-DSSE: Efficient Secure Dynamic Searchable Encryption Scheme with Conjunctive Search for Smart Healthcare
Ruiwei Hou; Fucai Zhou; Zongye Zhang; Jiacheng Li; Chongyang Wang

An Efficient and Secure Anonymous Query Protocol
Wenjv Hu; Yin Li

Privacy-aware Data Aggregation Using Functional Encryption
Sehrish Shafeeq; Mathias Fischer

Evaluating Web-Based Privacy Controls: A User Study on Expectations and Preferences
Yuemeng Yin; Rahat Masood; Suranga Seneviratne; Aruna Seneviratne

High-Capacity and High-Security Data Hiding in Encrypted Image Using Image Filtering and Image Blocking
Pengyan Xiang; Tao Zhang; Haoja Liu; Boxin Zhang; Yu Zhang

TrustCom-46: Privacy (IX)
Session Chair: Chaoming Shi (cmshi_xd@163.com), Xidian University

Cross-platform Network User Alignment Interference Methods Based on Obfuscation Strategy
Luyao Wang; Yan Liu; Xiaoyu Guo; Ziqi Long; Chunfang Yang

Research on Toxic Speech Detection Based on Large Language Models
Weihao Li; Yongbing Gao; Zhang Yu; Yang Lidong; Ruiping Gao

ZKFDT: A Fair Exchange Scheme for Data Trading Based on Efficient Zero-Knowledge Proofs
Jianwei Liu; Wei Wan; Chun Long; Jing Li; Fan Yang; Yuhao Fu

Dynamic Differential Privacy in Hierarchical Federated Learning: A Layerwise Adaptive Framework
Zhongyuan Qin; Dinglian Wang; Minghua Wang

OHSS: Optimizing Homomorphic Secret Sharing to Support Fast Matrix Multiplication
Shuguang Zhang; Jianli Bai

A Method for Quantitative Object De-Identification Analysis of Anonymized Video
Deok-Han Kim; Yujun Kim; Young-Gab Kim

Witness Encryption based on the SAT Problem
Xingbo Wang; Yuzhu Wang; Mingwu Zhang

TrustCom-47: Forensics and Analytics (II)
Session Chair: Jieming Yang (yjmlaile@gmail.com), Zhengzhou University

Research on Adaptive Attention Dense Network Structure in Camera Source Recognition Method
Haoxuan Wu; Zhiqiang Wen

Compressed Video Action Recognition Based on Neural Video Compression
Yuting Mou; Ke Xu; Xinghao Jiang; Tanfeng Sun

Construction of Cyber-attack Aattribution Framework Based on LLMs
Jinye Zhang; Ken Cheng; Xinli Xiong; Rongcheng Dong; She Jie

Discriminating Malware Families Using Partitional Clustering
Pooja Mishra; Paul T Black; Adil Bagirov; Shaning Pang

Investigating Patterns of Adversarial Techniques for Cyberattack Forensics
Liming Lu; Zhenlin Yu

WAPITI - A Weighted Bayesian Method for Private Information Inference on Social Ego Networks
Hervais Simo; Michael Kreutzer

TrustCom-48: Emerging Tech (VII)
Session Chair: Panpan Han (823518295@qq.com), Xidian University

DI-GAE: A Dynamic and Resource-Efficient Attack Detection Framework with Incremental Learning and Graph Autoencoders
Mengmi Tan; Jianyi Liu; Ru Zhang

Transfer Learning-Based Robust Insider Threat Detection
Yujun Kim; Deok-Han Kim; Young-Gab Kim

Model-based Data Markets: A Multi-Broker Game Theoretic Approach
Yizhou Ma; Xikun Jiang; Wenbo Wu; Luis-Daniel Ibáñez; Jian Shi

DcChain: A Novel Blockchain Sharding Method Based on Dual-constraint Label Propagating
Hao Zhou; Pengcheng Xia; Yiyang Ni; Jun Li

An Intelligent Charging Service Selection Scheme under the Cross-area Consensus of the Blockchain for the Internet of Vehicles
Shuming Xiong; Zhujun Feng; Qiqi Xu

FlexiContracts: A Novel and Efficient Scheme for Upgrading Smart Contracts in Ethereum Blockchain
Tahrim Hossain; Sakib Hassan; Faisal Haque Bappy; Muhammad Nur Yanhaona; Sarker Tanveer Ahmed Rumee; Moinul Zaber; Tariqul Islam

