# CONFERENCE PROGRAM

## 2026 4TH INTERNATIONAL CONFERENCE ON BIG DATA AND PRIVACY COMPUTING

# BDPC2026

**Beijing, China | May 29-31, 2026**

SPONSORED BY

中央财经大学 Central University of Finance and Economics

IEEE

HOSTED BY

中央财经大学 Central University of Finance and Economics 信息学院 School of Information

PATRONS

貴州大學 GUIZHOU UNIVERSITY

福建理工大学 FUJIAN UNIVERSITY OF TECHNOLOGY

澳門城市大學 Universidade da Cidade de Macau City University of Macau

# TABLE OF CONTENTS

TABLE OF CONTENTS ..... 2
ORGANIZING COMMITTEE ..... 3
WELCOME MESSAGE ..... 6
CONFERENCE VENUE ..... 7
PRESENTATION GUIDELINES ..... 8
DAILY SCHEDULE ..... 9
KEYNOTE SPEAKER ..... 13
Prof. Keke Gai ..... 13
Prof. Xinlei He ..... 14
Prof. Yue Zhang ..... 15
INVITED SPEAKER ..... 16
Dr. Guibo Luo ..... 16
Prof Ts Dr Madihah Mohd Saudi ..... 17
ONSITE SESSION 1 ..... 18
ONSITE SESSION 2 ..... 21
ONLINE SESSION A ..... 25
ONLINE SESSION B ..... 28
ONLINE SESSION C ..... 31

# ORGANIZING COMMITTEE

**Honorary Chair -**
Shiwen Mao, Auburn University, USA

**Conference General Chairs -**
Jianming Zhu, Central University of Finance and Economics, China
Yan Zhang, University of Electronic Science and Technology of China, China
Youliang Tian, Guizhou University, China
Xianhua Niu, Xihua University, China

**Conference Co-chairs -**
Changqing Luo, University of Houston, USA
Ning Zhang, Central University of Finance and Economics, China

**Technical Program Committee Co-chairs -**
Sheng Gao, Central University of Finance and Economics, China
Qing Yang, University of North Texas, USA
Jinbo Xiong, Fujian University of Technology, China
Jianbing Ni, Queen's University, Canada

**Publicity Chairs -**
Rohaya Binti Latip, Universiti Putra Malaysia, Malaysia
Huiyu Zhou, University of Leicester, United Kingdom
Man Fung LO, The University of Hong Kong, China
Zhe Sun, Guangzhou University, China

**Publication Chairs -**
Zuobin Ying, City University of Macau, Macau, China
Mohammad Ali, Amirkabir University of Technology, Iran

**Session Organizing Co-chair -**
Zhen Guo, Hainan University, China

**Track Chairs -**
Yi Sun, Beijing University Of Posts and Telecommunications, China (Track 1)
Pengfei zhang, Anhui University of science and technology, China (Track 2)
Renwan Bi, Minjiang University, China (Track 2)
Li Lin, Fujian Normal University, China (Track 3)
Liang Kou, Hanzhou Electronic Science and Technology University, China (Track 4)
Yongkai Fan, Communication University of China, China (Track 5)
Butian Huang, Hangzhou Dianzi University, China (Track 5)

**Technical Committees -**
Ali Arefi, Murdoch University, Australia
Ali Yavari, Swinburne University of Technology, Australia
Ankan Bhattacharya, Hooghly Engineering & Technology College
Anooja Ali, REVA University
Anuranjan Misra, Noida International University

Baciu George, The Hong Kong Polytechnic University
Bowen Zhao, Xidian University, China
Chih-Hua Tai, National Taipei University
Chin-Chen Chung, National Institute of Informatics, Japan
Chuan Zhang, Beijing Institute of Technology, China
Chunqiang Hu, Chongqing University, China
Cun JI, Shandong Normal University, China
Dickson K.W. Chiu, The University of Hong Kong, China
Dmitry Namoit, Lomonosov Moscow State University
Emre Erturk, Eastern Institute of Technology
Feiran Huang, Jinan University, China
Fernanda Otilia Figueiredo,University of Porto, School of Economics and Management, Portugal
GAJENDRA Sharma, Kathmandu University
Gengshen Wu, City University of Macau, China
Hamid Ali Abed AL-Asadi, Basra University
Han Weili, Fudan University, China
Hemn Abdalla, Wenzhou-Kean University, China
Hemn Barzan Abdalla, Wenzhou-Kean University, China
Hu Biao, China Agricultural University, China
Jianhong Zhang, North China University of Technology, China
Jianhua Yang, University of Science and Technology Beijing, China
Jianqiang Li, Beijing University of Technology, China
Jiaqi Zhao, Xidian University, China
Jie Zhang, Xi'an Jiaotong-Liverpool University, China
Jingjing Guo, Xidian University, China
June Tay, Singapore University of Social Sciences, Singapore
Jyh-haw Yeh, Boise State University, USA
Kiwon Lee, Hansung University, South Korea
Koorosh Gharehbaghi, RMIT University, Australia
Kushnazarov Farruh, Tashkent University of Information Technologies
Lijun Zhang, E-surfing Vision Technology Co., Ltd, China Telecom, China
Lingzhi Wang, Harbin Institute of Technology, Shenzhen, China
Loc Nguyen, Sunflower Soft Company, Vietnam
Madihah Mohd Saudi, Universiti Sains Islam Malaysia, Malaysia
Mark Van Buladaco, Davao del Norte State College, Philipine
Mehdi Gheisari, Islamic Azad University, Iran and Shenzhen BKD Co.LTD, China
Mingjun Wang, Xidian University, China
Mohd Nazri Ismail, National Defence University of Malaysia, Malaysia
Muhammad Abdullah Adnan, Bangladesh University of Engineering and Technology
Naiwei Liu, Inner Mongolia University of Technology, China
Naveed Ahmed Azam, Applied Mathematics and Physics
Nimsuk Nitikarn Nimsuk, Thammasat University, Thailand
Ning Xi, Xidian University, China
Pascal Lorenz, University of Haute Alsace, France
Putsadee Pornphol, Phuket Rajabhat University, Thailand
Qi Cao, National University of Singapore, Singapore
Qiang Yang, Zhejiang University, China
Radu Vasiu, Politehnica University of Timisoara, Romania

Wai Lok Woo, Northumbria University, UK
Wanyang Dai, Nanjing University, China
Wenjian Liu, City University of Macau
Xiangyu Wang, Xidian University, China
Xiaohua (Edward) Li, State University of New York at Binghamton, USA
Xiaoqiang Di, Changchun University of Science and Technology, China
Yang Liu, Swansea University, UK
Yangli Jia, Liaocheng, University, China
Yanhong Guo, Dalian University of Technology, China
Yew Kee WONG Eric, Hong Kong Chu Hai College, China
Yichuan Wang, Xi'an University of Technology, China
Yijun Bei, Zhejiang University, China
Yingyi Zhang, Beijing University of Civil Engineering and Architecture, China
Yixin Jiang, China Southern Power Grid Electric Power Research Institute, China
Yong Zhao, Sichuan University, China
Yu-Beng Leau, Universiti Malaysia Sabah, Malaysia
Zhang Xi, Beijing University of Posts and Telecommunications, China
Zheyi Chen, Fuzhou University, China
Zhihua Wu, Liming Vocational University, China
Zhihui Wang, Fudan University, China
Zhili Zhou, Guangzhou University, China

# WELCOME MESSAGE

2026 4th International Conference on Big Data and Privacy Computing (BDPC2026) will be held in Beijing, China during May 29-31, 2026. It is sponsored by the Central University of Finance and Economics and IEEE, hosted by the School of Information at the Central University of Finance and Economics, with the support of patrons including Guizhou University, Fujian University of Technology, and the City University of Macau.

This conference provides opportunities for the different areas Delegates to exchange new ideas and application experiences face to face, to establish business or research relations and to find global partners for future collaboration. We hope that the conference results constituted significant contribution to the knowledge in these up-to-date scientific field.

BDPC 2026 will place a special focus on educational and information technology to address multidisciplinary challenges. The event will feature oral presentations, poster presentations, workshops, keynote speeches by experts on state-of-the-art topics, and invited speeches. Our aim is to enrich the regular program with emerging topics of particular interest in the field of Big Data and Privacy Computing. We encourage authors to expand upon their research and share their knowledge to contribute to the collective effort to enhance educational and information technology.

On behalf of the conference committee, we sincerely thank all authors, reviewers, and attendees for your valuable contributions, hard work, and active participation in BDPC 2026. Your dedication, professional expertise, and insightful exchanges have laid a solid foundation for our high-quality academic program and made this conference a remarkable success. We greatly appreciate your continuous support and trust in BDPC. Finally, we wish all delegates a fruitful, inspiring, and pleasant conference experience!

