

*Time Zone: UTC+9*



## 2025 9th International Conference on Cryptography, Security and Privacy (CSP 2025)



## 2025 10th International Conference on Multimedia and Image Processing (ICMIP 2025)

**Okinawa, Japan | April 26-28, 2025**

*Co-Sponsored by*



**琉球大学**  
UNIVERSITY OF THE RYUKYUS

**R** RITSUMEIKAN  
UNIVERSITY



**西華大學**

*Technical Supported by*



*Published by*



PUBLISHED BY  
IEEE COMPUTER SOCIETY  
**CONFERENCE  
PUBLISHING  
SERVICES**

**SPIE.** DIGITAL  
LIBRARY

*Venue: University of the Ryukyus*

*Add.: 1 Senbaru, Nishihara-cho, Nakagami-gun, Okinawa, 903-0213 Japan*

# TABLE OF CONTENTS

Welcome Message.....	03
Conference Committee.....	04
General Information.....	06
Agenda Overview.....	07
Introduction of Speaker.....	10
On-site Session 1: Modern Cryptography Theory and Encryption Technology.....	15
On-site Session 2: Network Intrusion Detection and Defense.....	18
On-site Session 3: Data Privacy and Information Authentication.....	21
On-site Session 4: Computer Vision and Image Processing.....	24
Online Session 1: Information Security and Privacy Protection.....	27
Online Session 2: Image Analysis and Information Security Management.....	31
List of Delegate.....	35
One Day Tour.....	36
Note.....	37

## WELCOME MESSAGE

Dear all, we are delighted to welcome you to these conferences 2025 9th International Conference on Cryptography, Security and Privacy (CSP 2025), along with 2025 10th International Conference on Multimedia and Image Processing (ICMIP 2025) to be held in Okinawa, Japan during April 26-28, 2025, which is co-sponsored by University of the Ryukyus, Japan and Ritsumeikan University, Japan.

The objective of the conference is to provide a premium platform to bring together researchers, scientists, engineers, academics and graduate students to share up-to-date research results. We are confident that during this time you will get the theoretical grounding, practical knowledge, and personal contacts that will help you build a long term, profitable and sustainable communication among researchers and practitioners in the related scientific areas.

This year's program is composed of the keynote speeches delivered respectively by Prof. Yen-Wei Chen (Ritsumeikan University, Japan), Prof. Bin Xiao (The Hong Kong Polytechnic University, Hong Kong, China; Fellow, IEEE & AAIA), Prof. Changsheng Xu (Chinese Academy of Sciences, China; Fellow, IEEE & IAPR) and invited talks delivered respectively by Assoc. Prof. Mathew Nicho (Research and Innovation Centers, Rabdan Academy, UAE & UQ Cyber Research Centre, University of Queensland, Australia); Dr. Yang Liu (Swansea University, UK) with 4 offline technical sessions, 2 online technical sessions. We would like to express our gratitude to all the speakers in these conferences. Special thanks to all of our committee members, all the reviewers, the attendees for your active participation. We hope the conferences will be proved to be intellectually stimulating to us all. Finally, we wish you very successful conferences!

Conference Organizing Committee

### Contact Us

<b>CSP 2025</b>	<b>ICMIP 2025</b>
<b>Ms. Ching Cao</b>	<b>Ms. Sukie Yao</b>
<b>Email: <a href="mailto:iccsp_conf@126.com">iccsp_conf@126.com</a></b>	<b>Email: <a href="mailto:icmip2016@vip.163.com">icmip2016@vip.163.com</a></b>

# CONFERENCE COMMITTEE

*(in no particular order)*

## Advisory Committee

Bin Xiao, The Hong Kong Polytechnic University, Hong Kong, China (Fellow, IEEE)

## Conference Chair

Yen-Wei Chen, Ritsumeikan University, Japan

## Conference Organizing Chair

Shinya Nozaki, University of the Ryukyus, Japan

## Conference Co-Chair

Shuangbao Wang, Morgan State University, USA

## Conference Program Chairs

Hiroyuki Kudo, University of Tsukuba, Japan

Xiangyang Hao, Information Engineering University, China

Maozhi Xu, Peking University, China

Rose Shumba, Bowie State University, USA

## Conference Program Co-Chairs

Chin-Tser Huang, University of South Carolina, USA

Tomoko Tateyama, Fujita Health University, Japan

Masataka Seo, Osaka Institute of Technology, Japan

Paulo Batista, Cultures and Societies of the University of Evora, Portugal

Aleksandr Cariow, West Pomeranian University of Technology, Poland

## Conference Publicity Chairs

Huiyu Zhou, University of Leicester, UK

Jian Dong, Tianjin University of Technology and Education, China

Xiaofeng Wang, Xi'an University of Technology, China

Yutaro Iwamoto, Osaka Electro-Communication University, Japan

Phoebe Chen, La Trobe University, Australia

## Conference Finance Chair

Zhou Yadan, Shenzhen University, China

## Technical Program Committees

Pyke Tin, University of Miyazaki, Japan

Leila Rzayeva, Astana IT University, Kazakhstan

Heqing Huang, City University of Hong Kong, Hong Kong, China

Nilupulee Gunathilake, Edinburgh Napier University, UK

Mathew Nicho, Rabdan Academy, United Arab Emirates & The University of Queensland, Australia

Tokunbo Makanju, New York Institute of Technology, Canada

Meghana Kshirsagar, University of Limerick, Ireland

Reda Bellafqira, IMT Atlantique, France

Zhida Li, New York Institute of Technology - Vancouver Campus, Canada

Marlon A. Diloy, National University, Philippines  
Pham Thi Bach Hue, Viet Nam National University Ho Chi Minh City, Vietnam  
Xinli Xiong, National University of Defense Technology, China  
Tzu-Wei Lin, Feng Chia University, Taiwan  
Zhiyuan Shen, Nanjing University of Aeronautics and Astronautics, China  
Maleerat Maliyaem, King Mongkut's University of Technology North Bangkok, Thailand  
Zakaria Alomari, New York Institute of Technology, Canada  
Goutham Reddy Alavalapati, University of Illinois, Springfield, USA  
Xiaoyu Li, Zhengzhou University, China  
Arren Matthew C. Antioquia, De La Salle University, Philippines  
Kuo-Yu Tsai, Feng Chia University, Taiwan  
Chung-Wei Kuo, Feng Chia University, Taiwan  
Christian Schindelbauer, University of Freiburg, Germany  
Chao-Lung Chou, Feng Chia University, Taiwan  
Vikas Thammanna Gowda, Champlain College, USA  
Thi Thi Zin, University of Miyazaki, Japan  
Wolfgang Ruppel, RheinMain University of Applied Sciences, Germany  
Tien-Ying Kuo, National Taipei University of Technology, Taiwan  
Jie-Fan Chang, National Taiwan University, Taiwan  
Yufeng Li, The University of Southampton, UK  
Yikui Zhai, Wuyi University, China  
Rui Chen, Tianjin University, China  
Shixiang Cao, Beijing Institute of Space Mechanics & Electricity, China  
Li Xie, Zhejiang University, China  
Xin Nie, Wuhan Institute of Technology, China  
Xiwen Zhang, Beijing Language and Culture University, China  
Jaouhar Fattahi, Laval University, Canada  
Abdubast Ali Abushgra, Utica College, USA  
Yang Liu, Swansea University, UK  
Chris Joslin, Carleton University, Canada  
Carlos Guardado da Silva, University of Lisbon, Portugal  
Gabriela MOGOS, Xi'an Jiaotong-Liverpool University, China  
Jalel Ben-Othman, Université de Paris, France  
Jorge Sequeira, Lisbon Accounting and Business School Polytechnic University, Portugal  
Paulo Batista, Cultures and Societies of the University of Evora, Portugal  
Hung-Yu Chien, National Chi Nan university, Taiwan  
Ashraf Darwish, Helwan University, Russia  
Yi Ding, University of Electronic Science and Technology of China, China  
Chau Kien Tsong, Universiti Sains Malaysia, Malaysia  
Por Fei Ping, Wawasan Open University, Malaysia  
V. T. Humbe, Swami Ramanand Teerth Marathwada University, India  
Ivan Izonin, Lviv Polytechnic National University, Ukraine  
Khalid ABBAD, University of Sidi Mohammed Ben Abdallah, Morocco  
Tushar H. Jaware, R.C.Patel Institute of Technology, India  
Saju Subramanian, Indra Ganesan College of Engineering, India  
Almas Abbasi, International Islamic University Islamabad, Pakistan  
Priteshkumar Prajapati, Chandubhai S. Patel Institute of Technology, India

# GENERAL INFORMATION

## A Conference Venue



**Venue: University of the Ryukyus**

**Addr.:** 1 Senbaru, Nishihara-cho, Nakagami-gun, Okinawa, 903-0213 Japan

**Conference Room Information:** 1F, Researcher Exchange Facility 50th Anniversary - University of the Ryukyus (琉球大学 研究者交流施設 50周年記念館 1F) ([Venue Map](#))

## B On-site Registration

Registration desk → Inform the staff of your paper ID → Sign-in → Claim your conference kits.

## C Devices Provided by the Organizer

Laptops (with MS-Office & Adobe Reader) / Projectors & Screen / Laser Sticks

## D Materials Provided by the Presenter

Oral Session: Slides (pptx or pdf version). Format 16:9 is preferred.

Presentation Language: English only.

## E Duration of Each Presentation

Keynote Speech: 45min, including 5min Q&A.

Invited Speech: 25min, including 5 min Q&A.


Oral Session: 15min, including 3 min Q&A.

## F Notice

※ Please wear your delegate badge (name tag) for all the conference activities. Lending your badge to others is not allowed.

※ Please take good care of your valuables at any time during the conferences. The conference organizer does not assume any responsibility for the loss of personal belongings of the participants during conference day.