TrustCom-49: AI Trust (VIII)
Session Chair: Jie Wang (jiewang_xidian@163.com), Xidian University

Fedfair: A Debiasing Algorithm for Federated Learning Systems
Haibin Zheng; Tianxin Zhang; Jinyin Chen

Differentially Private Graph Convolutional Networks with Privacy Amplification
Yifan Sun; Meng Song

Destruction and Reconstruction Chain: An Adaptive Adversarial Purification Framework
Zeshan Pang; Shasha Guo; Xuehu Yan; Yuliang Lu

CNN-KOA-BiGRU: A High-accuracy APT Detection Model Based on Deep Learning networks
Chaoqin Zhang; Maoqi Sun; Guangwu Hu

Efficient and Secure Federated Learning via Enhanced Quantization and Encryption
Chengming Zhang; Bo Tang; Yifan Bian; Bingtao Han; Yongcheng Wang; Tao Liu

Human Action Recognition by Invisible Sensing with the Constraint of Privacy Preservation
Jun Guo; Minjuan Sun; Weiwei Zhang; Baoying Liu; Anwen Wang; Li Liu

TrustCom-50: AI Trust (IX)
Session Chair: Qixian Ren (qxren307@gmail.com), Xidian University

Traceable AI-driven Avatars Using Multi-factors of Physical World and Metaverse
Kedi Yang; Zhenyong Zhang; Youliang Tian

DDF-Net: A Cloud Computing Load Forecasting Method Integrating Spatiotemporal and Time-Frequency Domain Information
Yingjian Li; Yongsheng Wang; Gang Wang

HFL-AD: A Hierarchical Federated Learning Framework for Solving Data Contamination in DDoS Detection
Haishi Huang; Jiaping Gui; Jianan Hong; Cunqing Hua

Detectable Mislabeling - Can Faulty AI Models be Recognized from Incomplete Memory Traces?
Łukasz Krzywiecki; Tadeusz Kulczycki; Christian Emmanuel Nteranya; Andrzej Stos

Privacy-Preserving Real-Time Gesture Recognition Using Cloud-Trained Neural Networks
Kewin Ignasiak; Wojciech Kowalczyk; Łukasz Krzywiecki; Mateusz Nasewicz; Hannes Salin; Marcin Zawada

A Lightweight Privacy-Preserving and Verifiable Federated Learning-Based Protocol
Jiaqi Lei; Ke Gu; Long Cai

TrustCom-51: AI Trust (X)
Session Chair: Niklas Bunze (niklas.bunzel@sit.fraunhofer.de), Fraunhofer SIT, ATHENE, TU-Darmstadt

BIG: A Practical Framework for Balancing the Conflict Between Group and Individual Fairness in Graph Neural Networks
Kuan Yan; Dmytro Matsypura; Junbin Gao

EasyDector: Using Linear Probe to Detect the Provenance of Large Language Models
Jie Zhang; Jiayuan Li; Haiqiang Fei; Lun Li; Hongsong Zhu

FMTD: Federated Learning-Based Multi-Angle Feature Fusion Framework for Abnormal Transaction Detection in Digital Currency
Yaru Lv; Lijun Sun; Xiao Chen

Privacy Preservation in Cloud-Based Distributed Learning through Data Encoding and Partitioning
Łukasz Krzywiecki; Krzysztof Szymaniak; Marcin Zawada

Backdoor Attacks Optimized through Genetic Algorithm-Driven Data Augmentation Combinations in Deep Neural Networks
Yilun Lyu; Xu Ma; Yuan Ma

A Defensive Framework Against Adversarial Attacks on Machine Learning-Based Network Intrusion Detection Systems
Benyamin Tafreshian; Shenzhi Zhang

TrustCom-52: Security and Privacy
Session Chair: Wei Liu (weiliuxupt@163.com), Xi'an University of Posts & Telecommunications

Design and Implementation of Data Encryption Mechanism in Fiber Channel Network
Hongke Zhang; Zheng Yan

A Reliable Edge Server Deployment Algorithm Based on Spectral Clustering and a Deep Q-network Strategy Using Multi-objective Optimization
Zhou Zhou; Taotao Yu; Mohammad Shojafar; Xia Ou; Hongbing Cheng

RShield: Safeguarding Road Traffic Recognition Against Perturbation Attacks
Jianfei Sun; Hangcheng Cao; Yulan Gao; Ziyang He; Cong Wu; Shengmin Xu