BDPC2026 Conference Committee
2026 4th International Conference on Big Data and Privacy Computing
May, 2026

# CONFERENCE VENUE

## 北京新世纪饭店
## Beijing New Century Hotel

**Address: No. 6 Shouti South Road, Haidian District, Beijing 100044, China**

**地址： 北京市海淀区首体南路 6 号**

标准间 500 元/间 不含早；大床房 580 元/间 不含早 (早餐 70 一位)
预定住房：李经理
电话： 13910778088 预定是备注“BDPC2026”

Standard Room: ¥500 per room, without breakfast
King Room: ¥580 per room, without breakfast
(Breakfast: ¥70 per person)

Hotel Manager: Mr. Li Tel: 13910778088
Remark as "BDPC2026"

### 交通指引 (Transport Instruction)

北京新世纪饭店紧邻西二环，北邻中关村，南靠西客站，西近中央电视塔，东接金融街。距首都机场、北京火车站等各大交通枢纽仅半小时车程，同时周边拥有多条地铁线路，地铁 4 号线、6 号线、9 号线为您出行提供更多选择。

#### 机场出行 By Airport

1. 首都国际机场：地铁换乘至**白石桥南站**步行即达；打车约 50 分钟，费用 120-150 元
   Capital Airport: Take metro to Baishiqiao South Station and walk there. Taxi: 50 mins, CNY 120-150

2. 大兴国际机场：机场专线转地铁至白石桥南；打车约 60 分钟，费用 160-190 元（含高速费）
   English
   Daxing Airport: Take airport line plus metro. Taxi: 60 mins, CNY 160-190 (including highway toll)

#### 高铁站出行 By High-speed Railway Station

1. 北京西站：地铁 9 号线直达白石桥南，步行 5 分钟；打车 15 分钟，约 30 元
   Beijing West Station: Metro Line 9 direct. Taxi: 15 mins, CNY 30

2. 北京南站：地铁 4 号线直达站点；打车 25 分钟，约 45 元
   Beijing South Station: Metro Line 4 direct. Taxi: 25 mins, CNY 45

3. 北京站：地铁 2 号线转 4 号线；打车 30 分钟，约 50 元
   Beijing Railway Station: Transfer by metro. Taxi: 30 mins, CNY 50

备注：以上信息仅供参考，具体行程及费用请以实际情况为准。
Note: The above information is for reference only, and the actual itinerary and costs are subject to on-site conditions.

# PRESENTATION GUIDELINES

## ORAL PRESENTATION

1. The duration of an oral presentation slot is 15 minutes. Please target your lecture for a duration of about 10 minutes for the presentation plus about 5 minutes for questions from the audience.
2. Your punctual arrival and active involvement in each session will be highly appreciated.
- Get your presentation PPT or PDF files prepared and backed up.
3. Laptops, projector & screen, laser sticks will be provided by the conference organizer.
4. Join the meeting room at least 15 minutes before the session begins.

## ONLINE PRESENTATION | Password: BDPC

Download zoom: https://zoom.us/android/download

For oversea: https://www.zoom.com/

Online Room Link: https://us02web.zoom.us/launch/jc/86898180738

Room ID: 868 9818 0738

Password: BDPC

Time Zone: **China Standard Time (CST), UTC/GMT+8**

Please make sure that both the clock and the time zone on your computer are set to the correct China standard time.

## SECURITY

- Please take care of your belongings in public area. For your personal and property safety, delegates are suggested to wear representative card during conference and not to lend it to those unconcerned to enter event rooms. Conference does not assume any responsibility for loss of personal belongings of participants.
- Don't stay too late in the city, don't be alone in the remote area. Be aware of the strangers who offer you service, signature of charity, etc., at scenic spots. You can search more Tourist Information and Security tips online.
- Emergency Call; Ambulance: 120  Police: 110

Assistant Wechat QR code, remark as BDPC2026

添加会议秘书微信，备注 BDPC2026

Conference Program

扫描二维码 获取电子版日程

# DAILY SCHEDULE

| Day 1, May 29, 2026 | |
|---|---|
| **11:00-16:00** | **Onsite Sign in and Collect Conference Materials**<br>**北京新世纪饭店 大堂 \| Lobby of Beijing New Century Hotel** |
| | |
| **Online Pre-test Timetable and online sign** | |
| Online room: https://us02web.zoom.us/launch/jc/86898180738<br>Password: BDPC | |
| 14:00-14:30 | Online Invited Speakers & Session Chairs & Committees |
| 14:30-15:30 | Online Authors<br>C2190, C2865, C3661, C3669, C3696, C4039, C4050<br>C2303, C2619, C3646, C4367, C4498, C4593<br>C1315, C2431, C2570, C4622, C4790, C4804, C3319 |

# Day 2, May 30, 2026

| | |
|---|---|
| **山东厅 2楼 \| Shandong Hall 2nd Floor** | |
| **Host (Technical Program Committee Co-chair)**<br>**Jinbo Xiong, Fujian University of Technology, China** | |
| **OPENING CEREMONY** | |
| **09:00-09:05** | **Welcome Message (Conference Co-chair)**<br>**Ning Zhang, Central University of Finance and Economics, China** |
| **09:05-09:10** | **Opening Remarks (Conference General Chair)**<br>**Jianming Zhu, Central University of Finance and Economics, China** |
| *09:10-09:20* | *Group Photo* |
| **MORNING SPEECHES** | |
| **09:20-10:00** | **Keynote Speaker I**<br>**Keke Gai, Beijing Institute of Technology, China**<br>**Speech Title: Blockchain-based Distributed Digital Identity** |
| *10:00-10:20* | *Coffee Break* |
| **10:20-11:00** | **Keynote Speaker II**<br>**Xinlei He, Wuhan University, China**<br>**Speech Title: Exploring Backdoor Attacks and Defenses for Generative AI Models** |
| **11:00-11:40** | **Keynote Speaker III**<br>**Yue Zhang, Shandong University, China**<br>**Speech Title: Is Mobile Privacy Dead? Rethinking Security and Privacy Across Paradigms in the Age of AI Agents** |
| **11:40-12:00** | **Invited Speaker**<br>**Guibo Luo, Peking University, China**<br>**Speech Title: Generative Collaboration for Privacy-Preserving Multi-Institutional Medical Imaging** |
| *From 12:00* | *Lunch*<br>*一层 世纪咖啡厅 \| Century Café 1st Floor* |

| AFTERNOON ONSITE SESSIONS | |
|---|---|
| **山东厅 2楼 \| Shandong Hall 2nd Floor** | |
| **13:30-15:30** | **Onsite Session 1**<br>**Topic: Big Data Science and Applications**<br><br>**Session Chair: Assoc. Prof. Qi Cao, National University of Singapore, Singapore**<br><br>**Order: C2174, C1955, C2683-A, C2784, C2843, C3224, C3471, C3730** |
| *15:30-16:00* | *Coffee Break* |
| **16:00-18:15** | **Onsite Session 2**<br>**Topic: Data Security and Blockchain Application Technology**<br><br>**Session Chair: Assoc. Prof. Thepparat Phimolsathien, King Mongkut's Institute of Technology Ladkrabang, Thailand**<br><br>**Order: C3732, C1254, C1265, C1534, C2416, C2905, C3445, C3210, C3930** |
| *From 18:30* | *Dinner*<br>*一层 世纪咖啡厅 \| Century Café 1st Floor* |

# Day 3, May 31, 2026

## ONLINE SESSIONS

**Online Link: https://us02web.zoom.us/launch/jc/86898180738 Password: BDPC**

| | |
|---|---|
| **10:00-12:05** | **Online Session A**<br>**Topic: Data Encryption and Privacy Protection**<br><br>**Session Chair: Assoc. Prof. Renwan Bi, Minjiang University, China**<br><br>**Invited Speaker: Madihah Mohd Saudi Universiti Sains Islam Malaysia (USIM), Malaysia**<br><br>**Order: C2190, C2865, C3661, C3669, C3696, C4039, C4050** |
| *12:05-14:00* | *Break Time* |
| **14:00-15:30** | **Online Session B**<br>**Topic: Big Data Analysis and Computing**<br><br>**Session Chair: Prof. Yanhong Guo, Dalian University of Technology, China**<br><br>**Order: C2303, C2619, C3646, C4367, C4498, C4593** |
| *15:30-16:00* | *Break Time* |
| **16:00-17:45** | **Online Session C**<br>**Topic: Data Security and Blockchain Application Technology**<br><br>**Session Chair: Dr. Zhihui Wang, Fudan University, China**<br><br>**Order: C1315, C2431, C2570, C4622, C4790, C4804, C3319** |

# KEYNOTE SPEAKER

## Prof. Keke Gai
## Beijing Institute of Technology, China

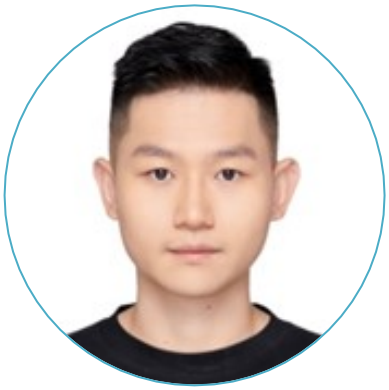
09:20-10:00, May 30, 2026 | Shandong Hall 2nd Floor | 山东厅 2 楼

Boi: Keke Gai is currently a full professor and a deputy dean at the School of AI, and also a professor with the School of Cyberspace Science and Technology, Beijing Institute of Technology, China. He is also a vice-president of Zhongguancun Academy. He was selected into the National Young Talents Program in 2022, and was selected into the list of top 2% scientists in the world, has published 4 technical books and more than200 refereed journals/conference papers. His cited counts (Google Scholar) reached more than 14500 till June 2026 with an h-index at 60. He is involved in a number of professional/academic associations, e.g., ACM, IEEE, and CCF. He is serving as a EiC of journal Blockchains, an Area Editor of JPDC (2021-current), and served as AEs of TDSC, FGCS, etc. He has worked as a program chair in a few academic conferences. He also serves as a co-chair of IEEE Technology and Engineering Management Society (TEMS)'s Technical Committee (TC) on Blockchain and Distributed Ledger Technologies (DLT), a Secretary-general at AEEEIT-BC (The Alliance of Emerging Engineering Education for Information Technologies - Blockchain Committee), a Standing Committee Member at CCF-BC (China Computer Federation - Blockchain Committee), a Secretary-General at IEEE STCSC (IEEE Special Technical Community in Smart Computing). His research interests include AI security, AI safety, cybersecurity, privacy computation, and blockchain.

**Title: Blockchain-based Distributed Digital Identity**

Abstract: Deriving from the development of the Internet, digital identity is becoming a virtual solution to identifying individuals, while considering flexible customer-centered applications. However, a few challenges still exist in this field, e.g., privacy leakage, since individuals' identities generally are governed by a centralized setting. Blockchain technology has provided an alternative for achieving a privacy-preserving decentralized identity solution. This talk will mainly cover following contents, including the mechanism of blockchain-based distributed digital identities, security issues, and solutions.