## G Zoom Meeting

	Room	Meeting ID	Link
✓ <a href="#">Zoom Download</a> ✓ <a href="#">Zoom Background</a> ✓ <a href="#">Conference Banner</a>	A	868 1176 6939	<a href="https://us02web.zoom.us/j/86811766939">https://us02web.zoom.us/j/86811766939</a>

Note:

1. We recommend to install the Zoom platform beforehand. New users can login the Zoom meeting **without registration**.
2. Please set your display name before joining the online meeting. For instance,  
 Committee/Speaker: Committee/Speaker\_Name < Committee/Speaker\_Veronica Reed >  
 Author/Presenter: Paper ID\_Name < IP001\_Veronica Reed >  
 Delegate: Delegate\_Name < Delegate\_Veronica Reed >

## AGENDA OVERVIEW

### SATURDAY, APRIL 26, 2025 (UTC+9)

13:00~17:00	On-site Registration <1F, Researcher Exchange Facility 50th Anniversary - University of the Ryukyus (琉球大学 研究者交流施設 50 周年記念館 1F)>
10:00~12:30	Zoom Test Session (Room A: 868 1176 6939, Link: <a href="https://us02web.zoom.us/j/86811766939">https://us02web.zoom.us/j/86811766939</a> )
10:00~11:00	IP042 IP515 IP014 IP016 IP021 IP048 IP045 IP701 IP017 IP038
11:00~12:00	IP047 IP502 IP505 IP516 IP052 IP517 IP034 IP054 IP5002&IP5003
12:00~12:30	For other online participants, includes but not limited to keynote speaker, invited speaker, session chair, committee member, delegate, etc.

Presenters are required to join the rehearsal in Zoom on Saturday, April 26. Duration: 2~3min apiece. Feel free to leave after you finish the test.

# AGENDA OVERVIEW

## SUNDAY, APRIL 27, 2025 (UTC+9)

Plenary Session | <Room A, 1F> | Room A: 868 1176 6939, <https://us02web.zoom.us/j/86811766939>

Chairman

**Yen-Wei Chen**, Ritsumeikan University, Japan (*Conference Chair*)

09:00~09:10

Opening Speech

**Yen-Wei Chen**, Ritsumeikan University, Japan (*Conference Chair*)

09:10~09:55

*On-site*

Keynote Speech I

*"Knowledge-Guided Deep Learning for Enhanced Medical Image Segmentation"*

**Yen-Wei Chen**, Ritsumeikan University, Japan

09:55~10:40

*Online*

Keynote Speech II

*"Web 3.0: Architecture, Authentication and Application"*

**Bin Xiao**, The Hong Kong Polytechnic University, Hong Kong, China (Fellow, IEEE & AAIA)

10:40~11:10

**Group Photo / Coffee Break <1F>**

11:10~11:55

*Online*

Keynote Speech III

*"Connecting Isolated Social Multimedia Big Data"*

**Changsheng Xu**, Chinese Academy of Sciences, China (Fellow, IEEE & IAPR)

11:55~12:20

*On-site*

Invited Talk I

*"Dimensionality Reduction for Enhancing Malware Classification Accuracy in Portable Executable Files"*

**Mathew Nicho**, Research and Innovation Centers, Rabdan Academy, UAE & UQ Cyber Research Centre, University of Queensland, Australia

12:20~13:30

**Lunch Time <Room A+B, 1F>**

## SUNDAY, APRIL 27, 2025 (UTC+9) | Technical Session (On-site)

13:30~15:15

**On-site Session 1: Modern Cryptography Theory and Encryption Technology**

IP019 IP501 IP518 IP030 IP024 IP025 IP032

<Room A, 1F>

13:30~15:15

**On-site Session 2: Network Intrusion Detection and Defense**

IP023 IP031 IP543 IP053 IP020 IP046 IP035

<Room B, 1F>

15:15~15:30

**Coffee Break <1F>**

15:30~17:15

**On-site Session 3: Data Privacy and Information Authentication**

IP542 IP040 IP540 IP022 IP026 IP028 IP039

<Room A, 1F>

15:30~17:30

**On-site Session 4: Computer Vision and Image Processing**

IP519-A IP533-A IP513 IP520 IP544 IP530-A IP522 IP547-A

<Room B, 1F>

18:00~20:00

**Dinner Time <Restaurant>**



# AGENDA OVERVIEW

SUNDAY, APRIL 27, 2025 (UTC+9) | Technical Session (Online)

Room A: 868 1176 6939, <https://us02web.zoom.us/j/86811766939>

13:30~16:10

**Online Session 1: Information Security and Privacy Protection**

Invited Talk II: "A Privacy-Preserving Mechanism for Targeted Mobile Advertising"

**Yang Liu, Swansea University, UK**

IP042 IP515 IP014 IP016 IP021 IP048 IP045 IP017 IP038

16:10~16:30

**Break Time**

16:30~19:15

**Online Session 2: Image Analysis and Information Security Management**

IP047 IP502 IP505 IP516 IP052 IP517 IP034 IP054 IP5002 IP5003 IP701

# INTRODUCTION OF KEYNOTE SPEAKER

09:10-9:55 | Apr. 27, 2025 | Room A <1F>  
Room A: 868 1176 6939, <https://us02web.zoom.us/j/86811766939>



## Yen-Wei Chen

Ritsumeikan University, Japan

### Knowledge-Guided Deep Learning for Enhanced Medical Image Segmentation

**Abstract:** Recently, Deep Learning (DL) has played an important role in various academic and industrial domains, especially in computer vision and image recognition. Although deep learning (DL) has been successfully applied to medical image analysis, achieving state-of-the-art performance, few DL applications have been successfully implemented in real clinical settings. The primary reason for this is that the specific knowledge and prior information of human anatomy possessed by doctors is not utilized or incorporated into DL applications. In this keynote address, I will present our recent advancements in knowledge-guided deep learning for enhanced medical image analysis. This will include two research topics: (1) our proposed deep atlas prior, which incorporates medical knowledge into DL models; (2) language-guided medical image segmentation, which incorporates the specific knowledge of doctors as an additional language modality into DL models.

**Biography:** Yen-Wei Chen received the B.E. degree in 1985 from Kobe Univ., Kobe, Japan, the M.E. degree in 1987, and the D.E. degree in 1990, both from Osaka Univ., Osaka, Japan. He was a research fellow with the Institute for Laser Technology, Osaka, from 1991 to 1994. From Oct. 1994 to Mar. 2004, he was an associate Professor and a professor with the Department of Electrical and Electronic Engineering, Univ. of the Ryukyus, Okinawa, Japan. He is currently a professor with the college of Information Science and Engineering, Ritsumeikan University, Japan. He is the founder and the first director of Center of Advanced ICT for Medicine and Healthcare, Ritsumeikan University, Japan.

His research interests include medical image analysis, computer vision and computational intelligence. He has published more than 300 research papers in a number of leading journals and leading conferences including CVPR, ICCV, MICCAI, IEEE Trans. Image Processing, IEEE Trans. Medical Imaging. He has received many distinguished awards including ICPR2012 Best Scientific Paper Award, 2014 JAMIT Best Paper Award. He is/was a leader of numerous national and industrial research projects.

# INTRODUCTION OF KEYNOTE SPEAKER

09:55-10:40 | Apr. 27, 2025 | Room A <1F>  
Room A: 868 1176 6939, <https://us02web.zoom.us/j/86811766939>



## Bin Xiao

Fellow, IEEE & AAIA

The Hong Kong Polytechnic University, Hong Kong, China

### Web 3.0: Architecture, Authentication and Application

**Abstract:** The rise of Web 3.0 technology and distributed ledger systems has led to a significant change in traditional centralized authentication systems in Web2. These conventional systems have inherent weaknesses, including technical issues like vulnerability to single-point failures and cybersecurity threats, as well as societal concerns about the excessive concentration of personal data. To address these issues, Web3-native decentralized identity and verifiable credential systems have been developed. These systems use blockchain technology and distributed storage protocols to improve security and privacy. Architecturally, this approach gives end users full control over their identifiers and credentials, allowing them unprecedented control over their personal data. In this talk, we will first show the architecture of a Web 3.0 system and identify the technical difference between Web 3.0 and Web 2.0. Then, we will present how to conduct authentication in Web 3.0 by utilizing decentralized identifiers (DID) and verifiable credentials. Finally, we will demonstrate a developed Web 3.0 application that can facilitate users to manage their own DIDs and credentials.

**Biography:** Dr. Bin Xiao is a professor at the Department of Computing, the Hong Kong Polytechnic University, Hong Kong. Prof. Xiao received the B.Sc and M.Sc degrees in Electronics Engineering from Fudan University, China, and a Ph.D. degree in computer science from the University of Texas at Dallas, USA. His research interests include AI security, data privacy, Web3, and blockchain systems. He is currently an Associate Editor of the IEEE Transactions on Cloud Computing. He has been the associate editor of the IEEE Internet of Things Journal, IEEE Transactions on Network Science and Engineering, and Elsevier Journal of Parallel and Distributed Computing. He is the IEEE Fellow, AAIA Fellow, IEEE ComSoc Distinguished Lecturer, and the chair of the IEEE ComSoc CISTC committee from 2024 to 2025. He has been the program co-chair of IEEE CNS2025, track co-chair of IEEE ICDCS2022, the symposium track co-chair of IEEE Globecom 2024, ICC2020, ICC 2018, and Globecom 2017, and the general chair of IEEE SECON 2018.

# INTRODUCTION OF KEYNOTE SPEAKER

11:10-11:55 | Apr. 27, 2025 | Room A <1F>

Room A: 868 1176 6939, <https://us02web.zoom.us/j/86811766939>



## Changsheng Xu

Fellow, IEEE & IAPR

Chinese Academy of Sciences, China

### Connecting Isolated Social Multimedia Big Data

**Abstract:** The explosion of social media has led to various Online Social Networking (OSN) services. Today's typical netizens are using a multitude of OSN services. Exploring the user-contributed cross-OSN heterogeneous data is critical to connect between the separated data islands and facilitate value mining from big social multimedia. From the perspective of data fusion, understanding the association among cross-OSN data is fundamental to advanced social media analysis and applications. From the perspective of user modeling, exploiting the available user data on different OSNs contributes to an integrated online user profile and thus improved customized social media services. This talk will introduce a user-centric research paradigm for cross-OSN mining and applications and some pilot works along two basic tasks: (1) From users: cross-OSN association mining and (2) For users: cross-OSN user modeling.

**Biography:** Dr. Xu is a Professor in National Lab of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences and Executive Director of China-Singapore Institute of Digital Media. His research interests include multimedia content analysis/indexing/retrieval, pattern recognition and computer vision. He has hold 30 granted/pending patents and published over 200 refereed research papers in these areas. Dr. Xu is an Associate Editor of IEEE Trans. on Multimedia, ACM Trans. on Multimedia Computing, Communications and Applications and ACM/Springer Multimedia Systems Journal. He received the Best Associate Editor Award of ACM Trans. on Multimedia Computing, Communications and Applications in 2012 and the Best Editorial Member Award of ACM/Springer Multimedia Systems Journal in 2008. He served as Program Chair of ACM Multimedia 2009. He has served as associate editor, guest editor, general chair, program chair, area/track chair, special session organizer, session chair and TPC member for over 20 IEEE and ACM prestigious multimedia journals, conferences and workshops. He is an ACM Distinguished Scientist, IEEE Fellow, and IAPR Fellow.

