CONFERENCE PROGRAM

CSP 2022

The 6th International Conference on CRYPTOGRAPHY, SECURITY AND PRIVACY

Virtual Conferenece	January 14-16, 2022

Beijing Time (**GMT +8:00**)

Sponsored by

天津職業技術師範大學
TIANJIN UNIVERSITY OF TECHNOLOGY AND EDUCATION

Hosted by

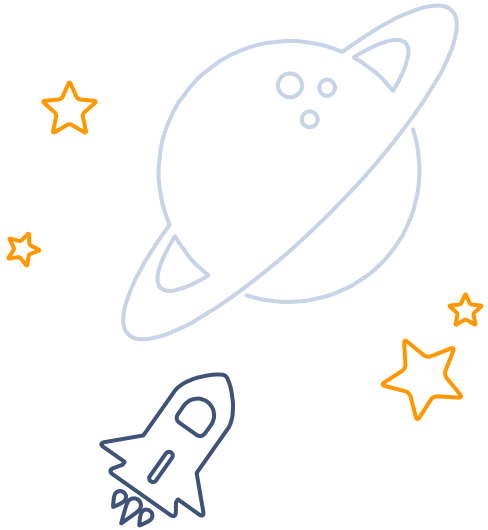
Supported by

ECU
COSIC 中国航天
UNIVERSITY OF LIMERICK OLLSCOIL LUIMNIGH
UNIVERSIDADE DE ÉVORA CIDEHUS

Published by

IEEE COMPUTER SOCIETY CONFERENCE PUBLISHING SERVICES

TABLE OF CONTENT



#CONFERENCE MATERIALS

- Zoom Guidance (click) *For new users.*
- Virtual Background.jpg (click)
- Electronic Banner.jpg (click)

1 WELCOME MESSAGE

Dear colleagues and friends,

On behalf of the conference organizing committees, we are delighted to welcome you to the virtual conference of the 6th International Conference on Cryptography, Security and Privacy (CSP 2022), to be held from January 14-16, 2022.

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 3 oral sessions, and 4 keynote speeches delivered respectively by ***Prof. Shahram Latifi*** (FIEEE, University of Nevada), ***Prof. Changsheng Xu*** (FIEEE, Chinese Academy of Sciences), ***Prof. Hiroyuki Kudo*** (University of Tsukuba), & ***Prof. Zheli Liu*** (Nankai University). We would like to express our gratitude to all the speakers in this conference. Special thanks to all of our committee members, all the reviewers, and the attendees for your active participation. We hope the conferences will be proved to be intellectually stimulating to us all.

Finally, we wish you a very successful conference!

Yours Sincerely,

Conference Organizing Committee-CSP 2022

2 MEETING AGENDA

Essential Information

Please make sure you are aware of the following details before the conference.

Time Zone

GMT +8:00
Beijing Time
Please be aware of time difference between this and your region/country.

Name Setting

Keynote Speaker: Keynote-Name
Committee: Position-Name
Author: Paper ID-Name
Listener: Listener-Name

Test Session

Check details of the testing time on **Friday, Jan 14**, and please make sure to show up on time.

Meeting ID

Room A: 986 1799 7698
https://zoom.us/j/98617997698
Room B: 973 4517 2118
https://zoom.us/j/97345172118
Room will be open 30 mins in advance.

2 MEETING AGENDA

Room B: 973 4517 2118
Meeting Link: https://zoom.us/j/97345172118

Friday
14.01.2022.

Zoom Test Sessions

13:00-14:00	14:00-15:00	15:00-16:00	16:00-17:00
CS001	CS019	CS034	**[Waiting Time]** for all participants who are unavailable at allocated time.
CS002	CS020	CS035	
CS004	CS021	CS036	
CS005	CS023	CS037	
CS007	CS024	CS038	
CS009	CS025	CS039	
CS011	CS030	CS1001	
CS012	CS031		
CS013	CS032		
CS014	CS033		

Pre-test for Formal Session

- We will test screen sharing, audio, video, and how to "Raise Hand" in Zoom. Please get your presentation slides and computer equipment prepared beforehand.
- All the presenters are required to join the Zoom test sessions on Jan. 14, to ensure the meeting next day run smoothly.
- It may only take you 3min to complete the test session, then free to leave.