# KEYNOTE SPEAKER



## Prof. Xinlei He
## Wuhan University, China

10:20-11:00, May 30, 2026 | Shandong Hall 2nd Floor | 山东厅 2 楼

Boi: Dr.Xinlei He is a research fellow in the Institude for Math & AI, Wuhan University. He obtained his Ph.D. from CISPA Helmholtz Center for Information Security. His research lies in the domain of trustworthy machine learning, with a special focus on privacy, security, and accountability issues stemming from machine learning paradigms. He has published over 40 papers in top-tier conferences/journals such as IEEE S&P, ACM CCS, NDSS, and USENIX Security. He served as the AE of TDSC and the TPC member of multiple conferences such as IEEE S&P, AAAI, KDD, etc. He was the recipient of the Norton Labs Graduate Fellowship 2022 (only two recipients around the world), LAMPS 2024 Best Paper Award, and NDSS 2025 Distinguished Poster Award. More details are at https://xinleihe.github.io/.

**Title: Exploring Backdoor Attacks and Defenses for Generative AI Models**

**浅谈生成式人工智能模型后门攻防**

Abstract: Backdoor attacks in generative AI models has emerged as a critical issue in the field of AI security. Backdoor attacks involve embedding malicious patterns into training data or the models themselves, causing the model to produce erroneous outputs when activated by specific trigger conditions. This poses a significant threat to the reliability and security of AI systems. In this talk, we focus on backdoor attack and defense mechanisms in critical contexts, including model merging and parameter-efficient fine-tuning (PEFT). We will examine current attack techniques, evaluate existing defense strategies, and introduce potential solutions to mitigate these risks.

# KEYNOTE SPEAKER

## Prof. Yue Zhang

## Shandong University, China

11:00-11:40, May 30, 2026 | Shandong Hall 2nd Floor | 山东厅 2 楼

Boi: Yue Zhang is a Professor at Shandong University. Before joining Shandong University, he worked as an Assistant Professor at Drexel University. His research focuses on system security, IoT security, AI/LLM security, and privacy. He has published more than 70 papers at top-tier security venues, including including 23 papers at the "Big Four" security conferences (i.e., ACM CCS, IEEE S&P, USENIX Security, and NDSS). His work has received over 5,000 Google Scholar citations, with one paper cited nearly 1,800 times. His honors include ACM CCS Best Paper Nomination, USENIX Security Best Paper Nomination, NDSS Distinguished Reviewer, USENIX Security Notable Reviewer, the Provincial Natural Science First Prize, the Provincial CCF Best Paper Award, and the ACM Qingdao Rising Star Award. He has also served as a track/session chair for conferences such as IEEE MASS and IEEE MSN, and as a program committee member for major security conferences including NDSS, ACM CCS, and USENIX Security. In addition, he serves as an Associate Editor or Editorial Board Member for journals such as T-IFS, and HCC. His research has uncovered critical vulnerabilities affecting organizations and companies including Bluetooth Special Interest Group, Google, Apple, Texas Instruments, MQTT, and Tencent. His work has received public acknowledgments, bug bounties, and research support from several major companies and organizations, and had attracted intense media attention such as CCTV, Hacker News, and Mirage News.

### Title: Is Mobile Privacy Dead? Rethinking Security and Privacy Across Paradigms in the Age of AI Agents

Abstract: This talk begins with our research on mobile privacy and security, focusing on a systematic analysis of age verification mechanisms in adult-oriented applications. By combining static and dynamic analysis techniques, we demonstrate how large-scale Android applications widely suffer from weak verification logic, identity misuse, and privacy-related trust failures. Our study shows that many applications rely only on superficial validation mechanisms, making them vulnerable to forged identities, fake inputs, and sensitive data misuse. Building on this experience, the talk further explores a broader question: as mobile security research becomes increasingly mature, where should system security researchers go next? Our core argument is that the technology stack itself is not obsolete: the problem space is simply shifting. Using emerging LLM and AI agent ecosystems as examples, we argue that systems such as MCP (Model Context Protocol) should be treated as "analyzable code," allowing researchers to transfer mature mobile security techniques such as UI analysis, taint tracking, and call-chain modeling, into the agent ecosystem to identify new privacy and security risks, including sensitive context leakage, permission overreach, identity confusion, and inconsistencies between descriptions and implementations. Through this "from Mobile to Model" perspective, the talk aims to show that traditional system security and privacy analysis techniques remain highly valuable in the era of AI agents, while encouraging researchers to rethink how their existing expertise can evolve within emerging ecosystems.

# INVITED SPEAKER

## Dr. Guibo Luo
## Peking University, China

11:40-12:00, May 30, 2026 | Shandong Hall 2nd Floor | 山东厅 2 楼

Boi: Guibo Luo is an Assistant Professor and Ph.D. Supervisor at the School of Electronic and Computer Engineering, Peking University. He received his Ph.D. degree from Peking University, and subsequently conducted postdoctoral research at Harvard Medical School and Massachusetts General Hospital. His research focuses on privacy-preserving computation and foundation model training, with an emphasis on discovering and quantifying scientific patterns from heterogeneous real-world data while ensuring privacy and security in collaborative settings. Recently, he has been investigating efficient multi-institutional collaborative intelligence without exposing private data. To this end, he has developed a systematic research framework that connects (i) the creation of real-world multi-center datasets, distribution-shift characterization, and benchmark evaluations, (ii) communication-efficient privacy-preserving learning and secure computation paradigms, and (iii) privacy-preserving collaboration between foundation models and lightweight edge models under stringent communication and compute constraints. His work further emphasizes reliability and accountability in real deployments, and has led to practical deployments in healthcare, embedded systems, and embodied intelligence. He has published more than 80 papers in leading journals and conferences, including IEEE TPAMI, IEEE JBHI, Radiology: AI, IEEE TCSVT, IEEE TCDS, Journal of Digital Imaging, CVPR, ECCV, AAAI, KDD, ICSE, IJCAI, and MICCAI. He also serves as a reviewer for journals and conferences such as IEEE TIP, IEEE TNNLS, Knowledge-Based Systems, CVPR, ICCV, ICLR, NeurIPS, KDD, and MICCAI.

**Title: Generative Collaboration for Privacy-Preserving Multi-Institutional Medical Imaging**

Abstract: Multi-institutional medical imaging intelligence plays an important role in disease diagnosis, precision treatment, and clinical decision support, yet its development is constrained by medical data silos, privacy protection requirements, cross-institutional data heterogeneity, and the high cost of deploying foundation models in real-world clinical environments. This speech introduces generative AI-driven privacy computing as a new pathway beyond conventional federated learning. Instead of relying primarily on multi-round parameter or gradient exchange, the proposed paradigm leverages generated data and generated representations to enable single-round or low-interaction privacy-preserving collaboration, supporting efficient cross-institutional knowledge sharing and model training while keeping sensitive data local. The talk further discusses collaborative mechanisms between cloud-hosted foundation models and edge-side lightweight models, where generative data-driven learning and bidirectional knowledge distillation combine the generalization capability of large models with the efficient deployment capability of small models.

# INVITED SPEAKER

## Prof Ts Dr Madihah Mohd Saudi
## Universiti Sains Islam Malaysia (USIM), Malaysia

May 31, 2026 | 10:00-10:20 | Online: https://us02web.zoom.us/launch/jc/86898180738 Password: BDPC

Boi: Professor Ts. Dr. Madihah Mohd Saudi is a pioneering force in cybersecurity and education. As a Professor in the Information Security & Assurance Programme(ISA) at Universiti Sains Islam Malaysia (USIM), she drives innovation in both realms. Her tenure as USIM's former Chief Information Officer underscores her visionary integration of technology and education. With a remarkable career spanning over 22 years, Prof. Madihah has authored numerous books, strategic plans, and impactful journal papers. She holds esteemed positions worldwide, including Honorary Visiting Research Fellow at the University of Bristol's CyberSecurity Group and Visiting Professor roles at prominent institutions in Indonesia and Uzbekistan. A member of influential organizations like IEEE Computer Society, she excels in cybersecurity and machine learning. Her educational journey, from a BScHons in Computer Science to a PhD in Computer Security, combined with certifications like GSEC and CEH, reflects her commitment to expertise. Prof. Madihah's influence resonates across borders, shaping a brighter future in cybersecurity and education. Her legacy of knowledge, mentorship, and global collaboration continues to guide aspiring minds and professionals alike.

**Title: Building National Resilience Against Cyber-Enabled Crime: The Fusion Centre Imperative**

Abstract: As cyber-enabled crime increasingly converges with traditional organized crime, establishing a Cyber Crime Fusion Centre (CCFC) is a strategic imperative for national resilience. This keynote address will evaluate our readiness to transition from reactive policing toward a systematic, resilient governance model. By examining international best practices, the session will unpack the structural incentivizers, and institutional coordination required to effectively govern and enforce cybersecurity. Furthermore, it explores critical mechanisms to break institutional silos through 'comply or explain' frameworks and scalable public-private partnerships. Ultimately, the address emphasizes balancing technical oversight with public legitimacy to ensure robust cross-border accountability

# ONSITE SESSION 1

- **Topic: Big Data Science and Applications**
- **Location: 山东厅 2 楼 | Shandong Hall 2nd Floor**
- **Time: May 30, 2026 | 13:30-15:30**