# INTRODUCTION OF INVITED SPEAKER

11:55-12:20 | Apr. 27, 2025 | Room A <1F>

Room A: 868 1176 6939, <https://us02web.zoom.us/j/86811766939>



## Mathew Nicho

Research and Innovation Centers, Rabdan Academy, UAE & UQ Cyber Research Centre, University of Queensland, Australia

### Dimensionality Reduction for Enhancing Malware Classification Accuracy in Portable Executable Files

**Abstract:** Portable executable (PE) files are a common vector used for the spread of malware. This paper reviews and evaluates machine learning-based PE malware detection techniques. A dataset was created using malicious samples from Virus Share and benign samples from github. Static analysis was used to extract highly ranked features and reduce the dimensions of the dataset using both Linear Discriminant Analysis (LDA) and Principal Component Analysis (PCA). K-Nearest Neighbors and Random Forest classifiers were shown to perform well returning accuracy between  $\approx 93\%$  and  $\approx 94\%$  when used in combination with Linear Discriminant Analysis (LDA).

**Biography:** Dr. Mathew Nicho is an Associate Professor of Cybersecurity at Rabdan Academy, UAE, and an Adjunct Associate Professor at UQ Cyber, School of Electrical Engineering and Computer Science, University of Queensland, Australia. He teaches cybersecurity to defence and law enforcement personnel in the UAE while conducting government-commissioned research. He holds a Master's (2004) and Ph.D. (2009) in IT from Auckland University of Technology (AUT), New Zealand, and has taught at universities in New Zealand, the UK, and the UAE, bringing a global perspective to his academic and research endeavors.

Dr. Nicho's teaching excellence is recognized through the Fellowship of the Higher Education Academy (FHEA, 2016) and four digital learning certifications from Blackboard Academy UK (2020–2021). He was nominated as an 'Exceptional' faculty member in 2018 and received the 'Exceptional Faculty' award in 2019. His research portfolio includes 70+ publications (72% as first author), spanning Q1–Q4 journals and conferences, with continuous research grants since 2014.

His recent industry-academic collaborations include a technical report on cybersecurity in the UAE's financial sector, conducted in partnership with ADGM Academy and the University of Queensland, as well as a collaboration with Abu Dhabi Police on crime prediction. As an industry speaker with multiple media interviews, Dr. Nicho has forged strong and ongoing connections with the IT security industry.

A dedicated academic, Dr. Nicho has supervised numerous Ph.D. and MSc theses, resulting in joint publications. His research interests lie at the intersection of cybersecurity, attacks on national critical infrastructure, machine learning, and situational cybercrime criminology, and digital learning, ensuring a strong alignment between academic theory and industry practice.

# INTRODUCTION OF INVITED SPEAKER

13:30-13:55 | Apr. 27, 2025

Room A: 868 1176 6939, <https://us02web.zoom.us/j/86811766939>



**Yang Liu**

Swansea University, UK

## A Privacy-Preserving Mechanism for Targeted Mobile Advertising

**Abstract:** The prevalent model of the current Internet economy allows consumers to access free services in exchange for targeted advertising. This approach leverages personal data collected from users' devices to deliver tailored advertisements, offering significant benefits to advertisers. However, targeted advertising raises several concerns, with privacy-related issues being particularly prominent. This talk introduces a simple privacy-preserving mechanism designed to address these concerns in Targeted Mobile Advertising while maintaining the current business model. By prioritizing consumers' privacy, the mechanism aims to build trust and enhance advertising outcomes. It also serves as a foundation to inspire innovative solutions for balancing privacy and personalization in mobile advertising.

**Biography:** Dr. Yang Liu received his D.Phil. in Computer Science from University of Oxford in 2018. He is currently a Senior Lecturer in the Department of Computer Science at Swansea University. Before joining Swansea University, he served as an Assistant Professor in Harbin Institute of Technology (Shenzhen) from 2018 to 2024. His research interests focus on data security and privacy-preserving computing. He has expertise in federated learning, blockchain applications, and the design of privacy protection mechanisms. His current work explores the convergence of artificial intelligence and cybersecurity technologies, aiming to enhance the robustness and security of intelligent systems.

# ON-SITE SESSION 1

SUNDAY, APRIL 27, 2025 <13:30~15:15>

<Room A, 1F>

Session Title: Modern Cryptography Theory and Encryption Technology

Chairperson: Dr. Reda Bellafqira, IMT Atlantique, France

<p>13:30-13:45 IP019</p>	<p>The Giant Footprint Is the Smallest: Low-Footprint Decryption of Classic McEliece <b>Cong Liu</b>, Panasonic Corporation, Japan</p> <p>Abstract-Classic McEliece has garnered attention as a candidate in NIST post-quantum cryptography standardization. However, it suffers from high computational demands in its decryption, making it unsuitable for resource-constrained devices. In this paper, we propose a low-footprint implementation method, named Giant Footprint Sharing, that reduces memory size during decryption in Classic McEliece. The decryption algorithm processes a large number of in-memory intermediate variables computed from the secrets. We identify the largest variable among them and implement a memory-sharing structure to store it, thereby reducing the overall memory size. Giant Footprint Sharing can also be combined with high-throughput acceleration techniques, such as fast Fourier transformation. We evaluate Classic McEliece with Giant Footprint Sharing on the Arm Cortex-M33 CPU and show that it reduces memory size by more than half without significant degradation in computation time compared with the existing optimized implementation (Chen et al., TCHES 2021). A detailed examination of the proposed method further reveals that our implementation achieves an optimal balance in the trade-off between memory size and computation time.</p>
<p>13:45~14:00 IP501</p>	<p>Performance Comparison of Machine Learning Algorithms for Forest Fire Detection in Peninsular Malaysia <b>Yee Jian Chew</b>, Multimedia University, Malaysia</p> <p>Abstract-This paper presents a pilot study evaluating 13 machine learning classifiers for detecting forest fires in Peninsular Malaysia using a forest fire inventory dataset generated through the Google Earth Engine (GEE) framework, developed in our previous work. The experimental results demonstrate the suitability of machine learning techniques for forest fire detection in the region. Among the classifiers tested, tree-based models outperformed others, with Random Forest achieving the highest recall of 99.7876%, followed closely by Gradient Boosting with a recall of 99.7345%. These findings suggest that tree-based classifiers are particularly well-suited for forest fire detection tasks. Future work is recommended to focus on refining or enhancing these models to further improve detection performance.</p>
<p>14:00~14:15 IP518</p>	<p>Real-Time Audio-Visual Deepfake Detection Using Multi-Model Pipeline in Video Conference <b>Ananya Jha</b> and <b>Bhoomi Bhat</b>, PES University, India</p> <p>Abstract-Video conferencing has become a cornerstone of communication in professional, educational, and social contexts globally. Due to the emergence of sophisticated real-time deepfake technology being open-source and easily accessible to anyone, the trust in the authenticity of participants during live video calls has diminished. As opposed to offline forensic analysis, detecting deepfakes in real-time is inherently more difficult. In this work, we present an approach to real-time deepfake detection that takes place in the context of video conferencing: a two-step verification process designed to verify user authenticity before the call and through additional continuous on-call monitoring, enabling participants to verify authenticity through optional video and audio detection.</p>

	<p>The framework employs four models, which are active iris pattern analysis, facial hue correlation, ResNeXt-LSTM model, and Mel spectrogram analysis. Complementary strengths of the modules enable reliable detection despite real-world variances, ensuring secure communication. Experiments on custom datasets demonstrate high accuracy under controlled conditions, highlighting challenges in scenarios like dim lighting, complex environments, and noisy audio.</p>
14:15~14:30 IP030	<p>Analysis on Rolling Re-Pseudonymization without Accessing Plaintext Data for Distributed Secure Information Discovery  <b>Hannes Restel</b> and <b>Sascha Peitzsch</b>, Fraunhofer FOKUS, Germany</p> <p>Abstract-In this paper, we explore a novel approach to rolling re-pseudonymization of encoded data records within the context of distributed secure information discovery. Our practical application context is a decentralized Hit/No-Hit system using modified Bloom filter pseudonymization, that we call “ADEP Technology”, which is currently used in the context of information discovery for Member States of the European Union. Frequent rolling re-pseudonymization, i.e. changing pseudonymization parameters and secrets, increases operational security by mitigating the risk associated to frequency attacks. We analyze trade-offs between privacy, linkage quality, and performance of two re-pseudonymization strategies: traditional repseudonymization from plaintext and a novel approach that does not require access to plaintext data. It requires the utilized modified Bloom filters to exhibit sufficiently low False Positive rates, which can be achieved with minor adjustments to the pseudonymization procedure and suitable choice of pseudonymization parameters.</p>
14:30~14:45 IP024	<p>Enhancing Side-Channel Attack Resistance of Post-Quantum Cryptographic Algorithm CRYSTALS-Kyber Using High-Order Chebyshev Filters  <b>Yu-Yi Hong</b>, Feng Chia University, Taiwan</p> <p>Abstract-As quantum computing progresses, traditional public key cryptographic algorithms are increasingly at risk of compromise, making post-quantum cryptography (PQC) critical for maintaining information security. In August 2024, NIST published its first post-quantum key encapsulation mechanism (ML-KEM), which is based on the CRYSTALS-Kyber algorithm with minor adjustments. Kyber, rooted in lattice-based cryptography, offers efficient encryption and decryption with strong resistance to quantum attacks. However, side-channel attacks (SCAs) employing artificial intelligence techniques pose a significant threat, enabling attackers to extract sensitive information through power trace analysis—even in masked Kyber implementations. To counteract this, we propose the approach of incorporating high-order Chebyshev filter to reduce identifiable features in power traces produced during encryption and weaken SCA models’ ability to pinpoint sensitive data. Our results demonstrate that this method reduces the attack success rate from 96% to 61%, providing a substantial defense mechanism for Kyber. This study highlights the potential of high-order Chebyshev filtering as a robust countermeasure against SCA on Kyber, underscoring its importance in strengthening quantumresistant protections.</p>
14:45~15:00 IP025	<p>Cryptography based on 2D Ray Tracing  <b>Sneha Mohanty</b>, University of Freiburg, Germany</p> <p>Abstract-We introduce the first symmetric key cryptographic scheme involving a light ray’s interaction with a 2D cartesian coordinate setup, several smaller boxes within this setup, of either reflection or refraction type and 1st, 2nd or 3rd degree polynomial curves inside each of these smaller boxes. We also incorporate boolean logic gates of types XOR, NOT-Shift and Permutation which get applied to the light ray after each interaction</p>