- Please note that times provided in the program are according to Beijing Time (GMT +8:00).

2 MEETING AGENDA

Room A: 986 1799 7698
Meeting Link: https://zoom.us/j/98617997698

Saturday
15.01.2022.

TIME	ACTIVITY	PRESENTER
Host: *Local Organizing Chair* - **Prof. Genghuang Yang** (Tianjin University of Technology and Education)		
09:00-09:10	**Opening Remarks**	*Conference Chair* - **Prof. Bing Yan** Tianjin University of Technology and Education
09:10-09:55	**Keynote Speech I** "Past, Present and Future of Facial Recognition"	**Prof. Shahram Latifi** Fellow of IEEE, Professor, University of Nevada
09:55-10:40	**Keynote Speech II** "Connecting Isolated Social Multimedia Big Data"	**Prof. Changsheng Xu** Fellow of IEEE & IAPR, Chinese Academy of Sciences
10:40-11:00	**Group Photo / Break Time**	
11:00-11:45	**Keynote Speech III** "Deep Learning in Tomographic Image Reconstruction"	**Prof. Hiroyuki Kudo** University of Tsukuba
11:45-12:30	**Keynote Speech IV** "Oblivious Random Access Machine and its Applications"	**Prof. Zheli Liu** Nankai University
12:30-13:30	**Break Time**	

- Please note that times provided in the program are according to Beijing Time (GMT +8:00).
- Each keynote talk includes a 5-minute Q&A session.

2 MEETING AGENDA

Room B: 973 4517 2118
Meeting Link: https://zoom.us/j/97345172118

Saturday 15.01.2022.

TIME	ACTIVITY	PRESENTER
13:30-16:00	**Session 1: Information Privacy and Data Security**	CS035 CS031 CS025 CS038 CS007 CS012 CS023 CS032 CS009 CS1001
16:00-16:05		Session Group Photo

Sunday 16.01.2022.

TIME	ACTIVITY	PRESENTER
09:30-11:45	**Session 2: Cyber Attacks and Security**	CS033 CS024 CS019 CS013 CS020 CS004 CS011 CS002 CS014
11:45-13:00		Session Group Photo / Break Time
13:00-15:00	**Session 3: Information Network and Information Management**	CS037 CS030 CS034 CS036 CS001 CS039 CS021 CS005

- Please note that times provided in the program are according to Beijing Time (GMT +8:00).
- Each oral presentation includes a 3-minute Q&A session.
- Session Group Photo: a picture captured at the end of each session.

3 KEYNOTE SPEAKER I

Room A: 986 1799 7698
Meeting Link: https://zoom.us/j/98617997698

Saturday
15.01.2022.

Prof. Shahram Latifi
Fellow of IEEE
University of Nevada

09:10-09:55

"Past, Present and Future of Facial Recognition"

Abstract: In recent years, there has been much progress in the area of Facial Recognition (FR) that address the shortcomings in conventional FR systems. Spoofing using a high resolution image, high false negative rates due to partial occlusion of the face (ex. mask), and high positive rates due to similarity of subjects are among such shortcomings. Aided by advancements in AI and image acquisition technology (i.e. high resolution 2D/3D) cameras, researchers have been able to push the quality of the facial recognition systems to an impressive new level. Despite the progress, there are still challenging issues lingering around ranging from technology matters (ex. real-time standoff detection) to policy concerns (ex. privacy and ethics). In this talk, I will address the progress in facial recognition and present the state of the art technologies developed by the world software giants such as Google, Facebook, Microsoft and Baidu in FR. Amid the growing concerns about misuse of FR by governments and other public entities, companies have started to move away from broad identification toward more restrictive forms of personal identification. At the end, I will focus on the trade-offs of restrictive FR and the need for including control, privacy and transparency in future systems.