- **Session Chair: Assoc. Prof. Qi Cao, National University of Singapore, Singapore**
- **Order: C2174, C1955, C2683-A, C2784, C2843, C3224, C3471, C3730**

| | |
|---|---|
| **C2174**<br>**13:30-13:45** | Semantify: Bridging the Gap Between Meaning and Keywords in Big Data Product Search<br>Author(s): Benjamin Choon How Loh, Chee Kiat Seow, Qi Cao<br>Presenter: **Qi Cao**, National University of Singapore, Singapore<br><br>Abstract: The global growth of business-to-business (B2B) e-commerce marketplaces has transformed how businesses procure products and services with a wide range of products from multiple suppliers in the form of big data. But diversity makes it increasingly difficult for buyers to efficiently locate the ideal product for their specific needs in big data of product categories. Buyers often search for complex technical products that require precise specifications. Despite advancements in search algorithms and B2B e-commerce marketplace design, limited understanding of both product titles and search queries in large database presents a persistent challenge. The objective of the research is to enhance the product search functionality in large product databases of B2B marketplaces by addressing challenges related to semantic understanding and data quality. An approach is proposed for semantic product search in big data that aims to reduce the reliance on manual data labelling and improve the effectiveness of product search in product catalogues. By harnessing natural language processing techniques for feature extraction, the proposed approach seeks to deliver a more accurate, scalable, and adaptable semantic search solution that effectively meets the dynamic needs of B2B markets with regard to returning relevant product title search results based on buyers' search queries. |
| **C1955**<br>**13:45-14:00** | An Efficient Unbalanced Privacy Set Intersection Scheme Based on Secret Sharing and TEEs<br>Author(s): Mingqin Hou, Wei Luo, Jiaqi Zhao, Chengyu Tan, Shanpeng Lai, Hui Zhu<br>Presenter: **Mingqin Hou**, Xidian University, China<br><br>Abstract: Private Set Intersection (PSI) is a fundamental cryptographic primitive for privacy-preserving data processing, where the unbalanced client-server setting is a particularly prevalent scenario. However, existing solutions often rely on computationally intensive tools such as fully homomorphic encryption (FHE), which can lead to significant performance bottlenecks. These approaches may impose substantial computational burdens on the resource-constrained party, such as exponent operations, and suffer from high costs associated with operations like homomorphic bootstrapping. This paper presents a highly efficient protocol for unbalanced PSI, which therefore innovatively combines Secret Sharing (SS) with the Trusted Execution Environments (TEEs) technique. Specifically, we leverage SS to perform the core intersection computation, thereby replacing the need for FHE. This design completely eliminates the limitations of circuit depth and circumvents the expensive overhead of homomorphic bootstrapping. Furthermore, our protocol offloads the client from performing any exponent computations. An enclave, deployed on the server side, acts as a trusted extension to manage sensitive data, significantly confining critical interactions within the server's local environment. Experiments demonstrate that the protocol is more efficient and practical for real-world unbalanced PSI applications. |
| **C2683-A**<br>**14:00-14:15** | Dynamic Identity Management in Online Health Communities: How Illness Stage Moderates the Effects of Anonymity — A Longitudinal Panel Data Analysis<br>Author(s): Yiming Yang<br>Presenter: **Yiming Yang**, Huazhong University of Science and Technology, China<br><br>Abstract Background :Cancer patients and caregivers face a fundamental "communication paradox" in online health communities (OHCs), torn between the need for social connection and the fear of personal exposure. Although anonymity offers a potential resolution, the extant study tends to reduce identity choice to a static and monolithic concept. Objective :In this study, |

| | |
|---|---|
| | we propose a “dynamic identity management” (DIM) framework to examine how anonymity shapes self-disclosure and social feedback, and how critical illness stages reconfigure these causal pathways. Methods :We analyzed a longitudinal dataset from the “Cancer” super-topic on Zhihu (N=1998 posts from 215 users). By integrating social psychological and communication theories with user fixed-effects models, we identified the causal effects of anonymity while controlling for time-invariant individual heterogeneity. Results :Anonymity exerted a selective influence, significantly enhancing intrinsic disclosure motivation and facilitating the expression of authentic—often negative—emotions. However, it did not increase the breadth or sensitivity of factual information disclosed. Illness stage emerged as a pivotal moderator. During strong situational contexts such as initial diagnosis and terminal stages, the negative effect of anonymity on social feedback (likes and comments) intensified, whereas its role in enabling profound emotional expression became more pronounced. Conclusions :Our findings demonstrate that users strategically employ anonymity throughout the illness trajectory, prioritizing psychological safety over the quantity of social connections during high-stakes phases. This dynamic perspective moves beyond static paradigms in health communication and offers concrete design implications for building responsive, human-centered health support ecosystems. |
| **C2784**<br>**14:15-14:30** | Accelerating NTRU based bootstrapping for MKFHE<br>Author(s): Xiuhui Li, Wei Du, Fuqun Wang, Renjun Zhang, Qi Xie<br>Presenter: **Xiuhui Li**, Hangzhou Normal University, China<br><br>Abstract: Multi-key fully homomorphic encryption (MKFHE) enables arbitrary computations on ciphertexts encrypted with distinct secret keys, thereby ensuring data privacy in multi-party scenarios. In this work, we design a new CMux gate using key unrolling (KU) algorithm, which makes the bootstrapping algorithm more efficient. Despite the number of RQ consisting evaluation key (evk) at each party increases from $(2n + 2)\ell$ to $(3n + 2)\ell$, the number of multiplications required for performing bootstrapping over the ring RQ is theoretically reduced by half. This trade-off is suitable for some fields such as healthcare and financial services, which require faster homomorphic computation and tolerate higher storage costs. |
| **C2843**<br>**14:30-14:45** | Mining Customer Lifecycle Advancement Patterns<br>Author(s): Chih-Hua Tai, Chen-An Hsiao<br>Presenter: **Chih-Hua Tai**, National Taipei University<br><br>Abstract: Customer Relationship Management (CRM) widely employs coupons to stimulate purchases and promote customer lifecycle progression, yet most promotion strategies remain rule-based rather than data-driven. Mining effective promotion patterns from transaction logs is challenging due to the interplay among coupon usage, co-purchase effects, and lifecycle stage transitions. In this paper, we propose Relationship Advancement Patterns (RAPs), which characterize promotion-driven behaviors by jointly specifying purchased products, coupon attributes, and customer lifecycle transitions. We define market support to measure pattern prevalence and average additional revenue to quantify the incremental economic benefit after accounting for coupon discounts. To efficiently discover valuable RAPs, we develop FRAPM, a level-wise mining algorithm that exploits the Apriori property of market support and a monotonic upper bound of average additional revenue for early pruning. Experiments on four real-world and two synthetic datasets demonstrate that FRAPM consistently outperforms a baseline in execution time and memory usage while effectively discovering high-quality promotion patterns. |
| **C3224**<br>**14:45-15:00** | Research Progress on Trust in LLM-Based Chatbots<br>Author(s): Haofang Dai<br>Presenter: **Haofang Dai**, Northwest University, China<br><br>Abstract: Against the backdrop of rapid advancements in generative artificial intelligence, the issue of trust in LLM-based chatbots has become an increasingly important topic. Based on relevant documents from the Web of Science Core Collection database, this study employs bibliometric methods to analyze publication trends, major research areas, and leading publishing countries in this field. Additionally, by combining keyword co-occurrence analysis with timeline analysis, this study identifies the primary research hotspots and their evolution within the field. The results indicate that research on trust in LLM-based chatbots has grown significantly in recent years and exhibits a strong interdisciplinary trend. Current research |

| | |
|---|---|
| | primarily focuses on artificial intelligence and large language models, trust and adoption mechanisms, user perceptions and interaction characteristics, as well as trust-building in specific application scenarios such as education and healthcare. At the same time, the research paradigm in this field is gradually expanding from the early perspective of technology acceptance to issues such as scenario-based trust, risk management, and ethical governance. This provides valuable insights to inform future research directions. |
| **C3471**<br>**15:00-15:15** | Digital Twin Dynamic Topology Simulation Platform Based on Semantic Integrity Verification<br>Author(s): Yu Han, Yichuan Wang, Xiaoxue Liu, Yanhua Feng, Xindong Wang, Yingfeng Shi<br>Presenter: **Yu Han**, Xi'an University of Technology, China<br><br>Abstract: This paper proposes a Digital Twin Dynamic Topology Simulation Platform Based on Semantic Integrity Verification. Built upon the Software-Defined Networking (SDN) architecture, the platform integrates semantic integrity verification and state monitoring modules into the Ryu controller, enabling real-time perception of host states and automated closed-loop control in Mininet-based digital twin networks. Leveraging the OpenFlow protocol for fine-grained switch port management and predefined host-to-port mapping policies, the system can rapidly execute port isolation and backup path rerouting upon detection of anomalous node states, thereby ensuring service continuity. The core contribution of this work lies in constructing a closed-loop feedback system that unifies "state perception-data verification-policy decision-command execution", complemented by formalized response time and port control models that mathematically analyze the system's real-time performance and reliability. Experimental results demonstrate that the proposed simulation platform effectively enhances state synchronization accuracy in digital twin networks and significantly improves the success rate of twin simulations in complex dynamic environments. |
| **C3730**<br>**15:15-15:30** | Exploration and Practice of AIGC-Enabled Teaching in the Course “Big Data Computing Technology”<br>Author(s): Piao Shi, Meijia Zhao, Guoqing Liu, Xiangming Zheng<br>Presenter: **Piao Shi**, Bozhou University, China<br><br>Abstract: In response to the prevalent challenges in teaching the course Big Data Computing Technology at local undergraduate universities, such as the scarcity of practical resources, rigid teaching paradigms, and inadequate integration of curriculum ideological and political education, this study proposes a teaching exploration and practice scheme empowered by Artificial Intelligence Generated Content (AIGC). Considering the specific context of local institutions, characterized by students' relatively weak academic foundations and limited teaching resources, this scheme adopts a core design philosophy centered on the ``trinity of collaboration" involving teachers, AIGC tools, and students. It aims to foster the collaborative development of this tripartite relationship, thereby constructing an AIGC-empowered teaching system. Furthermore, a targeted teaching practice plan is designed, and a lightweight deep learning network-based teaching model is established. The results demonstrate that this approach effectively enhances students' learning enthusiasm and practical skills while achieving the unified progression of knowledge acquisition and value cultivation. This study provides a valuable reference for the teaching reform of similar courses in local undergraduate universities. |