	<p>with a reflecting or refracting polynomial curve. This alternating interaction between Optical gates (polynomial curves) and Nonoptical gates creates a complex and secure cryptographic system. Furthermore, we design and launch customized attacks on our cryptographic system and discuss the robustness of it against these.</p>
<p>15:00~15:15 IP032</p>	<p>Reducing the e-KYC file searching time in the blockchain system using searchable symmetric encryption and turbulence padded chaotic map  <b>Lalu Raynaldi Pratama Putra</b>, Telkom University, Indonesia</p> <p>Abstract-E-KYC systems often face severe challenges regarding the security and privacy of the related documents stored in the cloud, which becomes a crucial issue. As the volume of data continues to grow, efficient verification becomes increasingly critical. Traditional methods, which require files to be verified individually, are time-consuming and inefficient. The proposed system implements Searchable Symmetric Encryption is used to handle searches from large data sets and maintain the security aspect of seed generation using Turbulence Padded Chaotic Map. Experimental research shows that the time for data searching on large datasets improved significantly while maintaining security.</p>

## ON-SITE SESSION 2

SUNDAY, APRIL 27, 2025 <13:30~15:15>

<Room B, 1F>

Session Title: Network Intrusion Detection and Defense

Chairperson: Assoc. Prof. Mathew Nicho, Research and Innovation Centers, Rabdan Academy, UAE & UQ Cyber Research Centre, University of Queensland, Australia

<p>13:30-13:45 IP023</p>	<p>Integrating Tree Structures with the MITRE ATT&amp;CK Framework for APT Detection <b>Chao-Lung Chou</b>, Department of Information Engineering and Computer Science, Feng Chia University, Taiwan</p> <p>Abstract-Advanced Persistent Threats (APTs) have become a major information security concern for modern organizations. Due to APT attacks' complexity and evolving nature, their Detection mains challenging. This paper proposes an APT pattern tree construction algorithm based on the MITRE ATT&amp;CK techniques and the concept of kill chain model stages. The APT pattern tree is constructed progressively using the different attack techniques identified in real-world databases. The successful construction of these APT pattern trees can examine the attack combinations forming the APT and potentially significantly improve APT detection capabilities, forensic investigations, and early warning systems. The proposed approach effectively helps enhance computer systems' security and reliability.</p>
<p>13:45~14:00 IP031</p>	<p>Optimization of Class Imbalance Techniques in Machine Learning Models for Network Intrusion Detection <b>Adetokunbo Makanju</b>, New York Institute of Technology, Canada</p> <p>Abstract-Machine learning based network intrusion detection has been well developed. The challenge of imbalanced datasets in network intrusion detection has been designed for a while. This paper investigates three class imbalance handling techniques, including random sampling (ROS), synthetic minority sampling technique (SMOTE), and a customized SMOTE approach (Strategy SMOTE) in the UNSW-NB15 dataset. By combining these methods with machine learning algorithms such as Random Forest, XGBoost, LightGBM, and Multi-Layer Perceptron, we demonstrate improvements in model performance, particularly in detecting minority attack classes. Our findings highlight the effectiveness of optimized imbalance handling in improving the reliability of intrusion detection systems.</p>
<p>14:00~14:15 IP543</p>	<p>Minimizing Resource Usage for Real-Time Network Camera Tracking of Black Cows <b>Aung Si Thu Moe</b>, University of Miyazaki, Japan</p> <p>Abstract-Livestock plays a crucial role in the farming industry to meet consumer demand. A livestock monitoring system helps track animal health while reducing labor requirements. Most livestock farms are small, family-owned operations. This study proposes a real-time black cow detection and tracking system using network cameras in memory and disk constrained environments. We employ the Detectron2 Mask R-CNN ResNeXt-101 model for black cow region detection and the ByteTrack algorithm for tracking. ByteTrack tracks multiple objects by associating each detection box. Unlike other deep learning tracking algorithms that use multiple features such as texture, color, shape, and size. ByteTrack effectively reduces tracking ID errors and ID switches. Detecting and tracking black cows in real-time is challenging due to their uniform color and similar sizes. To optimize performance on low-specification machines, we apply ONNX (Open Neural Network Exchange) to the Detectron2 detection model for optimization and quantization. The system processes input images from network</p>

	<p>cameras, enhances color during preprocessing, and detects and tracks black cows efficiently. Our system achieves 95.97% mAP@0.75 detection accuracy and 97.16 % in daytime video and 94.83 % in nighttime accuracy of tracking are effectively tracks individual black cows, minimizing duplicate IDs and improving tracking after missed detections or occlusions. The system is designed to operate on machines with minimal hardware requirements.</p>
14:15~14:30 IP053	<p>Optimizing Real-Time Network Intrusion Detection Using a Refined Data Filtering Method  <b>Adetokunbo Makanju</b>, New York Institute of Technology, Canada</p> <p>Abstract-This paper adopts a proactive cybersecurity approach to address the escalating challenges of the cyber threat landscape and the limitations of conventional security measures. Our work focuses on real-time monitoring and the deployment of cutting-edge machine learning techniques. We introduce a robust monitoring system and refined strategies to enhance model accuracy for effective network intrusion detection. A unique data feeding strategy, grounded in current research and emphasizing anomaly-driven filtering during training, is presented. Models are trained using the BGP anomalous dataset, Slammer, with all data rows labeled prior to training. This highlights our approach to refining data filtering algorithms. Three models are trained using one that employs non-filtered methods, another that utilizes a random selection filter, and the third incorporates a specific filtering algorithm. Testing results demonstrate that the model employing filtering algorithms exhibits the best detection accuracy, confirming the effectiveness of our approach.</p>
14:30~14:45 IP020	<p>Reusable Attack Tree Patterns Using Common Attack Pattern Enumeration and Classification  <b>Masaki Oya</b>, Graduate School of Information Security, Institute of Information Security, Japan</p> <p>Abstract-Attack trees are a threat analysis method that breaks down cyber attack scenarios into individual steps that an attacker can choose. While this generally has the advantage of being able to structurally represent threats to target information systems, it also has cost-related challenges such as requiring a high level of expertise, experience, and sufficient working time for analysis. To address this, we propose a method to generate attack tree patterns from Common Attack Pattern Enumeration and Classification (CAPEC) attack patterns and reuse them to improve the efficiency of attack tree generation. In this study, we (1) developed a method to generate attack tree patterns from CAPEC, (2) verified the effectiveness of the proposed method through a case study targeting web application systems, and (3) developed and evaluated an automatic generation tool for attack tree patterns. The case study demonstrated that patterns could be reused when local subgoals matched, even for scenarios with different final goals across different web application systems. Additionally, the developed automatic generation tool was able to appropriately convert 71% of CAPEC patterns into attack tree patterns. In the first half of this paper, we introduce the proposed method and describe the verification results through case studies. In the latter half, we report on the performance evaluation of the automatic generation tool for attack tree patterns.</p>
14:45~15:00 IP046	<p>Shift-Left Security: Integrating Security in the Initial Phase of the DevOps Methodology  <b>Israel Effiong</b>, Robert Gordon University, UK</p> <p>Abstract-Traditional software development practices often defer security implementation to later stages of the development cycle, leading to delayed vulnerability detection, increased remediation costs, and increased security risks. The emerging “Shift-Left” paradigm addresses these challenges by integrating security considerations early in the development process. This paper proposes a five-step approach to integrating security</p>

	<p>earlier in the DevOps development methodology. It utilises the STRIDE model during the planning phase of DevOps to elicit, specify, and validate security requirements early in the development process. To this effect, the research uses the CAIRIS platform to facilitate comprehensive requirements, security and usability engineering activities during the plan phase of the DevOps methodology. Our approach is validated through a detailed organisational case study of a globally deployed distributed management system that orchestrates stakeholder network operations. Through a comprehensive two-tier approach that combines qualitative interviews and experimental implementation, we systematically identified and analysed the threats and vulnerabilities of the system. Our intervention revealed distinct security threats across all five categories of the STRIDE methodology, each of which were mapped to corresponding mitigation strategies. These findings validate the practical benefits of our methodology in strengthening system security during the initial development phases.</p>
<p>15:00~15:15 IP035</p>	<p>Strengthening LoRaWAN Security Protocol Against Replay Attack Combined With RF Jamming Technique Using Time Differential Privacy <b>Daffa Tsany Rahmantlyo</b>, Telkom University, Indonesia</p> <p>Abstract-As the number of IoT devices surged past 10.7 billion in 2021, ensuring secure communication within resourceconstrained environments remains a formidable challenge. A particularly critical vulnerability in IoT networks using LPWAN technologies, such as LoRaWAN, lies in the Over-the-Air Activation (OTAA) join process. Attackers can exploit this by performing selective radio frequency (RF) jamming to intercept and block initial Join-Request messages from end devices, preventing them from reaching the Network Server. By subsequently replaying a captured Join-Request, adversaries can cause a resynchronization between the end device, the Network Server, and the Join Server, undermining network integrity and security. This study proposes enhancements to the LoRa OTAA join procedure to mitigate these known vulnerabilities. This study proposes a novel enhancement to the LoRa OTAA join procedure using Truncated Laplace Distribution (TLD)-based timestamp perturbation and threshold-based validation. The TLD mechanism adds noise to the timestamps, effectively mitigating replay attacks while maintaining synchronization between network entities. In the numerical experiments, the effectiveness of the proposed mechanism was evaluated under varying conditions of timestamp perturbation and validation thresholds. The results showed that the mechanism effectively prevents LoRaWAN against replayed Join-Requests and reduces the success rate of such attacks to negligible levels while maintaining the execution time.</p>