Bio: Shahram Latifi, an IEEE Fellow, received the Master of Science Degree in Electrical Engineering from Fanni, Teheran University, Iran in 1980. He received the Master of Science and the PhD degrees both in Electrical and Computer Engineering from Louisiana State University, Baton Rouge, in 1986 and 1989, respectively. He is currently a Professor of Electrical Engineering at the University of Nevada, Las Vegas. Dr. Latifi is the director of the Center for Information and Communication Technology (CICT) at UNLV. He has designed and taught graduate courses on Bio-Surveillance, Image Processing, Computer Networks, Fault Tolerant Computing, and Data Compression in the past twenty years. He has given seminars on the aforementioned topics all over the world. He has authored over 200 technical articles in the areas of image processing, biosurveillance, biometrics, document analysis, computer networks, fault tolerant computing, parallel processing, and data compression. His research has been funded by NSF, NASA, DOE, Boeing, Lockheed and Cray Inc. Dr. Latifi was an Associate Editor of the IEEE Transactions on Computers (1999-2006) and Co-founder and General Chair of the IEEE Int'l Conf. on Information Technology. He is also a Registered Professional Engineer in the State of Nevada.

3 KEYNOTE SPEAKER II

Room A: 986 1799 7698
Meeting Link: https://zoom.us/j/98617997698

Saturday
15.01.2022.

Prof. Changsheng Xu
Fellow of IEEE & IAPR

Institute of Automation,
Chinese Academy of Sciences

09:55-10:40

"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.

Bio: Changsheng Xu, is a distinguished professor of Institute of Automation, Chinese Academy of Sciences. His research interests include multimedia content analysis/indexing/retrieval, pattern recognition and computer vision. He has hold 50 granted/pending patents and published over 300 refereed research papers including 100+ IEEE/ACM Trans. papers in these areas. Prof. Xu is Editor-in-Chief of Multimedia Systems. He serves/served Associate Editor of IEEE Trans. on Multimedia and ACM Trans. on Multimedia Computing, Communications and Applications. He received the Best Paper Awards of ACM Multimedia 2016 and 2016 ACM Trans. on Multimedia Computing, Communications and Applications. 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.

3 KEYNOTE SPEAKER III

Room A: 986 1799 7698
Meeting Link: https://zoom.us/j/98617997698

Saturday
15.01.2022.

Prof. Hiroyuki Kudo

University of Tsukuba

11:00-11:45

"Deep Learning in Tomographic Image Reconstruction"

Abstract: Image reconstruction in CT, MRI, and PET has been performed by using a class of analytical reconstruction methods such as Filtered BackProjection (FBP) for a very long time up to 2000. In this talk, we will introduce our two example studies on the DL reconstruction as well as explaining its principles for unfamiliar audience. Our first study concerns reconstructing higher-quality images from sparse-view or low-dose CT projection data. The explanation is constructed as follows. First, we explain the standard approach to use DL for the CT reconstruction. Next, we explain our original approach (called CSDL-net) which combines DL and CS in a successful way to achieve much higher image quality compared to the case where CS or DL is used alone. We show typical examples which demonstrate that CSDL-net achieves a dramatic improvement on image quality. Our second study concerns how to use DL to image reconstruction in PET/SPECT. We have developed a DL-based method which corrects the degradations. The proposed method inputs a PET/SPECT degraded image reconstructed by FBP method with (or without) a CT/MRI image corresponding to the same transaxial slice into U-Net. As an output of network, an improved image with correction is obtained. We show typical examples which demonstrate that the proposed method with the PET/S`PECT plus CT/MRI input works well. In the final part of this talk, we will explain our opinion about what is the main advantage of the DL approach, what problems exist in the DL approach at the current stage, and our expectation on the future direction.

Bio: In March 1990. Hiroyuki Kudo received his doctoral degree in electrical and communication engineering from the Tohoku University, Japan. Since then, he has worked at the Tohoku University for 2 years, and then at the University of Tsukuba for 28 years. Currently, he is a Professor at Faculty of Engineering, Information and Systems, the University of Tsukuba, Japan. His scientific interests include medical image analysis, image reconstruction for medical tomography devices such as Computed Tomography (CT) and Positron Emission Tomography (PET), and computer-aided-diagnosis. In particular, he spent a long time of his research career to develop advanced image reconstruction methods in tomography. Most of his research results have been published in top journals in this research field such as Physics in Medicine and Biology and IEEE Transactions on Medical Imaging. More

3 KEYNOTE SPEAKER IV

Room A: 986 1799 7698
Meeting Link: https://zoom.us/j/98617997698

Saturday
15.01.2022.