# ONSITE SESSION 2

- **Topic: Data Security and Blockchain Application Technology**
- **Location: 山东厅 2 楼 | Shandong Hall 2nd Floor**
- **Time: May 30, 2026 | 16:00-18:15**

- **Session Chair: Assoc. Prof. Thepparat Phimolsathien, King Mongkut's Institute of Technology Ladkrabang, Thailand**
- **Order: C3732, C1254, C1265, C1534, C2416, C2905, C3445, C3210, C3930**

| | |
|---|---|
| **C3732**<br>**16:00-16:15** | Enhancing Good Governance in Thai Customs: An Analysis of Blockchain Technology in Import-Export Procedures<br>Author(s): Thepparat Phimolsathien<br>Presenter: **Thepparat Phimolsathien**, King Mongkut's Institute of Technology Ladkrabang, Thailand<br><br>Abstract: The increasing integration of digital technologies plays a pivotal role in transforming organizational operations, fostering business growth, and enhancing the efficiency of work processes across various sectors. The decentralized nature of blockchain, where no single entity has control over the entire system, allows for immutable data storage and promotes greater security, transparency, and accountability in data management. The Customs Department, a key government agency responsible for levying duties and facilitating trade, has adopted various digital technologies to enhance service delivery and governance. These include systems for tariff payments, customs fees, and the development of the National Single Window (NSW) for more efficient customs processing This study aims to investigate stakeholders' understanding of blockchain's application in import and export procedures and its potential to enhance good governance in service provision. It also explores the impact of blockchain on these procedures and offers recommendations for mitigating the positive and negative effects associated with its implementation. |
| **C1254**<br>**16:15-16:30** | Multi-Hop Privacy-preserving Cross-chain Payment Channels for Multi-chain Ecosystems<br>Author(s): Chuan Zhang, Jiayi Xu, Mengxuan Liu, Haotian Deng, Xuhao Ren, Licheng Wang, Liehuang Zhu<br>Presenter: **Jiayi Xu**, Beijing Institute of Technology, China<br><br>Abstract: Multi-hop cross-chain payment channels enable efficient asset transfer in multi-chain ecosystems, but extending single-hop privacy-preserving designs to routed paths faces a fundamental bottleneck: synchronization puzzles must be reused or propagated across hops, which exposes correlation handles to relay nodes and breaks unlinkability. To address this limitation, we propose MP2C, a privacy-preserving multi-hop cross-chain payment channel scheme that extends the atomicity guarantees of P2C2T while preserving unlinkability in multi-hop networks via secure multi-party computation. MP2C integrates multi-party adapter signatures and verifiable timed discrete logarithms to cryptographically bind hop-by-hop asset release and timeout refunds, and incorporates bonding and slashing mechanisms to enhance robustness against aborting or malicious participants. Implementation and evaluation results show that MP2C supports multi-hop cross-chain payments with practical off-chain overhead: compared to P2C2T, it increases per-hop running time by about 17.1% and per-hop communication by about 5.6% , while storage remains lightweight. |
| **C1265**<br>**16:30-16:45** | E-Raft: A Node Identity Privacy Enhancement Scheme For Raft Consensus Algorithm<br>Author(s): Mengjie Tian,Minghua Zhao,Yichuan Wang, Xiaoxue Liu and Yeqiu Xiao<br>Presenter: **Mengjie Tian**, Xi'an University of Technology, China<br><br>Abstract: In the Raft algorithm, since the issue of identity privacy leakage is not considered in the algorithm, eavesdroppers or external attackers can track node identities, making specific candidate nodes vulnerable to targeted network attacks, resulting in poor privacy protection of the Raft consensus mechanism. To solve the above problems under the Crash Fault Tolerance (CFT) model, this article uses the ECC encryption algorithm and non-interactive Zero-Knowledge Proof method to improve the identity privacy protection properties of the Raft |

| | |
|---|---|
| | consensus mechanism, ensuring the fairness of the election and data consistency, while ensuring the privacy of node identities. This not only enhances the security of the election process and prevents malicious nodes from interfering with normal leader elections by forging identities, but also protects the identity privacy of nodes and prevents possible identity attacks or privacy leaks. |
| **C1534**<br>**16:45-17:00** | A Lightweight Hierarchical Blockchain Architecture for Multi-Party Data Collection in IoT<br>Author(s): Xingyi Li, Yueming Lu, Daquan Yang, Junqing Xi<br>Presenter: **Xingyi Li**, Beijing University of Posts and Telecommunications, China<br><br>Abstract: Multi-party data collection in Internet of Things (IoT) scenarios faces challenges such as high computational overhead, poor scalability, and storage redundancy when using traditional blockchain architectures. This paper proposes a lightweight hierarchical blockchain architecture to address these issues. The architecture employs a three-layer structure with static clustering, an improved Raft consensus mechanism featuring batch proposal and dual-trigger strategies, and an intelligent hierarchical data storage and routing policy. Experimental evaluation in a simulated wind power generation environment demonstrates that the proposed architecture significantly reduces storage overhead by 66.7\% and global consensus operations by 85.7\%, while achieving an average transaction latency of 47.85 ms. The system exhibits near-linear scalability, providing an efficient and scalable solution for trusted data collection in resource-constrained IoT environments. |
| **C2416**<br>**17:00-17:15** | TEE and Blockchain-Assisted Attribute Based Access Control for Fog-enabled IoT Systems<br>Author(s): Zhuoxin Liao, Shuai Shang,Yi Wu, Chenmin Wang, Tao Liu,Chunhua Su<br>Presenter: **Zhuoxin Liao**, University of Aizu, Japan<br><br>Abstract: The nature of the Internet of Things (IoT), imbalanced capabilities and limited resources, leads to challenges for secure access control. Blockchain is an emerging technology that can enhance authorization schemes for distributed IoT systems. However, existing authorization methods that directly store authorization-related data and execute authorization logic on-chain lead to high gas costs, increased latency, and potential exposure of sensitive information. To address the issues of confidentiality and performance, this paper proposes a fog-enabled IoT authorization system utilizing attribute-based access control (ABAC) and integrates permissioned blockchain with a Trusted Execution Environment (TEE). We design a fine-grained ABAC scheme for IoT systems. Meanwhile, the blockchain records IoT states on-chain, while the TEE stores sensitive data and performs authorization off-chain, thereby providing state transparency and auditability while maintaining confidentiality and efficiency. Experimental results show that the proposed system achieves lower gas consumption and processing latency compared to previous schemes. |
| **C2905**<br>**17:15-17:30** | An Evolutionary Vulnerability Analysis Method Combining K-Truss Constraints and Improved Matroid Closure<br>Author(s): Ziyuan Liu, Xinhong Hei, Yichuan Wang, Xiaoxue Liu, Peipei Li, Weilin Zhu<br>Presenter: **Ziyuan Liu**, Xi'an University of Technology, China<br><br>Abstract: Addressing dual challenges of combinatorial explosion and hidden structure mining in complex network critical link identification, this paper proposes an evolutionary vulnerability analysis method. It combines K-Truss pruning with improved connected matroid closure. Through Block-Cut tree decomposition and K-Truss constraints, the global exponential search space $O(2^{\|E\|})$ is decomposed into local subproblems. An improved closure generation algorithm is further designed. It uses path compression and connectivity filters. This constructs multi-scale closure lattices and proposes the MEV quantification metric. Simulations on IEEE 118-Bus, US Airlines, and Internet AS networks demonstrate that MEV has topological adaptability. It can lock onto "non-hub bridges" and cut-sets with insignificant degrees but crucial for global connectivity. The axiomatic model established in this paper maps from geometric topology to algebraic structure. It provides new theoretical and computational tools for evolutionary vulnerability assessment in large-scale complex systems. |
| **C3445**<br>**17:30-17:45** | Research on Hierarchical Governance of Social Media Account Inheritance: Centered on the Balance between Users' Information Self-determination Right and Platform Responsibility<br>Author(s): Yuanqing Wen, Yiming Guo<br>Presenter: **Yuanqing Wen**, Beijing Normal University, China |