## ON-SITE SESSION 3

SUNDAY, APRIL 27, 2025 <15:30~17:15>

<Room A, 1F>

Session Title: Data Privacy and Information Authentication

Chairperson: Dr. Yee Jian Chew, Multimedia University, Malaysia

<p>15:30-15:45 IP542</p>	<p>Privacy in Image Transmission <b>Bruno Carpentieri</b>, Università di Salerno, Italy</p> <p>Abstract-Most of the compressed digital images transmitted across today's high-speed networks is intrinsically linked to human actions. It captures our activities, visual experiences, locations, interactions, and virtually every aspect of our daily lives. This raises critical concerns about the need to ensure user privacy and secure digital multimedia content, which is essential for enhancing modern experiences. In this paper we deal with the privacy in image transmission by scrambling ROIs in the image (for example faces of people in the image) or even the whole image, in a reversible way.</p>
<p>15:45~16:00 IP040</p>	<p>A Blockchain-Enhanced Reversible Watermarking Framework for End-to-End Data Traceability in Federated Learning Systems <b>Reda Bellafqira</b>, IMT Atlantique, France</p> <p>Abstract-In federated learning (FL) environments, ensuring data traceability presents significant challenges, particularly when data move between multiple entities such as data centers, edge nodes, and data scientists. This paper presents a novel framework that combines robust reversible watermarking and blockchain technology to achieve end-to-end traceability of medical images in a FL context. Based on the watermark, it becomes possible to interrogate the blockchain about the life cycle of an image to ensure data traceability, authenticity, and integrity. We use a histogram shifting-based reversible watermarking scheme with a new overflow management procedure, integrated with a private blockchain that records all watermarking and verification operations. Experimental results demonstrate the effectiveness of our approach in terms of watermark robustness considering a chest X-ray image dataset. We further show that watermarking does not interfere in the training and inference phase of a VGG-16 classification model for a Covid-19 medical database. A model trained on protected data can be used to classify nonwatermarked data as well.</p>
<p>16:00~16:15 IP540</p>	<p>A Temporal Information-Based Network Model for Vehicle Lane-Change Behavior Recognition <b>Yafei Liu</b>, Southeast University, China</p> <p>Abstract-Accurate recognition of vehicle lane-change behavior is crucial for autonomous driving. Traditional approaches relying on IMU data or visual information are often constrained by inherent sensor errors and environmental obstructions, leading to limited performance. Moreover, the scarcity of publicly available datasets has impeded the development of robust lane-change recognition systems. To address these challenges, this study proposes a low-cost, efficient, and accurate method for vehicle lane-change behavior recognition, applicable to lane-level vehicle localization. A dedicated dataset was meticulously constructed, integrating multiple inputs—acceleration, angular velocity, and lateral distance—to mitigate uncertainty errors from single-sensor data, capturing critical parameters of lane-change behavior. Leveraging the temporal nature of lane-change actions, a hybrid CNN+TCN+BiLSTM network model was developed. The Temporal Convolutional Network (TCN) residual block enhances short- and long-term temporal dependency modeling, while the BiLSTM captures bidirectional sequential patterns, and a</p>

	<p>3D tensor-based attention mechanism extracts key time-step information from the data. The proposed model was rigorously trained and tested on the constructed dataset, achieving a recognition accuracy of 99.5%. Real-world road tests confirmed its robustness in complex urban environments, maintaining reliable performance even under suboptimal visual conditions. This method effectively identifies lane-change behavior with high precision, and the dataset is made publicly available to support further research (<a href="https://github.com/liuyafei666/LaneChangeRecognitionDataset">https://github.com/liuyafei666/LaneChangeRecognitionDataset</a>).</p>
16:15~16:30 IP022	<p>Defending Against Gaussian Process Membership Inference Attack <b>Md Rashedul Islam</b>, University of The Ryukyus, Japan</p> <p>Abstract-Gaussian Process (GP) models, popular for their flexibility and ability to quantify uncertainty, have been increasingly adopted in various machine learning applications, including healthcare, finance, and autonomous systems. However, their use in sensitive areas exposes them to membership inference attacks, in which an adversary aims to determine whether a specific data item was part of the model's training phase. This research examines the susceptibility of GP models to membership inference attacks and suggests effective security strategies for reducing these threats. We first examine the attack vectors and quantify the extent of information leakage in GP models. Our defense framework incorporates differential privacy and data regularization techniques, balancing privacy protection with model performance. Our defense mechanisms greatly reduce the success rate of membership inference attacks on benchmark datasets while maintaining high predictive accuracy. This work highlights the importance of safeguarding GP models against privacy attacks and sets a foundation for future research in secure GP applications.</p>
16:30~16:45 IP026	<p>SRAM PUFs for Device Authentication on Resource-constrained Systems <b>Manuel Penz</b>, Embedded Systems Lab / University of Applied Sciences Upper Austria, Austria</p> <p>Abstract-Physically unclonable functions (PUFs) are a vital component of many state-of-the-art techniques to ensure that software is executable only on a predetermined, unique device and becomes unusable on any other. SRAM PUFs are especially suitable for protecting existing hardware used in productive systems, as almost any microcontroller unit (MCU) already has SRAM onboard. In this paper, we present a novel approach utilizing SRAM PUFs, devised specifically for use on highly resource-constrained devices like MCUs. SRAM-based PUFs exhibit noise due to environmental parameters such as temperature. Therefore we propose a deterministic fuzzy extractor to uniquely identify a device despite the noisy PUF. The memory requirements of our fuzzy extractor rises with noisier data, thus we introduce the concept of stability masks, to preselect the PUF data. Our results show that stability masks significantly improve the reconstruction capabilities of the fuzzy extractor while still functioning with severe memory limitations. We demonstrate our concepts of an automated, scalable multi-stage process implemented in a functional prototype.</p>
16:45~17:00 IP028	<p>Privacy-preserved PQC-based UCSO in Telemedicine Systems <b>Chieh-Jung Yu</b>, Feng Chia University, Taiwan</p> <p>Abstract-People nowadays have high acceptance of healthcare self-monitoring and self-management using smart healthcare devices, and medical professionals can access information immediately to know users' health condition. Telemedicine systems, which have become popular among medical institutes because of COVID-19, is a multi-functional remote medical service and provides long distance medical communication and services. Because of services properties, telemedicine systems have to be established in</p>

	<p>public networks for communication between medical professionals and patients outside, and privacy preservation issues of sensitive and private transmitted information is rising. Moreover, security issues are rising because of rapid development of quantum computing which might endanger systems using current cryptographic mechanisms. User-controlled single sign-on (UCSSO) scheme is one of the means of proving user authentication and secure communication with authenticated session keys, which has ability of resistance to potential cyber-attacks while allowing patients use a single pair of identity and password to access to multiple telemedicine services. In this work, we proposed an approach of privacy-preserved PQCbased UCSSO in telemedicine systems. Proposed remains above merits while achieving privacy preservation and enhancing security properties including resistance of potential attacks from quantum computers.</p>
17:00~17:15 IP039	<p><b>Commitment based Identity-based Homomorphic Signatures for E-document</b> <b>Apurva Kiran Vangujar</b>, University College Cork, Ireland</p> <p>Abstract-Multi-key Homomorphic Signatures (HS) preserve the integrity of data during computations over private inputs from multiple parties. This paper introduces module variants of the Shortest Integer Solution (MSIS)-based Commitment Identity-based Homomorphic Signatures (CIBHS) to address the growing need for secure, efficient, and scalable HS for edocuments. Our proposed CIBHS scheme enables the verification of signatures from multiple identities (A,B,C) without accessing the original data, ensuring homomorphism in keys and messages. This promotes confidentiality and collaboration in e-document environments. The scheme streamlines transaction verification by allowing efficient combined signature validation without revealing individual inputs. The construction of the CIBHS framework is built upon Buvana et al. [1] and includes three phases: Registration, Form Completion, and Verification executed through seven key algorithms: KeyGen, KeyExt, Commit, Sign, Open, Eval, and Verify. These contributions significantly advance signature schemes, providing practical and robust solutions for maintaining data integrity and confidentiality in collaborative e-document workflows.</p>

## ON-SITE SESSION 4

SUNDAY, APRIL 27, 2025 <15:30~17:30>

<Room B, 1F>

Session Title: Computer Vision and Image Processing

Chairperson: Prof. Pyke Tin, University of Miyazaki, Japan

<p>15:30-15:45 IP519-A</p>	<p>From Zero-Shot Generalization to Domain-Specific Optimization in CLIP Models <b>Kazuya Ueki, Meisei University, Japan</b></p> <p>Abstract-Vision-language models have demonstrated remarkable performance across various tasks such as image/video recognition and retrieval. This study explores the optimization of pre-trained vision-language models for improved performance in specific applications, with a focus on video retrieval. Using advanced fine-tuning techniques and integrating domain-specific caption generation, the proposed approach improves the ability of models to retrieve relevant content effectively. The experimental results confirm significant improvements in retrieval accuracy, showcasing the potential of this method for video search and other related domains. These findings highlight the adaptability and scalability of multimodal models for various real-world applications.</p>
<p>15:45~16:00 IP533-A</p>	<p>An Improved Fractional Hessian Framework for Efficient Retinal Blood Vessel Segmentation <b>Priyanka Harjule, Malaviya National Institute of Technology Jaipur, India</b></p> <p>Abstract-This study proposes an improved method for retinal blood vessel segmentation to enhance the diagnosis of diabetes-related complications. The method extracts local shape elements from retinal images using a fractional Hessian matrix, which is modeled as surfaces with ridges and valleys induced by the varying curvature of blood vessels. The proposed method integrates adaptive principal curvature estimation with a new framework leveraging the fractional Hessian matrix with non-singular and non-local kernels. The effectiveness of the suggested method is assessed using publicly accessible datasets, including DRIVE, HRF, STARE, and some real images obtained from a local hospital. The proposed segmentation achieves 95.69% accuracy and 97.86% specificity on the DRIVE database, 95.83% accuracy and 98.73% specificity on STARE, and 95.90% accuracy and 98.36% specificity on the HRF database. Our findings indicate that the suggested method outperforms most listed techniques, including deep learning techniques, and achieves this with significant computational efficiency. The output of the suggested method may be used as input in deep learning techniques, which will be further applied in the clinical application of diabetic retinopathy and glaucoma to discover abnormalities likely related to the progression and different stages.</p>
<p>16:00~16:15 IP513</p>	<p>Smooth Deep Saliency <b>Rudolf Herdt, University of Bremen, Germany</b></p> <p>Abstract-In this work, we investigate methods to reduce the noise in deep saliency maps coming from convolutional downsampling. Those methods make the investigated models more interpretable for gradient-based saliency maps, computed in hidden layers. We evaluate the faithfulness of those methods using insertion and deletion metrics, finding that saliency maps computed in hidden layers perform better compared to both the input layer and GradCAM. We test our approach on different models trained for image classification on ImageNet1K, and models trained for tumor detection on Camelyon16 and in-house real-world digital pathology scans of stained tissue samples. Our results show that the checkerboard noise in the gradient gets reduced, resulting in smoother and therefore easier to interpret saliency maps.</p>