Prof. Zheli Liu

Nankai University

11:45-12:30

"Oblivious Random Access Machine and its Applications"

Abstract: Encryption alone may not be secure enough because an untrusted server can gain sensitive information from user's access pattern. Oblivious random access machine (ORAM) is the solution to protect access pattern in memory or encrypted cloud storage. In this talk, we will take symmetric search operation as an example and introduce the concept of access pattern, review the typical ORAM models and introduce our work about how to use it to protect the search pattern in the keyword search over ciphertexts.

Bio: Zheli Liu is vice dean of College of Computer Science, vice dean of College of Cyber Science, Nankai University, now. His current research interests include applied cryptography and data privacy protection. He has published more than 50 papers in well-known journals or top conferences, including Usenix Security, VLDB, IEEE TDSC, IEEE TKDE, IEEE TIFS, IEEE TC, IEEE TSC, IEEE INFOCOM and so on. The Google Scholar citations have been over 3400 and eight papers have been the Top 1% highly cited papers.

He was the chairs of several international conferences, including SPNCE 2021, SOCIALSEC 2020, SPNCE 2019, ICA3PP 2018, CSE2017, SPNCE2016, BWCCA2015, EIDWT2013, etc. He is the Associate editor of Springer Cybersecurity, HCIS, and has served as guest editors for many well-known journals, including Springer MoNET, Elsevier JNCA, etc.

4 ABSTRACT OF SESSION

01

No-Show Policy

A paper not presented will be removed from the final conference proceedings.

No refund will be approved to authors of those papers.

02

Duration of Presentation

15min

12min for presentation, and 3min for Q&A.

Presenter's certificate will be sent out by email, one week after the meeting.

03

Report File

a. PowerPoint file
b. PDF file
c. Pre-recorded video

are all acceptable.

Please join Zoom conference at least 10min before your session starts to get prepared.

04

"Best Presentation" Award

It will be selected from each virtual session by the session chair.

Please visit our website a week after the meeting for info.

The presenter will receive a certificate of "Best Presentation".

- Please note that times provided in the program are according to Beijing Time (GMT +8:00).
- Each oral presentation includes a 3-minute Q&A session.

4 ABSTRACT OF SESSION 1

Session 1: Information Privacy and Data Security Session Chair: Dr. Sarfraz Iqbal, Linnaeus University, Sweden	**Time: 13:30-16:00 // Room B: 973 4517 2118** Meeting Link: https://zoom.us/j/97345172118

Time & ID	Presentation
13:30-13:45 **CS035**	Differential Privacy under Incalculable Sensitivity ***Tomoaki Mimoto**, Advanced Telecommunications Research Institute International(ATR), Japan* Abstract—Differential privacy mechanisms have been proposed to guarantee the privacy of individuals in various types of statistical information. When constructing a probabilistic mechanism to satisfy differential privacy, it is necessary to consider the impact of an arbitrary record on its statistics, i.e., sensitivity, but there are situations where sensitivity is difficult to derive. In this paper, we first summarize the situations in which it is difficult to derive sensitivity in general, and then propose a definition equivalent to the conventional definition of differential privacy to deal with them. This definition considers neighboring datasets as in the conventional definition. Therefore, known differential privacy mechanisms can be applied. Next, as an example of the difficulty in deriving sensitivity, we focus on the t-test, a basic tool in statistical analysis, and show that a concrete differential privacy mechanism can be constructed in practice. Our proposed definition can be treated in the same way as the conventional differential privacy definition, and can be applied to cases where it is difficult to derive sensitivity.
13:45-14:00 **CS031**	Blockchain-based Identity Dicovery between Heterogenous Identity Management Systems ***Marcin Dabrowski**, AGH University of Science and Technology, Poland* Abstract—Identity Management Systems (IdMS) have seemingly evolved in recent years, both in terms of modelling approach and in terms of used technology. The early centralized, later federated and user-centric Identity Management (IdM) was finally replaced by Self-Sovereign Identity (SSI). Solutions based on Distributed Ledger Technology (DLT) appeared, with prominent examples of uPort, Sovrin or ShoCard. In effect, users got more freedom in creation and management of their identities. IdM systems became more distributed, too. However, in the area of interoperability, dynamic and ad-hoc identity management there has been almost no significant progress. Quest for the best IdM system which will be used by all entities and organizations is deemed to fail. The environment of IdM systems is, and in the near future will still be, heterogenous. Therefore a person will have to manage her or his identities in multiple IdM systems. In this article authors argument that future-proof IdM systems should be able to interoperate with each other dynamically, i.e. be able to discover existence of different identities of a person across multiple IdM systems, dynamically build trust relations and be able to translate identity assertions and claims across various IdM domains. Finally, authors introduce identity relationship model and corresponding identity discovery algorithm, propose IdMS-agnostic identity discovery service design and its implementation with use of Ethereum and Smart Contracts.