| | |
|---|---|
| | Abstract: Based on an analysis of user agreements from 36 major social platforms and survey responses from 214 users, this paper reveals a deep conflict between the platform's complete ban on account inheritance and users' information self-determination rights as well as the inheritance rights of close relatives. Ultimate purpose of data governance is people rather than data itself.Theoretically, it argues for the inheritability of social media accounts from the perspectives of data management ethics and legal theory. What is inheritable is the data carrier rather than personality rights. It also acknowledges platforms' legitimate role as big data managers in ensuring cybersecurity, protecting communication secrets, and safeguarding personal information, while maintaining that their managerial power must be constrained by the principle of fairness and the principle of proportionality. At the level of institutional design, a governance framework centered on data classification was proposed. This framework classifies social data into five major categories: public content, private content, interactive content, virtual property, and metadata by constructing an attribute vector composed of privacy sensitivity, externalities, asset utility, and time decay. Based on this, it implements differentiated inheritance rules. Finally, from the perspective of technical implementation, this paper suggests that the platform establish a user intention setting module, a death recognition mechanism, and a privacy desensitization engine, and transform the institutional principles into system execution power through identity authentication and permission isolation technologies. |
| **C3210**<br>**17:45-18:00** | A Method for Detecting Cyberattacks Based on the Semantic Mapping of the Kill Chain<br>Author(s): Yingfeng Shi, Yichuan Wang, Dian Zhang, Xiaoxue Liu, Xindong Wang, Yu Han<br>Presenter: **Yingfeng Shi**, Xi'an University of Technology, China<br><br>Abstract: To address the semantic fragmentation and defense latency issues inherent in software-defined networks when confronting advanced persistent threats, this paper proposes a network attack detection method grounded in kill chain semantic mapping. First, an attack semantic mapping model is constructed. Macroscopic attack logic is abstracted into a finite state automaton. Quantitative associations are established between this abstraction and underlying multi-dimensional telemetry features. Second, a lightweight architecture integrating event-driven and asynchronous polling mechanisms is designed. This architecture extracts five-dimensional core features characterizing network connection properties with minimal overhead. Finally, an attack phase classification framework is built upon the random forest algorithm. Experimental results demonstrate that this method achieves phase identification in complex noisy environments. It exhibits low space complexity and smooth computational overhead during large-scale topology expansion. It effectively mitigates the state explosion bottleneck plaguing conventional deep packet inspection mechanisms. Thereby, it confers global attack semantic cognition capabilities upon SDN to enable proactive defense against sophisticated network threats. |
| **C3930**<br>**18:00-18:15** | Blockchain Adoption Strategies in Data Supply Chains under Cost-Sharing Contracts<br>Author(s): Lei Wang, Jianming Zhu<br>Presenter: **Lei Wang**, Central University of Finance and Economics, China<br><br>Abstract: To address the issue of unauthorized resale of data products during their trading process, this paper focuses on the data supply chain comprising data providers and data trading platforms, and constructs a Stackelberg game model in which the data provider acts as the leader and the data trading platform as the follower. This paper systematically analyzes three blockchain implementation scenarios: no blockchain technology, blockchain technology only introduced by data trading platforms, and blockchain technology collaboratively introduced by data providers and platforms through cost-sharing contracts, and explores the optimal equilibrium solution under each scenario. The study finds that: (1) Blockchain technology enhances the pricing power, effort levels, and market demand of all parties in the data supply chain by reducing unauthorized resale. (2) When only the platform adopts blockchain technology, data providers exhibit significant "free-riding" behavior. Cost-sharing agreements can effectively address this "free-riding" issue, alleviate the platform's cost investment constraints, and achieve a Pareto improvement in the data supply chain. (3) Under the cost-sharing contract scenario, data providers' profits exhibit a typical inverted Ushaped pattern as the cost-sharing ratio increases, indicating the existence of an optimal cost-sharing ratio. When the cost-sharing ratio exceeds a critical threshold, providers' profits fall below those in the baseline scenario without blockchain, and providers lose the economic incentive to fulfill the |

| | |
|---|---|
| | cost-sharing contract. This study provides decision-making guidance for blockchain adoption and contract design in data trading markets. |

# ONLINE SESSION A

- **Topic: Data Encryption and Privacy Protection**
- **Online Link: https://us02web.zoom.us/launch/jc/86898180738 Password: BDPC**
- **Time: May 31, 2026 | 10:00-12:05**

- **Session Chair: Assoc. Prof. Renwan Bi, Minjiang University, China**
- **Invited Speaker, C2190, C2865, C3661, C3669, C3696, C4039, C4050**

| | |
|---|---|
| **Invited Speaker**<br>**10:00-10:20** | **Prof Ts Dr Madihah Mohd Saudi, Universiti Sains Islam Malaysia (USIM), Malaysia**<br><br>**Title: Building National Resilience Against Cyber-Enabled Crime: The Fusion Centre Imperative** |
| **C2190**<br>**10:20-10:35** | Privacy Entity Recognition in Social Networks Based on Residual BiLSTM and Span-Level Extraction<br>Author(s): Zhen Guo, Shengzhi Feng, Jia Xu<br>Presenter: **Shengzhi Feng**, Hainan University, China<br><br>Abstract: The growth of user-generated content on social networks has increased the risk of exposing privacy-sensitive information. In this setting, privacy entity recognition is difficult because social media posts are informal, boundary-ambiguous, and may contain nested or overlapping entities. We propose RBLS-PER, a span-based privacy entity recognition framework for social network text. RBLS-PER combines an improved GAU-BERT encoder, a residual BiLSTM module, and efficient global pointer (EGP) decoding: GAU-BERT provides contextual token representations, the residual BiLSTM refines local sequential and boundary cues, and EGP scores privacy-type-specific start-end token pairs. The model is trained with multilabel categorical cross-entropy and fast gradient method (FGM) adversarial training to reduce span imbalance and improve stability under surface variation. On a real-world Weibo privacy dataset, RBLS-PER achieves 94.13% accuracy and 94.04% F1-score on the independent test set. Additional evaluations on external Chinese benchmarks further indicate cross-dataset robustness within the tested settings. |
| **C2865**<br>**10:35-10:50** | Research on Privacy Analysis Technology of Multi-tab Website Fingerprinting for Anonymous Networks<br>Author(s): Shengwei Xu, Weigang Ma, Litao Qiao, Yichuan Wang<br>Presenter: **Shengwei XU**, Xi'an University of Technology, China<br><br>Abstract: Multi-tab browsing generates interleaved traffic that severely degrades the performance of traditional website fingerprinting (WF) attacks due to feature entanglement. Existing methods, limited by the single-tab assumption and restricted receptive fields of CNNs, struggle to decouple mixed traces and handle open-world noise. To address these challenges, we propose MTP-Net, a multi-label WF framework tailored for multi-tab scenarios. MTP-Net incorporates a dilated residual network to expand the receptive field for capturing multi-scale temporal dependencies and utilizes a dynamic focus loss to enhance discrimination on hard samples. Extensive experiments on both simulated and real-world datasets demonstrate that MTP-Net consistently outperforms state-of-the-art methods. Notably, it achieves an 11.8% accuracy improvement over TMWF in dualtab scenarios while maintaining a low false positive rate. These results underscore critical privacy vulnerabilities in anonymous communication systems and offer insights for robust defense mechanisms |
| **C3661**<br>**10:50-11:05** | An Automatic Privacy Data Perception Model for Social Networks Based on Dynamic Prompt and Cross-Attention Gated Fusion<br>Author(s): Jiayi Li, Jia Xu, Zhen Guo<br>Presenter: **Jiayi Li**, Hainan University, China<br><br>Abstract: Online social networks (OSNs) generate massive volumes of user-created text in which sensitive personal information is often implicitly embedded within unstructured content, posing potential privacy leakage risks. However, existing privacy entity recognition methods are limited by data sparsity and the noisy nature of informal social media language, |

| | |
|---|---|
| | making it difficult to effectively capture both global contextual semantics and fine-grained local features. To address these issues, we propose a dynamic prompt and cross-attention gated fusion framework for privacy entity recognition (DP-CAGF). At the encoding stage, a dynamic prompt mechanism enhances the THUCBERT encoder to enable context-adaptive semantic representation learning. For feature modeling, cross-attention and adaptive gating are integrated into a BiGRU to fuse global semantic representations with local sequential features while reducing noise propagation. At the decoding stage, a dual-masked global pointer (DMGP) with span-length priors is employed to prune invalid candidate spans and improve nested entity extraction. Experiments on real-world OSN datasets show that DP-CAGF achieves an F1-score of 94.46\%. Compared with existing methods, the proposed framework demonstrates stronger generalization capability and robustness, effectively protecting privacy information in OSNs. |
| **C3669**<br>**11:05-11:20** | TradeTrace-WM: Scalable white-box watermarking with model traceability and ownership verification in model Marketplaces<br>Author(s): Yujie Yao, Youliang Tian, Shuai Wang<br>Presenter: **Yujie Yao**, Guizhou University, China<br><br>Abstract: In model marketplaces, copyright protection needs to support not only ownership verification but also authorized distribution, leakage tracing, and license evolution throughout the model lifecycle. Existing white-box watermarking methods often exhibit low efficiency in tracing leaked models in large-scale authorization settings and become less reliable after common post-processing operations such as fine-tuning, pruning, and quantization. They also provide limited support for preserving an auditable history when license states change due to resale, renewal, or permission updates. To address these issues, we propose TradeTrace-WM, a unified framework for model trading and copyright governance. The framework embeds a buyer- linked white-box watermark consisting of a public short retrieval tag and an ECC-protected payload, which enables efficient candidate filtering and robust user-level attribution. To handle dynamic license evolution, it combines chameleon hash with append-only Merkle Mountain Range (MMR) logs, allowing legitimate license updates while preserving a stable certificate anchor and a verifiable transfer history. Based on this design, TradeTrace-WM unifies system initialization, buyer-specific wa- termark issuance, license-state update, and leakage tracing with license-chain validation, while producing portable verification materials for independent auditing. The framework provides an integrated solution for ownership verification, scalable leakage tracing, and auditable license governance in model marketplaces. |
| **C3696**<br>**11:20-11:35** | A Mediation-Based Approach to Measuring Privacy Willingness<br>Author(s): Yiming Guo; Jiayi Liu; Yapeng Li; Xiaolong Zhao<br>Presenter: **Yiming Guo**, Beijing University of Technology, China<br><br>Abstract: As digital platforms become deeply embedded in daily life, the formation mechanism of users' privacy willingness has emerged as a critical issue in privacy governance and platform design. Existing research has mostly focused on subjective privacy concerns or fragmented external factors, lacking a unified quantitative framework that integrates objective environmental factors with subjective cognition. This paper proposes a structural equation model of "objective environmental factors — subjective cognitive factors — privacy willingness," incorporating objective variables such as regulations, media exposure, security incidents, and platform settings along with subjective variables including perceived risk, perceived benefit, controllability, and trust into a unified mediation model. Empirical analysis based on 862 survey responses and externally coded data shows that objective factors primarily influence privacy willingness indirectly through subjective cognitive factors. The full mediation model demonstrates explanatory power and predictive accuracy superior to the objective-only model, classic privacy calculus models, and machine learning baselines. This study provides an extensible theoretical framework and operational methodological approach for the quantification of privacy needs, offering empirical support for platform governance and policy intervention. |
| **C4039**<br>**11:35-11:50** | Attention-Based Adaptive Differential Privacy Noise Injection Framework for Privacy-Preserving Income Classification<br>Author(s): Jiaming Zhang, Shuai Shang, Yi Wu, Tao Liu, Chunhua Su<br>Presenter: **Jiaming ZHANG**, University of Aizu, Japan |