Deepfakes: a New Kind of Adversarial Attacks Against Face Recognition Systems?
Raphael Antonius Frick; Lukas Graner

AttDet: Attitude Angles-Based UAV GNSS Spoofing Detection
Luyao Wang; Xiaomin Wei; Hongtao Zhang; Lingtao Jia

IoT Vulnerability Detection Using Featureless LLM CyBert Model
Shancang Li; Sarah Bin Hulayyil; Neetesh Saxena

AI Empowered Senstive Information Detection and Anonymisation in PDF Files
Hongping Li; Zheng Gao

TrustCom-53: Data Security and Privacy
Session Chair: Jice Wang (wangjice@hainanu.edu.cn), Hainan University

Analysis of Data Export Business Processes Based on Petri Nets
Yongqiang Chen; Meiqi Liu; Jingfeng Rong; Xujie Liu; Anshun Zhou; Anmin Fu; Yuqing Zhang

Research on Lifecycle-Driven Government Data Security Model and Data Grouping Technology
Siyu Chen; Jingfeng Rong; Zhiyuan Fu; Xujie Liu; Anmin Fu; Anshun Zhou; Yuqing Zhang

A Review of Data Security Research in Energy Storage Systems
Meiqi Liu; Yongqiang Chen; Chaoyang Zhu; Shuang Yao; Jingfeng Rong; Xiaolong Zhao; Xijuan Si; Guang Yang; Yuqing Zhang

Risk Assessment Based on Dataflow Dynamic Hypergraph for Cross-Border Data Transfer
Zhou Fang; Kai Zhang; Yigang Diao; Yixuan Song; Yanwei Sun; Jinqiao Shi

LogContrast: Log-based Anomaly Detection Using BERT and Contrastive Learning
Wei Yuan; Hongyu Sun; Mo Pang; He Wang; Gaofei Wu; Yuqing Zhang

A Study of Backdoor Attacks on Data Distillation for Text Classification Tasks
Sixian Sun; Hongyu Sun; Haoxing Zhang; Yuqing Zhang

TrustCom-54: Trustworthy Crowd Computing
Session Chair: Yaxing Chen (yxchen@nwpu.edu.cn), Northwestern Polytechnical University

Distributed Data Possession - Blockchain Based Scalability
Bartłomiej Dzikowski; Łukasz Krzywiecki; Ksawery Możdżyński; Karol Niczyj; Hannes Salin

Trusted and Spectrum-Efficient Crowd Computing in Massive MIMO Cellular Networks
Pengfeng Zhang; Lei Li; Xin Liu; Rui Wang; Donglan Liu; Bing Su; Yuntao Wang; Yiliang Liu; Zhou Su

Trustworthy Approaches to RSA: Efficient Exploitation Strategies Based on Common Modulus
Mahdi Mahdavi Oliaee; Navid Abapour; Zahra Ahmadian

Trust Evaluation in Mobile Crowd Sensing Networks Based on Age of Trust (AoT)
Xiayue Wang; Mingyang Li; Yuting Tao; Xuanzhe Wang; Hao Wu

MT-Index: A Trustworthy Index for Multimodal Data Sharing
Qianyue Fan; Shiqian Wang; Zhe Feng; Li Di

Honeybee-RS: Enhancing Trust through Lightweight Result Validation in Mobile Crowd Computing
Sanjay Segu Nagesh; Niroshinie Fernando; Seng W Loke; Azadeh Ghari Neiat; Pubudu Pathirana

The BigDataSE-2024 Presentation Program

BigDataSE-1: Data Analytics and Processing
Session Chair: Haipeng Du (duhaipeng@xjtu.edu.cn), Xi'an Jiaotong University

Payload Level Anomaly Network Traffic Detection via Semi-Supervised Contrastive Learning
Xinglin Lian; Yang Liu; Shanfeng Wang; Yu Zheng

DualConvNet: Enhancing CNN Inference Efficiency Through Compressed Convolutions and Reparameterization
Haipeng Du; Muyan Jiao; Jiageng Zhang; Xin Lv; Jie Zhang

Navigating Time's Possibilities: Plausible Counterfactual Explanations for Multivariate Time-Series Forecast Through Genetic Algorithms
Gianlucca Zuin; Adriano Alonso Veloso