4 ABSTRACT OF SESSION 1

Time & ID	Presentation
14:00-14:15 **CS025**	Evaluation Study on Privacy Policies of Express Companies Based on Cloud Model ***Qian ZHANG**, School of Management, Guangdong University of Technology, China* Abstract—In the era of the Internet of things (IoT), smart logistics is quietly rising, but user privacy security has become an important factor hindering its development. Because privacy policy plays a positive role in protecting user privacy and improving corporate reputation, it has become an important part of smart logistics and the focus of express companies. In this paper, through the construction of the privacy policy evaluation index system of express companies, aiming at qualitative indicators that are difficult to evaluate, we introduce the cloud model evaluation method that can combine the qualitative and quantitative together, and comprehensively evaluate the privacy policy of five express companies in China from four indicators: general situation, user informed consent, information security control and personal rights protection. The results show that: Overall, the privacy policies of the five express companies have not reached the "good" level, and there is a certain gap between the privacy policies of different express companies. From the comparison of indicators, the five express companies generally score relatively good; However, the overall score of information security control index is relatively poor, and the other two indexes are quite different. Cloud model evaluation method has strong applicability for the evaluation of express company privacy policy, which provides a reference for improving the privacy policy formulation and improving the privacy protection level of China's express delivery industry in the era of IoT.
14:15-14:30 **CS038**	Analyzing Initial Design Theory Components for Developing Information Security Laboratories ***Sarfraz Iqbal**, Linnaeus University, Sweden* Abstract—Online information security labs intended for training and facilitating hands-on learning for distance students at master's level are not easy to develop and administer. This research focuses on analyzing the results of a DSR project for design, development, and implementation of an InfoSec lab. This research work contributes to the existing research by putting forth an initial outline of a generalized model for design theory for InfoSec labs aimed at hands-on education of students in the field of information security. The anatomy of design theory framework is used to analyze the necessary components of the anticipated design theory for InfoSec labs in future.