| | |
|---|---|
| | Abstract: Tabular datasets containing sensitive personal attributes are widely used for classification but pose substantial privacy risks. Uniform differential privacy mechanisms such as DP-SGD apply a fixed privacy budget across features, often over-noising predictive attributes and under-protecting weak ones. This paper introduces an Attention-Based Adaptive Differential Privacy Noise Injection Framework that uses Transformer encoders and multi-head self-attention to estimate feature importance and allocate local privacy budgets. High-importance features receive smaller noise for utility preservation, whereas low-importance features receive stronger protection. The noisy embeddings are processed by a DP-SGD optimized MLP classifier with contrastive learning. Experiments on the Adult Census Income and Bank Marketing datasets show competitive privacy-utility trade-offs across multiple ε values while keeping membership-inference risk low. |
| **C4050**<br>**11:50-12:05** | Defending Federated Learning Against Model Poisoning Attacks via Eliminating Malicious Features<br>Author(s): Weiqi Qiu, Qinbo Liu, Ziqian Zeng, Yuchen Tian, Zoe L Jiang, Yang Liu<br>Presenter: **Weiqi Qiu**, Harbin Institute of Technology, Shenzhen, China<br><br>Abstract: Federated learning (FL) is susceptible to model poisoning attacks, in which malicious clients compromise the global model by sending manipulated model updates to the server. While numerous studies have proposed defenses against such attacks, these defenses often struggle to handle complex attack patterns or heterogeneous data distributions in practical scenarios. Moreover, existing defenses face significant limitations in efficiency and applicability, particularly when dealing with large-scale or highly sophisticated attacks. This article studies model poisoning attacks in FL, showing the effectiveness of such attacks and the difficulties of defending against them via a theoretical foundation. To address the above challenges, we introduce a novel defense method designed to mitigate model poisoning attacks more effectively by eliminating malicious features, and design differential privacy-based defense (DPD) and selective aggregation-based defense (SAD), respectively. Empirical evidence from experiments with public datasets verifies their effectiveness. In particular, SAD outperforms all baseline defense methods in defending against Min-Max attacks. Additionally, SAD effectively defends against other attack types, achieving optimal or near-optimal defense performance in our experiments. |

# ONLINE SESSION B

- **Topic: Big Data Analysis and Computing**
- **Online Link: https://us02web.zoom.us/launch/jc/86898180738 Password: BDPC**
- **Time: May 31, 2026 | 14:00-15:30**

- **Session Chair: Prof. Yanhong Guo, Dalian University of Technology, China**
- **Order: C2303, C2619, C3646, C4367, C4498, C4593**

| | |
|---|---|
| **C2303**<br>**14:00-14:15** | The impact of enterprise incremental innovation on stock return<br>Author(s): Yong Li<br>Presenter: **Yong Li**, Guangdong University of Science and Technology, China<br><br>Abstract: We use text-mining techniques to analyze the similarity of patent content, quantify the degree of enterprise incremental innovation within firms, and further examine the impact of enterprise incremental stock return and its mechanisms by applying the fixed-effect panel model. The research results show that the enterprise incremental innovation has a positive impact on stock return. Second, enterprise incremental innovation improves stock return by increasing return to scale. Third, the positive impact of enterprise incremental innovation on stock returns is more significant for non-state-owned firms during periods of bear market environment. This study provides a new practical case for the application of big data analysis methods in empirical studies. |
| **C2619**<br>**14:15-14:30** | HieraPower: A Hierarchical SAC-TD3 Framework for Task Scheduling in Computing Power Networks<br>Author(s): JiaXing Zhu, ChongWu Dong, Zhe Sun, WuShao Wen<br>Presenter: **Jiaxing Zhu**,Sun Yat-sen University, China<br><br>Abstract: Computing Power Networks (CPNs) are increasingly becoming key infrastructure in the era of large foundation models. These networks bring together geographically dispersed computing resources that are usually managed by different organizations or administrative domains. Unlike traditional cloud architectures, CPNs face distinct challenges, such as crossdomain coordination, handling unpredictable load changes, and supporting latency-sensitive model inference. With the large-scale deployment of large language models (LLMs), scheduling tasks in these networks has become more complex. Traditional rule-based scheduling methods often cannot adapt to these dynamic, largescale scenarios, which highlights the need for more intelligent approaches. In response, we propose HieraPower, a hierarchical reinforcement learning framework for intelligent task scheduling in CPNs. HieraPower uses the Soft Actor-Critic (SAC) algorithm for intra-domain queue management and the Twin Delayed Deep Deterministic Policy Gradient (TD3) algorithm for crossdomain coordination. This combination allows it to optimize both task ordering and node selection. We also use graph neural networks (GNNs) to model the structural relationships in hierarchical computing settings. Through hierarchical decisionmaking, HieraPower learns a scheduling policy that better fits the practical needs of real-world computing tasks, rather than merely theoretical scenarios. |
| **C3646**<br>**14:30-14:45** | Futures Price Prediction Based on FourierGNN<br>Author(s): Shuangyi Zhang, Ning Zhang<br>Presenter: **Shuangyi Zhang**, Central University of Finance and Economics, China<br><br>Abstract: The multi-commodity futures market is characterized by complex spatiotemporal dependencies and high volatility, making accurate price prediction a challenging task. Traditional forecasting models often focus on single-commodity analysis or rely on discrete spatiotemporal modeling, failing to capture the dynamic interdependencies and periodic patterns across diverse commodities. This paper adopts FourierGNN, a universal multi-commodity futures price prediction model that integrates multi-scale feature extraction, hypervariate graph modeling, and frequency-domain graph convolutions. By mapping multivariate time series into a unified hypervariate graph, the model jointly captures temporal evolutions and cross-commodity spatial correlations. The frequency-domain graph convolution |

| | |
|---|---|
| | mechanism efficiently extracts periodic features while maintaining log-linear computational complexity. Empirical evaluations on a comprehensive dataset of 59 futures commodities across five categories demonstrate that FourierGNN significantly outperforms state-of-the-art baselines in both long-term and short-term prediction tasks. The results highlight the model's superior generalization ability and robustness in volatile market environments, providing a scalable framework for multi-commodity financial forecasting. |
| **C4367**<br>**14:45-15:00** | GRAD:Gradient-based Robustness Audit for Multimodal Diffusion Models<br>Author(s): Zhenghong He, Yani Wang, Zijie Pan, Zuobin Ying<br>Presenter: **Zhenghong He**, City University of Macau, China<br><br>Abstract: Multimodal diffusion models synthesize visual con tent by mapping text and image conditions into latent spaces. Current safety protocols primarily rely on post-hoc filtering to intercept non-compliant outputs. However, these mechanisms operate independently of the internal computation graph, leav ing intrinsic vulnerabilities within the cross-attention layers unquantified. In this work, we propose GRAD, a Gradient-based Robustness Audit framework designed to quantify the secure margins of diffusion architectures via latent sensitivity analysis. By backpropagating semantic losses to the embedding space, GRAD maps the susceptibility of internal feature manifolds using a novel sensitivity metric, which identifies the maximum alignment between gradient vectors and the discrete vocabulary. Our audit on the official I2P benchmark reveals a scaling-induced robustness: while Stable Diffusion XL(SDXL) reduces the empirical ASR to 2.08%, its internal sensitivity is concurrently suppressed by an order of magnitude compared to Stable Diffusion v1.5(SD v1.5). Index Terms—Diffusion Models, robustness audit, gradient based analysis, multimodal security. |
| **C4498**<br>**15:00-15:15** | A Circular Bounding Box Detection Algorithm Based on Improved YOLOv8 for Dense Fruit Images<br>Author(s): JunYu Zhu, Xiaoying Zheng<br>Presenter: **JunYu Zhu**, Wuhan Institute of Technology, China<br><br>Abstract: Aiming at the problems of background noise interference and low positioning accuracy of rectangular bounding boxes in dense mixed fruit image detection, this paper proposes a fruit object detection algorithm based on circular bounding boxes. Built on the YOLOv8 architecture, the algorithm constructs a circular annotated dataset and optimizes the core calculation modules of object detection by deriving the analytical expressions of circle center coordinates and radius, realizing the intersection over union calculation and non-maximum suppression of circular bounding boxes. Through multi-scale feature extraction via deep convolutional networks and position prediction of circular objects, the algorithm effectively reduces background interference in dense scenes and enhances recognition accuracy. This method realizes the integration of intelligent detection technology and agricultural big data applications, and provides a practical technical scheme for the precise identification of agricultural products. It not only solves the key technical problem of dense object detection in agricultural visual tasks, but also expands the application scope of big data science in the field of smart agriculture |
| **C4593**<br>**15:15-15:30** | Membership and property inference attacks on text data in transfer learning<br>Author(s): Zhiqian Jiang<br>Presenter: **Zhiqian Jiang**,City University of Macau, China<br><br>Abstract: In recent years, with the rapid development of machine learning technologies and significant improvements in computer hardware performance, deep learning has also experienced rapid growth and has been widely applied across almost all fields, including healthcare, finance, education, and biology. With the widespread adoption of artificial intelligence technologies, a series of issues inevitably arise, especially in the area of AI security. Drawing from the concept of unlearning, it is known that large models tend to "memorize" part of the information from the training data, or learn the distribution of global attributes. Attackers can exploit this to carry out property inference attacks and membership inference attacks. Although large models represent an advanced and efficient technology, the costs of time and resources often make it impractical to train a model from scratch for each specific task. Today, a common practice is to use transfer learning. Therefore, it is essential to conduct in-depth research on property inference attacks and membership inference attacks in the context of transfer learning. Natural language processing is an important branch of artificial |

| | |
|---|---|
| | intelligence. However, existing research on membership inference attacks and property inference attacks has paid relatively little attention to textual data. To address this gap, this paper shifts the focus of inference attacks to textual data. |