An Experimental Study on Half-Closed TCP Connections in Public Cloud Gateways
Zhuang Yuan; Rui Li; Fa Zhang; Kejing Xu; Liang Xu; Weizhan Zhang

A Multi-Stage Spike Stream Processing and Image Reconstruction Method for Industrial Applications
Shuaipeng Wu; Changhao Yuan; Kejiang Ye

Fraud Detection in Supply Chain Order Management via Kolmogorov-Arnold Networks
Haowei Huo; Ting Lv; Ningbo Zhao; Gefan Ai; Qi He; Ying Kong; Yu Zhang; Yiwei Li; Jiangyao Wei; Chen Liu; Yuan Liu; Lichuan Ma

The CSE-2024 Presentation Program

CSE-1: Computational Intelligence Analysis

Session Chair: Xuyang Jing (jingxuyang@xidian.edu.cn), Xidian University

Multi-Scale Fuzzy Graph Convolutional Network for Hyperspectral Image Classification
Mingxin Jin; Cong Wang; Shanglin Yang; Heng Wang; Ju Huang; Jun Zhao

RTM-CMD: Exploring Advanced Underground Target Detection in Coal Mines through Modified RTMDET Methodology
Longlong Gao; Tao Xue; Long Xi

Your Data is Leaking! An Empirical Study of User Habits during Smartphone Charging
Steven Krudsen; Wenjuan Li

Anticipated Failure Determination-based Weakness Analysis with Common Weakness Enumulation
Toru Sakon

Hardware Latency-Aware Differential Architecture Search: Search for Latency-Friendly Architectures on Different Hardware
Jiaqi Han; Dan Wang; Hong Luo; Ye Zhou; Bin Song

Large-Scale Thermo-Hydraulic Analysis of Fuel Rod Bundles Based on YH-ACT
Min Song; Chao Li; Xiaowei Guo; Jie Liu; Huajian Zhang; Rui Xia

The EUC-2024 Presentation Program

EUC-1: Embedded and Ubiquitous Computing
Session Chair: Zhao Li (zli@xidian.edu.cn), Xidian University

Machine Learning Enhanced Indoor Positioning with RIS-Aided Channel Configuration and Analysis
Yanhong Xu; Zhao Li; Ziru Zhao; Blaise Herroine Aguenoukoun; Jia Liu; Zhixian Chang; Yicheng Liu

An Automated PM2.5 Analysis and Prediction System with Encoder-Decoder Architecture and Continual Learning Mechanism
Le Anh Duc Vu; Minh Hai Vu; Ngoc Tran Bao; Minh Tung Hoang; Duc Anh Nguyen; Minh Quan Hoang; Phi Le Nguyen

Multi-Sensor Fusion-Based Cow Health Monitoring IoT System
Zhenyu Lai; Yijia Xu; Jialei Zhang; Bowen Jia; Liangyan Wang; Qinglei Bu; Jie Sun; Quan Zhang

A Digital Traditional Chinese Medicine Splint for Treatment of Distal Radius Fracture
Siyuan Wang; Shuchen Liu; Zheng Jin; Zheng Yan; Tao Chen; Qinglei Bu; Zhiqiang Wang; Jintao Liu; Jie Sun

The iSCI-2024 Presentation Program

iSCI-1: Smart City and Informatization
Session Chair: Lei Mu (leimu@swun.edu.cn), Southwest Minzu University

Deep Reinforcement Learning for Active RIS-Assisted Full-Duplex Integrated Sensing and Communication Systems
Bingxin Zhang; Kang Zheng; Chao Tong; Kun Yang; Kang Yan

A Corrected Method for Parameters in the Signal Propagation Model
Yan Liang; Xin Dong; Song Chen; Dazheng Li; Minzhi Chang

Research on Energy Management Strategy of Microgrid Based on Improved Deep Q Network Algorithm
Le Tian; Changshen Ou; Weilin Huang

A Cross-Domain Authentication Scheme Based on Quantized Trust Relationship for Smart Grid
Tianang Chen; Haojie Qin; Jin Qian; Jun Luo; Yinhua Jiang; Liquan Chen

Long-Term Privacy-Preserving Incentive Scheme Design for Federated Learning
Xin Liu; Rui Wang; Pengfeng Zhang; Liang Xie; Yiliang Liu; Zhou Su; Donglan Liu; Yingxian Chang

Research on Distributed Machine Learning Defence Strategies Under Byzantine Attacks
Chen Jin; Xi Chen; Junyu Pu; Boyu Fan