<p>16:15~16:30 IP520</p>	<p>Text-Driven 3D Scene Generation by Panoramic Neural Radiance Fields <b>Tsz-Lok Ng</b>, The Hong Kong Polytechnic University, Hong Kong SAR, China</p> <p>Abstract-While 3D scene generation has been widely applicable to game development, interior design and video editing, recent works target to generate 3D scene from a simple text prompt to further minimize the workload. However, existing approaches are either limited to simple geometries due to their explicit representation or limited to a narrow field of view. In this work, we present a text-driven 3D scene generation method based on a panoramic neural radiance fields framework. Given a text prompt, we first generate a corresponding panorama and predict its depth map. Using the panorama and its depth map, we generate different samples with masked occlusion for panoramic NeRF training, which serves as the 3D scene representation. However, different from a perspective image, a panorama contains high-frequency detail. We propose an additional filtering module to resolve the high-frequency detail. Experiments were conducted to evaluate and benchmark the proposed framework, and the results demonstrate that the proposed framework is effective in generating the 3D scene by text prompt when compared to the other state-of-the-art methods. Additionally, we evaluate the performance of our filtering module and demonstrate the effectiveness of reconstructing the high-frequency details.</p>
<p>16:30~16:45 IP544</p>	<p>Machine Learning-Based Prediction of Cattle Body Condition Score using 3D Point Cloud Surface Features <b>Pyae Phyo Kyaw</b>, University of Miyazaki, Japan</p> <p>Abstract-Body Condition Score (BCS) of dairy cattle is a crucial indicator of their health, productivity, and reproductive performance throughout the production cycle. Recent advancements in computer vision techniques has led to the development of automated BCS prediction systems. This paper proposes a BCS prediction system that leverages 3D point cloud surface features to enhance accuracy and reliability. Depth images are captured from a top-view perspective and processed using a hybrid depth image detection model to extract the cattle's back surface region. The extracted depth data is converted into point cloud data, from which various surface features are analyzed, including normal vectors, curvature, point density, and surface shape characteristics (planarity, linearity, and sphericity). Additionally, Fast Point Feature Histograms (FPFH), triangle mesh area, and convex hull area are extracted and evaluated using three optimized machine learning models: Random Forest (RF), K-Nearest Neighbors (KNN), and Gradient Boosting (GB). Model performance is assessed using different tolerance levels and error metrics, including Mean Absolute Error (MAE) and Mean Absolute Percentage Error (MAPE). Among the models, Random Forest demonstrates the highest performance, achieving accuracy rates of 51.36%, 86.21%, and 97.83% at 0, 0.25, and 0.5 tolerance levels, respectively, with an MAE of 0.161 and MAPE of 5.08%. This approach enhances the precision of BCS estimation, offering a more reliable and automated solution for dairy cattle monitoring and health management.</p>
<p>16:45~17:00 IP530-A</p>	<p>A Point Fractal Network Based Real-time Completion Method for Three-dimensional Intraoral Scanning <b>ZHENG QIANHAN</b> and <b>CHEN JIAHAO</b>, Stomatology Hospital of Zhejiang University School of Medicine, China</p> <p>Abstract-Intraoral scanning (IOS) technology can capture and reflect the surface morphology of teeth in real time, making it a commonly used data acquisition method in clinical dentistry. However, due to the complexity of the oral environment, partial data loss may occur during the scanning process. Therefore, this study develops and evaluates a real-time completion method for incomplete IOS data based on a point fractal network. The proposed method adopts an encoder-decoder architecture. The encoder extracts core geometric features and local details of tooth morphology through a multi-scale</p>

	<p>feature extraction module. The decoder, designed with a fractal structure, progressively refines the point cloud from low to high resolution, ensuring both global consistency and local detail preservation. Additionally, the model incorporates a generative adversarial network for data training, where the generator (decoder) produces the completed point cloud, and the discriminator, based on a PointNet module, distinguishes between real and generated point clouds. The adversarial loss optimization further enhances the realism of the generated data. Experimental results demonstrate that the proposed method performs exceptionally well in restoring missing point cloud regions. The model effectively reconstructs various levels of data loss, maintaining an average Chamfer Distance value consistently below 0.01. Visual comparisons with real point clouds show high consistency in overall shape and size. Furthermore, the model can restore missing regions within approximately 0.5 seconds, enabling real-time completion during scanning. The proposed method significantly enhances the efficiency of digital dental workflows and improves the overall patient experience.</p>
<p>17:00~17:15 IP522</p>	<p>STHAPATI AI - Generating Temple Architecture and Designs <b>Diya Pardhi, Ishwari Magdum, Harshavardhana R Bellad</b> and <b>J Meghana</b>, PES University, India</p> <p>Abstract-This research studies the effective preservation of South Indian temple architecture through the use of RAG models together with Stable diffusion and ControlNet. Through its design function from Agama Shastras principles the system produces faithful architecture representations which respect the cultural heritage. AI achieves automated complex temple design by applying transfer learning alongside edge extraction methods as a solution for labor and financing problems. South Indian temple heritage preservation and cultural architecture applications together with ethical aspects and operational efficiency demonstrate through this study.</p>
<p>17:15~17:30 IP547-A</p>	<p>A Depth Camera-Based Dangerous Action Detection System in Elderly Care Center <b>Remon Nakashima</b>, University of Miyazaki, Japan</p> <p>Abstract-In Japan's aging society, monitoring and early detection of dangerous actions in elderly care facilities is crucial. This paper presents a novel non-contact system that focuses on analyzing residents' body poses relative to predetermined semantic regions within the care environment. The proposed framework first employs a state-of-the-art pose estimation network to extract skeletal Keypoints, particularly focusing on critical joint positions such as the shoulders and hips. Next, a semantic segmentation algorithm is applied to delineate key furniture regions (e.g., beds and chairs) within the facility. A spatial analysis is then performed to determine the degree of overlap between the resident's bounding box and these segmented regions, thus identifying deviations from expected safe postures. A temporal smoothing mechanism, based on a sliding window with majority voting, is incorporated to correct transient misclassifications and stabilize the detection results. The system was validated through experiments conducted in an actual elderly care facility, where various dangerous actions such as abrupt postural changes and unsupervised bed-leaving were simulated. Quantitative analysis of the experimental data demonstrated that the method reliably classifies actions into three distinct risk levels: Safe, Attention, and Danger. This detailed analytical approach provides a solid basis for early detection of hazardous actions by continuously monitoring posture dynamics and spatial relationships, thereby facilitating timely intervention. The results of this study underscore the potential of the proposed method to contribute significantly to the proactive management of safety risks in elderly care settings.</p>

# ONLINE SESSION 1

SUNDAY, APRIL 27, 2025 <13:30~16:10>

Room A:  
<https://us02web.zoom.us/j/86811766939>

Session Title: Information Security and Privacy Protection

Chairperson: Asst. Prof. Tzu-Wei Lin, Feng Chia University, Taiwan

13:30~13:55	<p>Invited Talk II: "A Privacy-Preserving Mechanism for Targeted Mobile Advertising"  <b>Yang Liu</b>, Swansea University, UK</p>
13:55~14:10 IP042	<p>A Blockchain-Integrated IoT System Leveraging Hyperledger Fabric  <b>Yiming Sun</b>, New York Institute of Technology, Canada</p> <p>Abstract-Blockchain technology has been increasingly applied across various fields due to its advantages in distribution and security. Its integration with IoT devices is particularly promising, given their distributed deployment and limited computational capabilities. This paper presents a solution based on the Hyperledger Fabric framework, leveraging the strengths of blockchain while addressing the limitations of traditional blockchain systems, such as the inability to support deletion and modification operations. The proposed approach integrates IoT devices and evaluates the performance of two consensus algorithms, PBFT and RAFT, to highlight their respective efficiencies.</p>
14:10~14:25 IP515	<p>A Smart Machine Learning-Based Training System for Simulating Natural Disasters using 3D Modeling and the Internet of Things  <b>Jay Tsuei</b>, Diamond Bar High School, USA</p> <p>Abstract-The frequency and intensity of natural disasters have been rising globally, leaving a significant portion of the population unprepared to respond effectively in emergencies. This paper presents a novel approach to disaster preparedness through a game-based application that engages users in interactive simulations of natural disasters. Developed using Unity, the game incorporates dynamic mechanics such as fire spread and object fracturing to realistically simulate events like wildfires and earthquakes. Additionally, an environmental monitoring system using Raspberry Pi and DHT11 sensors was introduced to collect real-time temperature and humidity data in fire-prone areas. These data support proactive measures for disaster prevention and education. Ultimately, this project offers an engaging and impactful tool to educate users of all ages on critical survival strategies, promoting preparedness and resilience.</p>
14:25~14:40 IP014	<p>Investigating Sample Selection Methods for Fast and Precise Feature Attribution Explanations in Intrusion Detection  <b>Elyes Manai</b>, Department of Computer Science and Software Engineering, Laval University, Canada</p> <p>Abstract-In cybersecurity, the speed of intrusion detection is critical for effective defense. This paper investigates efficient sampling strategies to accelerate the feature attribution generation process in tabular datasets, which is the common format of intrusion detection. Traditional feature attribution methods, while valuable for understanding model behavior, often suffer from high computational complexity, making them impractical for real-time cybersecurity applications. In this study, we evaluate various sampling strategies to assess their ability to maintain the fidelity of feature attributions while significantly reducing the computation time required. Our findings reveal that Latin Hypercube Sampling (LHS) and its improved versions offer a compelling balance between speed and accuracy, achieving nearly identical performance using only 0.1% of the full training set. These results underscore the potential of optimized sampling methods in</p>