# ONLINE SESSION C

- **Topic: Data Security and Blockchain Application Technology**
- **Online Link: https://us02web.zoom.us/launch/jc/86898180738 Password: BDPC**
- **Time: May 31, 2026 | 16:00-17:45**

- **Session Chair: Dr. Zhihui Wang, Fudan University, China**
- **Order: C1315, C2431, C2570, C4622, C4790, C4804, C3319**

| | |
|---|---|
| **C1315**<br>**16:00-16:15** | Blockchain as a Privacy-Preserving Control Environment for Skills Data Sharing and Data-Driven Hiring<br>Author(s): Li chunba and Joao C Ferreira<br>Presenter: **Joao C Ferreira**, Molde University Collegue, Norway<br><br>Abstract: Professional skills reputation is increasingly critical in modern labor markets, where individuals must demonstrate competencies across multiple employers, platforms, and countries. However, today's credentialing and reputation mechanisms remain fragmented, centrally controlled, and vulnerable to falsification, misrepresentation, or loss of verification context. This paper proposes a blockchain-based framework for building a portable professional reputation layer grounded in verifiable skills, certifications, and performance evidence. The framework leverages decentralized identifiers (DIDs), verifiable credentials (VCs), and smart contracts to ensure integrity, traceability, and tamper-resistance across the professional lifecycle. We present a conceptual architecture, governance model, and use cases ranging from higher education and continuous professional development to regulated professions and cross-border employability. Challenges related to privacy, scalability, and adoption are discussed, and future research directions are proposed |
| **C2431**<br>**16:15-16:30** | Automatic Anonymization of Unstructured Text: Detecting Sensitive Information with Fine-Tuning Large Language Models<br>Author(s): Zhuo Yao, Keyong Hong, Xiangyu Wang, Jianfeng Ma<br>Presenter: **Zhuo Yao**, Xidian University Xi'an, China<br><br>Abstract: In the age of digital connectivity, vast amounts of data are openly shared across social platforms, e-commerce platforms, and other online channels, potentially leading to inadvertent exposure of sensitive information. As a crucial mechanism for protecting sensitive information, anonymization techniques for structured data have already reached a relatively mature stage. Nevertheless, unstructured textual data lacks fixed structures and involves diverse entity types, making sensitive information difficult to identify through automated methods. Meanwhile, automated anonymization of unstructured text still relies heavily on manual processing, which is costly and inefficient, and thus requires further optimization. Presently, Large Language Models (LLMs) have demonstrated remarkable capabilities in semantic understanding and reasoning, but its effectiveness in anonymizing sensitive information within unstructured text still lacks systematic research. In this paper, we employ two finetuning approaches, namely Prefix Tuning and Low-Rank Adaptation (LoRA) Fine-Tuning, and verify that fine-tuned LLMs still achieve excellent performance in the task of anonymizing sensitive information in texts. Furthermore, we conduct a comparative evaluation and analyze their similarities and differences with traditional Named Entity Recognition (NER) and rule based anonymization approaches. The evaluation results indicate that the fine-tuning model achieves outstanding performance in sensitive information anonymization tasks. Index Terms—Sensitive Information Anonymization, Fine-Tuning Large Language Models, Named Entity Recognition, Unstructured Text. |
| **C2570**<br>**16:30-16:45** | Identity Authentication for Satellite + Telecommunications Network Converged Access<br>Author(s): Yaling Zhang, Ruixuan Zhang, Yichuan Wang , Xiaoxue Liu<br>Presenter: **Ruixuan Zhang**,Xi'an University of Technology, China<br><br>Abstract: In extreme geographical environments such as oceans, deserts, and deep mountains, extending the 5G core network (5GCN) using non-terrestrial networks (NTN) is key to ensuring communication and IoT access. However, the existing terminal (UE) direct-to-satellite mode is |

| | |
|---|---|
| | limited by terminal power and faces challenges such as insufficient budget, signal blockage, and signaling congestion. To address these issues, this paper proposes a joint authentication method based on satellite relay bridging and Double Proxy Re-Encryption (Double PRE). At the physical layer, bridging nodes are introduced, and through signal aggregation and directional beam technology, the connection survival of terminals is ensured while preventing eavesdropping. To address the trust issue introduced by the relay, a four-party joint authentication protocol of "Terminal-BridgeSatellite-Network" is designed. Using Double PRE, the satellite acts as a proxy to convert the terminal's encrypted data into a format recognizable by the 5GCN, combined with HKDFHMAC key derivation technology to replace the traditional multistep handshake process. Security analysis demonstrates that this scheme can resist various attacks. Performance analysis shows that the authentication latency of the scheme is 42.858 ms and its communication overhead is 2384 bits, exhibiting low authentication latency and communication overhead while ensuring security. |
| **C4622**<br>**16:45-17:00** | Trust-Adaptive Byzantine Consensus in Dynamic Vehicular Networks<br>Author(s): Yuxin Zhu, Li Lin, Jinbo Xiong, Xing Wang, Biao Jin, Ruihong Huang, and Limei Lin<br>Presenter: **Yuxin Zhu**, Fujian Normal University, China<br><br>Abstract: Dynamic vehicular networks present significant challenges for Byzantine consensus because node reliability, network connectivity, and attack intensity can vary significantly over time. Consequently, conventional Practical Byzantine Fault Tolerance (PBFT)-style protocols are difficult to apply directly in such settings because they rely on equal-weight voting, static fault thresholds, and limited responsiveness to intermittent adversarial behaviors such as On-Off attacks. To address these limitations, this paper presents a trust-adaptive consensus framework tailored for dynamic vehicular networks, in which continuous trust assessment guides consensus influence, leader selection, and feedback-based correction within a closed-loop design. By translating trust assessment into a control signal within the consensus process, the framework dynamically adjusts voting weights and effectively mitigates the disruptive impact of unreliable nodes. Representative NS-3 simulations demonstrate encouraging performance trends over conventional baselines in the evaluated settings, suggesting that trust-adaptive control is a promising direction for resilient coordination in dynamic vehicular networks. |
| **C4790**<br>**17:00-17:15** | When Data Trading Meets Secure Computation<br>Author(s): Zhao Bowen, Tian Bo, Yang Kaixiang, Yuling Chen, Yulong Shen, Pei Qingqi<br>Presenter: **Tian Bo**, XIdian University, China<br><br>Abstract: Data trading is a crucial component of the digital economy; however, it faces several challenges. The data capacity must exceed the market's demand due to the replicability of data, which results in excess capacity. Identical data may be sold multiple times or by multiple parties simultaneously, disrupting the data trading market. Data privacy concerns impede data trading and its usability. Unfortunately, how to tackle the above challenges remains an open problem. To this end, this paper aims to discuss two types of data trading: on-exchange trading and off-exchange trading, and seeks to answer two key questions: 1) \textit{Can trading data be prevented from being resold, given that it can be copied}? 2) \textit{If the answer to the first question is yes, can privacy-preserving data trading be achieved through secure computation}? Subsequently, this paper presents privacy-preserving on-exchange data trading using secure outsourced computation and privacy-preserving off-exchange data trading through secure two-party computation. Finally, it outlines the research challenges associated with privacy-preserving data trading. |
| **C4804**<br>**17:15-17:30** | Breaking the Memory Wall: Hessian-Regularized Gradient Boosting for Edge-Based IIoT Security<br>Author(s): Weifeng Zeng, Zuobin Ying, Jiayi Chen<br>Presenter: **Weifeng Zeng**, City University of Macau, Macao SAR, China<br><br>Abstract: Industrial Internet of Things (IIoT) edge gateways increasingly require local intrusion detection, but these embedded devices often reserve only limited static storage for auxiliary security models and may face temporally skewed traffic distributions. Although resampling methods such as SMOTE can mitigate distribution skew, they introduce additional training-time memory overhead and are therefore less suitable for edge-side adaptation. This paper proposes FL-BHT-LightGBM, a compact gradient boosting framework that combines cost-sensitive focal |

| | |
|---|---|
| | loss (FL) with Bounded Hessian Transformation (BHT). Under non-convex focal-type losses, unreliable second-order derivatives may destabilize LightGBM leaf updates. BHT addresses this issue by replacing negative or near-zero curvature terms with a lower-bounded positive surrogate while preserving well-conditioned positive Hessians, thereby stabilizing boosting without relying on synthetic sample generation. Experiments on the ML-EdgeIIoT dataset using chronological walk-forward validation show that the proposed method maintains competitive detection performance while avoiding resampling-induced memory overhead. The compiled model occupies only 0.333 MB and achieves an average per-sample inference latency of 0.0548 ms. In addition, a lightweight temporal aggregation module reduces isolated packet-level false positives before SOC escalation. These results indicate that FL-BHT-LightGBM offers a deployment-oriented balance among numerical stability, compactness, and edge-side intrusion detection efficiency. |
| **C3319**<br>**17:30-17:45** | A Timing-Aware Camouflage Against Website Fingerprinting in Anonymous Communication<br>Author(s): Hao Pang, Yichuan Wang, Litao Qiao, Xiaoxue Liu, Ziyuan Liu, Ruixuan Zhang<br>Presenter: **Hao Pang**, Xi'an University of Technology, China<br><br>Abstract: Website fingerprinting attacks infer user browsing behavior by analyzing encrypted traffic patterns, posing a severe threat to user privacy in anonymous networks. Existing defense mechanisms employ global padding strategies, incurring prohibitive bandwidth overhead and latency costs. To address these limitations, this paper proposes WTFF, a timing-aware camouflage approach for website fingerprinting defense. WTFF constructs website timing profiles and employs burst-gap padding to morph raw traffic features toward target distributions selected from a temporal feature sequence pool, effectively obfuscating fingerprints and misleading attack classifiers while ensuring low latency and communication integrity. Evaluations on public datasets demonstrate that WTFF achieves robust defense against RF, CUMUL, DF, and Var-CNN attacks with minimal bandwidth and latency overhead. |

# MEMO