4 ABSTRACT OF SESSION 1

Time & ID	Presentation
14:30-14:45 **CS007**	Vertical Scanning Behavior Analysis of High-Frequency Superpoints ***Wenxian Guo**, Southeast University, China* Abstract—Access superpoint is a host that communicates with a large number of peers at the same time in the network, occupying a large number of network communication resources. Under the background that access superpoint detection algorithms have been developed relatively mature, the anomaly detection research based on this is the direction worth exploring at present. In terms of time, access superpoints can be divided into high-frequency, medium-frequency and low-frequency superpoints. Among them, high-frequency superpoints often contain important data resources and are the first choice for hackers to attack, while vertical scanning is a common pre-invasion method for attackers. Therefore, detecting and analyzing the vertical scanning behavior of high-frequency superpoints plays an important role in the protection of high-frequency superpoints. In this paper, a time-frequency attribute is defined for the detected access superpoints and a time-frequency classification algorithm based on sliding window is proposed. The experimental results show that the algorithm has a high accuracy of 98.26% in a high-speed network environment. The vertical scanning behavior was screened based on the rules. And XGBoost algorithm was used to generate a classifier that can distinguish the abnormal behaviors of high frequency superpoints caused by vertical scanning. The classifier can identify the abnormal behaviors of high frequency superpoints caused by vertical scanning with an accuracy of 93.19%.
14:45-15:00 **CS012**	A Lightweight Advertisement Ecosystem Simulation Platform for Security Analysis ***Chenjia Yu**, Harbin Institute of Technology, Shenzhen, China* Abstract—Based on the statistics, advertisements (ads) generate more than 80% of companies' revenues. However, the complexity of the ads ecosystem blurs the boundaries of responsibility between companies. It can not analyze privacy and security issues in such an ecosystem. For example, collecting user information without user consent for data analysis and displaying ads will cause privacy leakage. But we can not explain which types of the company need to take measures to protect privacy. In our paper, to clarify the responsibility of companies in the advertisement ecosystem, we divide them into six types of entities according to their needs and functions. Then, we design a lightweight simulation platform to illustrate the advertisement ecosystem and support security and privacy analysis. Finally, we take personal ads recommendations based on federated learning as an example to verify the feasibility for privacy and security analysis in this platform.

4 ABSTRACT OF SESSION 1

Time & ID	Presentation
15:00-15:15 **CS023**	From Machine Learning Based Intrusion Detection to Cost Sensitive Intrusion Response ***Tazar Hussain**, Ulster University, United Kingdom* Abstract—Machine learning (ML) based intrusion detection systems (IDS) are increasingly used to discover abnormal patterns in network data and predict cyberattacks. However, the construction of intrusion response systems (IRS) used to deploy countermeasures and prevent malicious activities is more challenging because they require in-depth understanding of attack patterns, attacker behavior, and the correlation between different types of attacks. Furthermore, IDSs generate a large number of false positives and the confidence with which an attack can be predicted is usually unknown. As a result of these challenges in IDS and IRSs, inappropriate actions may be deployed, which may reduce network performance and users' ability to perform typical tasks. Therefore, the present work proposes an intrusion detection and response method based on the Calibrated Random Forest (CRF) algorithm to overcome the key challenges related to the construction of an efficient IRS. The proposed CRF is used to quantify uncertainty in the prediction of cyberattacks and expresses each attack as a probability distribution. Subsequently, the predicted probabilities are used as confidence scores and integrated with domain expert knowledge for decision making in an IRS. We then use publicly available intrusion detection data sets to test and evaluate the proposed method based on three metrics: log loss, Brier score, and expected calibration error (ECE). Experimental results show that the proposed method makes intrusion response more reasonable and cost-sensitive, and has the ability to manage criticality, integrate domain knowledge and explain model behavior. It also demonstrates that this method provides an effective solution for security analysts in how to appropriately deploy and prioritize actions.
15:15-15:30 **CS032**	Cyber-Security Enhanced Network Meta-Model and its Application ***Xinli Xiong**, National University of Defense Technology, China* Abstract—In this paper, we expand the traditional graph model to include security information in cyberspace. And a metamodel in networks that contain both typical network elements and security information is proposed. Detailed definitions of nodes, edges, structures, and paths in a network are given to present security elements from both macroscopic and microcosmic perspectives. Meanwhile, two remarkable case studies, AI-driven penetration testing and cascading failures in routing networks are shown to demonstrate that our model is prevailing in solving frontier issues of security in cyberspace.