	enhancing the responsiveness of cybersecurity systems, paving the way for faster, more accurate intrusion detection mechanisms.
14:40~14:55 IP016	<p>Leveraging Open Source Intelligence (OSINT) for Cryptocurrency Crime Investigation: Tools and Techniques  <b>Byung Wan Suh</b>, Fairsquarelab., Co., Ltd., South Korea</p> <p>Abstract-This research explores the application of Open Source INTelligence (OSINT) techniques for investigating cryptocurrency-related crimes, a rapidly growing area with unique challenges for traditional law enforcement methods. Given the decentralized and pseudonymous nature of cryptocurrencies, this study proposes a framework leveraging publicly available online data to enhance investigative capabilities. The research first reviews the burgeoning cryptocurrency market, the prevalent types of associated crimes, and the definition and classification of OSINT, highlighting its increasing importance in various investigative domains. The core research focuses on utilizing OSINT tools and techniques, specifically blockchain explorers and cryptocurrency analysis platforms, integrated within a four-stage cybercrime investigation process. The study also demonstrates how these tools can be strategically applied at each stage, illustrating their effectiveness in tracking cryptocurrency transactions, identifying suspicious patterns, and tracing the flow of funds. The research concludes that OSINT significantly enhances the investigation of cryptocurrency crimes by providing a systematic approach to analyzing publicly available data within the established cybercrime investigation framework and discusses further research areas.</p>
14:55~15:10 IP021	<p>CSSM: A combined structure of SM4-like structure and MARS-like structure  <b>Zhengyi Dai</b>, National University of Defense Technology, China</p> <p>Abstract-SM4-like structure and MARS-like structure are generalized Feistel structures with the property that the decryption is similar to the encryption. These two structures are the same up to affine equivalence. In this paper, we propose a new generalized Feistel structure, CSSM, which combines the design philosophies of both SM4-like and MARS-like structures. We further investigate the refined full-diffusion round and analyze the number of rounds of impossible differentials, zero correlation linear hulls, and integral distinguishers for d-branch CSSM with bijective f-functions. If <math>d/2</math> is an odd number, then the refined full-diffusion round of CSSM is at least <math>d</math>, and there exist <math>3d/2</math>- round impossible differentials, <math>3d/2</math>-round zero correlation linear hulls, and <math>3d/2</math>-round integral distinguishers. If <math>d/2</math> is an even number, then the refined full-diffusion round of CSSM is at least <math>d - 1</math>, and there exist <math>(3d/2 - 1)</math>-round impossible differentials, <math>(3d/2 - 1)</math>-round zero correlation linear hulls, and <math>(3d/2 - 1)</math>-round integral distinguishers. The structure proposed in this paper may contribute to the design of block ciphers.</p>
15:10~15:25 IP048	<p>Further Attacks on the Micali-Schnorr Pseudorandom Generator  <b>Liam Heng</b>, University of New South Wales, Australia</p> <p>Abstract-The Micali-Schnorr pseudorandom generator has been in use since its inception in 1990. However, serious concerns about the possibility of a backdoor have been raised since its security is not tightly coupled to the RSA problem. Our work begins by extending the state of the art in small state attacks by uncovering a new range of vulnerable parameter choices. We provide an implementation which proves its practical as well as theoretical viability. We then demonstrate the existence of vulnerable exponents and implement an algorithm for their generation from any moduli. Lastly, we build upon this to develop and implement a framework to use only an exponents public moduli to detect if it has been maliciously constructed to contain a backdoor.</p>

<p>15:25~15:40 IP045</p>	<p>Research on Integrity Measurement of Trusted Access for Cloud Manufacturing Equipment Terminals <b>Wenbo WEI</b>, Taiyuan University of Science and Technology, China</p> <p>Abstract-To address the issues of security in cloud servers and unauthorized device access resulting from illegal access to cloud manufacturing equipment resources, a trusted computing-based integrity measurement scheme for secure access to cloud manufacturing equipment resource terminal trusted access is proposed. This scheme consists of two parts. Firstly, the trust root is constructed by introducing the TPM(Trusted Platform Module), and the integrity measurement of the device resource terminal is carried out using the SM2-based uncertified interceptable signature algorithm. The trust state is transmitted layer by layer to the entire device resource terminal in a trust chain manner, completing the establishment of its internal trusted environment and integrity measurement; Secondly, by calling the SM2-based uncertified interceptable signature algorithm in TPM through the interface, a public-private key AIK (Attestation Identity Key) is generated. Based on the integrity verification strategy of publicprivate key cooperation, the device resource terminal can be trusted to access the cloud service. Finally, the effectiveness of the proposed method was verified through experiments.</p>
<p>15:40~15:55 IP017</p>	<p>Edge-based Machine Learning Models in IoT Devices for improved Anomaly and Intrusion Detection <b>Theodore Kindong</b>, Linköping University, Sweden</p> <p>Abstract-The rapid proliferation of IoT devices has increased security and privacy vulnerabilities due to device resource restrictions and a lack of edge intelligence. To better understand how Supervised Machine Learning (ML) may be used at edge devices, this study examined how industry actors can use ML to improve IoT edge security. Despite the interest in ML for intrusion detection in IoT, edge device security is in demand as IoT devices spread. The current technique is computationally costly, and resource-limited IoT devices struggle to run ML algorithms. Using a mixed-method approach, this study uses EuX testbed and UNSW-NB 15 network datasets to train, assess, and finetune ML models for edge deployment. The study’ s findings present the model's performance, best features, compute time, and resource needs from an exploratory examination of the data sets. This study concludes that ML models can improve IoT real-time anomaly and intrusion detection by boosting edge device intelligence. However, ML deployments also require algorithm optimization and computational reduction.</p>
<p>15:55~16:10 IP038</p>	<p>Towards Systemic IT Security. Introducing a holistic conceptual framework for a societal perspective on IT and cyber security <b>Rainer Rehak</b>, Weizenbaum Institute for the Networked Society, Germany</p> <p>Abstract-Digital systems are everywhere and we rely so much on those ubiquitous systems that “the digital” could be called a hyper-infrastructure, but given the ongoing grave IT security incidents a defective one. To approach this problem I suggest a new paradigm called systemic IT security extending traditional understandings. I first map out the academic consensus that the current state of IT security is not sufficient given the roles IT plays in digitally networked societies. I then explicate the societal consequences of IT insecurity. Using two major real-world incidents, the Mirai botnet and the WannaCry ransomware, I then flesh out how the current individual and organisational paradigm of IT security theory can not sufficiently grasp this increasingly interconnected issue. For furthering the fruitful academic discourse, I propose the holistic concept of systemic IT security. With it I define a criteria framework for extending current IT security approaches with the seven dimensions: problem scope, relation of control and</p>

responsibility, sustainability, impact, pro-re-activeness, fairness, and absence of complications. This framework can be used to extend IT security theory, assess concrete IT security measures in a structured manner, and even to analyse policies regarding their contribution to systemic IT security. Together with the framework I propose a new IT security protection goal of intention and expectation alignment and two new actor categories for threat modelling: systems manufacturers and service operators. Finally, the contextualized societal merits of the new perspective are explicated and the argument summarized.

## ONLINE SESSION 2

SUNDAY, APRIL 27, 2025 <16:30~19:15>

Room A:  
<https://us02web.zoom.us/j/86811766939>

Session Title: Image Analysis and Information Security Management

Chairperson: Dr. Yufeng Li, The University of Southampton, UK

<p>16:30~16:45 IP047</p>	<p>Interrupt Trace Fusion for Enhanced Website Fingerprinting Attacks under Defensive Mechanisms  <b>Yefeng Lv</b>, Shanghai Maritime University, China</p> <p>Abstract-Machine learning has significantly enhanced the effectiveness of website fingerprinting attacks, increasing the success rate of privacy leakage to 93.7%. Website fingerprinting attacks analyze various side-channel signals to deduce the specific websites a user visits, thus posing a threat to user privacy. In response to this threat, advanced defense mechanisms have been developed, such as randomized timers. These defenses alter the pattern of interrupt events, reducing the success rate of interrupt-based side-channel attacks to 1.8%, thereby significantly disrupting attackers' ability to accurately infer information. To counter these effective defenses, we propose an interrupt trace fusion-based attack model. By combining interrupt traces from multiple attack sources, this model captures a more comprehensive set of interrupt features, thereby improving both the accuracy and stability of the attacks. Compared to single-source methods, this fusion model can still effectively extract useful information under strong defensive measures, enhancing overall attack performance. Experimental results show that this model raises the attack success rate from 93.7% to 94.9% under no defense. Under robust defenses, its accuracy increases from 1.8% to 45.3%.</p>
<p>16:45~17:00 IP502</p>	<p>Jumping Beyond Limits: A Comprehensive Dataset for Long Jump Analysis  <b>Tarunya Prasad</b>, PES University, India</p> <p>Abstract-In today's technology-driven world, data serves as the foundation for innovation across industries, including sports. Sports analytics isn't just for the elite anymore; it's time to put data in every athlete's hands. Professional coaches can easily identify visual flaws in an athlete's performance, but they cannot quantify and provide numerical values to support it. Our work addresses this gap by providing a novel dataset of long jump athletes along with their extracted metrics to follow a data-driven approach for coaches and athletes to better themselves. The entire dataset is public and developed using a phone camera to ensure wide-range accessibility. The numerical data captured from the long jump videos including stride lengths, take-off angle, and effective jump distances, are extracted using computer vision techniques. These quantifiable metrics serve as benchmarks to the athlete and help track progression, identify weak areas, and change workout plans accordingly. This study leverages computer vision technologies to create a novel dataset that quantifies long jump biomechanics for performance optimization.</p>
<p>17:00~17:15 IP505</p>	<p>Analysis of Shoreline Changes Using CCTV Imagery  <b>Hsing-Yu Wang</b>, Department of Shipping Technology, National Kaohsiung University of Science and Technology, Taiwan</p> <p>Abstract-This study utilizes Closed-Circuit Television (CCTV) images to monitor shoreline changes, addressing the challenges of traditional coastal monitoring methods, such as high costs, labor-intensive processes, and weather dependence. The proposed methodology includes camera calibration, ground control point measurements, and</p>

	<p>applying a U-Net convolutional neural network for automated shoreline extraction from images. The U-Net model achieves high accuracy by integrating manual labeling and data augmentation techniques, with an average relative error of 2.05% during validation. Compared to traditional field surveys and satellite remote sensing, the CCTV-based approach demonstrates significant advantages in cost efficiency and long-term monitoring capabilities. This study contributes to the advancement of shoreline monitoring technologies by presenting an effective, scalable, and low-cost solution that aligns with the global need for sustainable coastal management.</p>
<p>17:15~17:30 IP516</p>	<p><b>ChromAdapt: A Dual-Clustering Framework for Personalized Enhancement of CVD Images</b> <b>Neeharika Anand</b>, PES University, India</p> <p>Abstract-Color Vision Deficiency (CVD) affects millions worldwide, impacting their ability to perceive color distinctions essential for visual media comprehension. Existing solutions tend to utilise generalized recoloring strategies, which often neglect individual differences in CVD type and severity. Furthermore, they are typically tailored to simple visual inputs, reducing their effectiveness when applied to the complexity and diversity of real-world imagery.</p> <p>We present ChromAdapt, a novel framework for personalized enhancement of images for individuals with CVD. Our approach introduces two key innovations: a dual-clustering architecture that combines superpixel clustering and object-level segmentation, and a severity-aware loss function that dynamically adapts to the type and extent of CVD. This enables targeted recoloring that enhances visual clarity for affected users without compromising the naturalness or semantic integrity of the image. ChromAdapt advances the field of adaptive image enhancement by delivering computational efficiency and personalization, making it practical for real-world applications.</p>
<p>17:30~17:45 IP052</p>	<p><b>Evaluating Boundary Restriction Methods Against Hardware Transient Faults on Website Fingerprinting Attacks</b> <b>Chaoyue Ren</b>, Shanghai Maritime University, China</p> <p>Abstract-Boundary restriction methods are increasingly used to mitigate the impacts of transient hardware faults due to their low overhead and ease of use. Besides the typical safetycritical applications such as self-driving and health-care, the machine learning-assisted website fingerprinting (WF) attacks, which aim to infer sensitive user activities from encrypted traffic patterns, require high computational reliability. However, transient hardware faults (e.g., bit-flips) may degrade attack accuracy by distorting feature extraction. Therefore, this paper aims to enhance the robustness of website fingerprinting (WF) attack models against hardware transient faults by evaluating boundary restriction methods. Three boundary restriction methods including layer-level clipping, neuron-level smooth restrictions, and hybrid strategies are selected for mitigating fault propagation in the WF learning models. The evaluation of fault containment efficacy is through hardware-calibrated fault injection across convolutional (Conv), activation, and fully-connected (FC) layers. The experiments on interrupt-driven datasets reveal that layerlevel approaches maintain inference accuracy yet show limited fault resilience. Neuron-level methods reduce fault propagation but degrade feature extraction, with accuracy drops of 2.78% in fault-free scenarios and nonlinear performance decay under increasing Bit Error Rates (BERs). Hybrid strategies balance these tradeoffs by selectively integrating layer-level and neuronlevel restrictions, achieving 35.3% accuracy under BER equal to <math>3 \times 10^{-6}</math> while maintaining moderate fault-free accuracy (0.32% drop). The comprehensive results analysis provides design principles for integrating boundary restrictions into reliable WF attacks while harmonizing hardware reliability and algorithmic precision.</p>



<p>17:45~18:00 IP517</p>	<p>Spatio-Temporal Transformers and Semantic Insights: Redefining Video Anomaly Detection <b>Amara Sai Prasad</b>, PES University, India</p> <p>Abstract-Traditional video surveillance systems often rely on manual monitoring, resulting in labor-intensive processes that are prone to errors, particularly in detecting complex events that hinder public safety and security. This study addresses these limitations by integrating advanced deep learning models for comprehensive video and text feature extraction, leveraging the power of multi-modal fusion. We employ TimeSformer to capture intricate spatio-temporal patterns within video data and RoBERTa to extract semantic insights from accompanying text captions. Our approach utilizes three multi-modal fusion techniques: Concatenation Fusion, Gated Fusion, and Compact Bilinear Pooling. These methods effectively combine visual and textual representations to enhance anomaly detection capabilities. Experimental results reveal that Concatenation Fusion significantly outperforms the other methods, achieving an accuracy of 85.19% in complex video scenarios. This fusion-based approach not only improves detection accuracy but also reduces the reliance on continuous human oversight, making it a practical solution for applications in public safety and security.</p>
<p>18:00~18:15 IP034</p>	<p>Optimizing Hybrid Cryptographic Frameworks for Secure Financial Data Transmission in Resource-Constrained Environments <b>Paul Kobina Arhin Jnr</b>, University of Cape Coast, Ghana</p> <p>Abstract-This paper proposes a novel hybrid cryptographic algorithm that combines the ElGamal cryptographic algorithm and ChaCha20-Poly1305 authenticated symmetric encryption to address the dual requirements of security and performance in financial transactions in Africa. The proposed hybrid encryption algorithm seeks to provide a safe, efficient and flexible approach to protect financial transactions in Africa and beyond, by combining the security and strength of both algorithms. ElGamal is dependent on Discrete Logarithm Problem (DLP). DLP is a hard computational problem in cryptography making it computationally hard to solve with modern technology and algorithms. This makes it highly secured. The complexity of the algorithm has resulted in slower encryption and decryption process. ChaCha20-Poly1305, a modern high speed symmetric encryption algorithm, is well known for its fast performance in resource constrained environments and authenticated encryption features. It is less computationally intensive which is effective for devices and environment with limited resource capabilities. By combining these two algorithms, the hybrid system provides a secure and efficient solution tailored to the transactional needs of African financial institutions where there is widespread use of less powerful device like mobile phones. The proposed system leverages ElGamal for secure key exchange and ChaCha20-Poly1305 for fast, authenticated encryption of transactional data. This combination addresses critical security challenges, including confidentiality, integrity, and authentication, while optimizing performance for resource-constrained environments.</p>
<p>18:15~18:30 IP054</p>	<p>Cryptanalysis of an effective certificateless aggregate signcryption scheme <b>Surmila Thokchom</b>, National Institute of Technology Meghalaya, India</p> <p>Abstract-For V2G communication, Wang et al. Proposed an effective and reliable certificateless aggregate signcryption scheme to preserve the confidentiality, integrity, and authenticity of the shared data. They demonstrated that their scheme achieves unforgeability. However, we have proven that their scheme can be compromised by an A1 adversary. We present a detailed examination of these vulnerabilities and propose an improved scheme that resolves them. Through a performance evaluation, we demonstrate that our proposed scheme offers superior computational and communication</p>

	<p>efficiency compared to related approaches.</p>
<p>18:30~18:45 IP5002</p>	<p>WTUNet: Minimize Your U-Net Through Wavelet Transformation for Lung Nodules Segmentation <b>Gina Jinna CHEN</b>, Southern University of Science and Technology, China</p> <p>Abstract-Medical image processing remains a crucial and challenging task due to two main factors: Dramatic computational cost and unique structured characteristics. Conventional CNNs may not fully exploit low-frequency characteristics, and their receptive field is limited due to their local aggregation calculation. Wavelet transformation inherently excels at capturing directional frequency information due to its spatial localization properties, which enable it to focus on changes in image gradients. Therefore, we propose the Wavelet Transformation-based UNet, which first reconstructs the whole U-shape Network through Wavelet Transformation. Taking pulmonary nodules segmentation as a case study, we employ the wavelet-based down-sampling method and reconstruct the up-sampling process using inverse wavelet transformations instead of adopting big kernels to expand the receptive field while minimizing the learnable parameters. Experimental results demonstrate that WTUNet outperforms models of equivalent depth. In contrast, its model size is approximately one-twenty-fifth of that of comparable networks, exhibiting its superior segmentation performance and impressive reduced computational demands, underscoring its potential advantages for medical image segmentation tasks.</p>
<p>18:45~19:00 IP5003</p>	<p>MSADNet: Enhancing Bronchial Segmentation via Multi-Scale Features and Attention Distillation <b>Gina Jinna CHEN</b>, Southern University of Science and Technology, China</p> <p>Abstract-Many bronchial segmentation algorithms based on encoding and decoding structures have recently been proposed. Still, the effect of the feature loss problem on the final segmentation effect during feature extraction performed on bronchial branches has not been considered. In this study, we propose a multi-scale feature extraction network with an attention distillation mechanism (MSADNet) for bronchial segmentation by investigating how to better capture the features of bronchial branches with different morphologies during the encoding process. In detail, in this paper, we design a novel multi-scale feature extraction module (MSF) in the encoding process so that the encoder can fully extract features of various branch sizes and reduce the loss of key features in feature extraction for bronchial branching modules. During the decoding process, attention distillation (AD) is applied to the attention maps of different resolutions to preserve the key features in the encoding stage, thus improving the segmentation accuracy. With MSF and attention distillation, MSADNet is more capable of concentrating on the intricate branching structure of the bronchial airway tree and is more adaptable to the segmentation of the complex airway tree structure. Our method shows excellent segmentation results on both ATM2022 datasets compared with the baseline.</p>
<p>19:00~19:15 IP701</p>	<p>Electromagnetic Side-Channel Analysis of PRESENT Lightweight Cipher <b>Nilupulee Gunathilake</b>, Edinburgh Napier University, UK</p> <p>Abstract-Side-channel vulnerabilities pose an increasing threat to cryptographically protected devices. Consequently, it is crucial to observe information leakages through physical parameters such as power consumption and electromagnetic (EM) radiation to reduce susceptibility during interactions with cryptographic functions. EM side-channel attacks are becoming more prevalent. PRESENT is a promising lightweight cryptographic algorithm expected to be incorporated into Internet-of-Things (IoT) devices in the future. This research investigates the EM side-channel robustness of PRESENT using a correlation attack model. This work extends our previous Correlation EM Analysis (CEMA)</p>

of PRESENT with improved results. The attack targets the Substitution box (S-box) and can retrieve 8 bytes of the 10-byte encryption key with a minimum of 256 EM waveforms. This paper presents the process of EM attack modelling, encompassing both simple and correlation attacks, followed by a critical analysis.

## LIST OF DELEGATE

Naoto Yanai, Panasonic Holdings Corporation, Japan
Akira Maruko, Panasonic Corporation, Japan
Chung-Wei Kuo, Feng Chia University, Taiwan
Jia-Ning Luo, National Defense University, Taiwan
Wen-Tsung Tsai, Chung Cheng Institute of Technology, NDU, Taiwan
Taeyoung Kim, Samsung Medical Center, South Korea
Thi Thi Zin, University of Miyazaki, Japan
Pyke Tin, University of Miyazaki, Japan
ZHANG WEIFANG, Stomatology Hospital of Zhejiang University School of Medicine, China

# ONE DAY TOUR

MONDAY, APRIL 28, 2025

08:00 Meet up at <University of the Ryukyus>

Travel route:

万座毛 Cape Manzamo

古宇利島 Kouri Island

縄美ら海水族館 Okinawa Churaumi Aquarium

アメリカンビレッジ American Village

*\*Return around 6:30pm; Lunch and ticket are included in registration fee*

*\*Registration closes at 5pm, April 15, 2025 (JST), with a registration fee of 150 USD.*

*\*The itinerary may change depending on the number of participants and weather conditions.*



# NOTE

A series of horizontal dashed lines for writing notes.