4 ABSTRACT OF SESSION 1

Time & ID	Presentation
15:30-15:45 **CS009**	Electromagnetic Side-Channel Attack Resilience against PRESENT Lightweight Block Cipher ***Nilupulee A. Gunathilake**, Edinburgh Napier University, United Kingdom* Abstract—Lightweight cryptography is a novel diversion from conventional cryptography that targets internet-of-things (IoT) platform due to resource constraints. In comparison, it offers smaller cryptographic primitives such as shorter key sizes, block sizes and lesser energy drainage. The main focus can be seen in algorithm developments in this emerging subject. Thus, verification is carried out based upon theoretical (mathematical) proofs mostly. Among the few available side-channel analysis studies found in literature, the highest percentage is taken by power attacks. PRESENT is a promising lightweight block cipher to be included in IoT devices in the near future. Thus, the emphasis of this paper is on lightweight cryptology, and our investigation shows unavailability of a correlation electromagnetic analysis (CEMA) of it. Hence, in an effort to fill in this research gap, we opted to investigate the capabilities of CEMA against the PRESENT algorithm. This work aims to determine the probability of secret key leakage with a minimum number of electromagnetic (EM) waveforms possible. The process initially started from a simple EM analysis (SEMA) and gradually enhanced up to a CEMA. This paper presents our methodology in attack modelling, current results that indicate a probability of leaking seven bytes of the key and upcoming plans for optimisation. In addition, introductions to lightweight cryptanalysis and theories of EMA are also included.
15:45-16:00 **CS1001**	The processing goes far beyond "the app" – Privacy issues of decentralized Digital Contact Tracing using the example of the German Corona-Warn-App ***Rainer Rehak**, Weizenbaum-Institut for the Networked Society, Germany* Abstract—Since SARS-CoV-2 started spreading in Europe in early 2020, there has been a strong call for technical solutions to combat or contain the pandemic, with contact tracing apps at the heart of the debates. The EU's General Data Protection Regulation (GDPR) requires controllers to carry out a data protection impact assessment (DPIA) where their data processing is likely to result in a high risk to the rights and freedoms (Art. 35 GDPR). A DPIA is a structured risk analysis that identifies and evaluates possible consequences of data processing relevant to fundamental rights in advance and describes the measures envisaged to address these risks or expresses the inability to do so. Based on the Standard Data Protection Model (SDM), we present the results of a scientific and methodologically clear DPIA. It shows that even a decentralized architecture involves numerous serious weaknesses and risks, including larger ones still left unaddressed in current implementations. It also found that none of the proposed designs operates on anonymous data or ensures proper anonymisation. It also showed that informed consent would not be a legitimate legal ground for the processing. For all points where data subjects' rights are still not sufficiently safeguarded, we briefly outline solutions.

4 ABSTRACT OF SESSION 2

Session 2: Cyber Attacks and Security Session Chair: Asst. Prof. Abdulbast Ali Abushgra, Utica College, USA	**Time: 09:30-11:45 // Room B: 973 4517 2118** Meeting Link: https://zoom.us/j/97345172118

Time & ID	Presentation
09:30-09:45 **CS033**	CoAP-DoS: An IoT Network Intrusion Dataset ***Jared Mathews**, The Citadel, USA* Abstract—The need for secure Internet of Things (IoT) devices is growing as IoT devices are becoming more integrated into vital networks. Many systems rely on these devices to remain available and provide reliable service. Denial of service attacks against IoT devices are a real threat due to the fact these low power devices are very susceptible to denial-of-service attacks. Machine learning enabled network intrusion detection systems are effective at identifying new threats, but they require a large amount of data to work well. There are many network traffic data sets but very few that focus on IoT network traffic. Within the IoT network data sets there is a lack of CoAP denial of service data. We propose a novel data set covering this gap. We develop a new data set by collecting network traffic from real CoAP denial of service attacks and compare the data on multiple different machine learning classifiers. We show that the data set is effective on many classifiers.
09:45-10:00 **CS024**	Multifaceted Analysis of Malicious Ethereum Accounts and Corresponding Activities ***Jia Wang**, Yokohama National University, Japan* Abstract—In recent years, Ethereum, one of the leading applications to realize the service of blockchain technology, has received a great deal of attention with the usability and functionality to execute smart contracts, arbitrary programmable calculations in addition to cryptocurrency trading. However, misconfigured Ethereum clients with application programming interface (API) enabled, JSON-RPC in particular, are targeted by cyberattacks. In this research, we propose a new framework to detect malicious and suspicious Ethereum accounts using 3 different data sources (honeypot, Internet-wide scanner and blockchain explorer). The honeypot, named Etherpot, utilizes a proxy server placed between a real Ethereum client and the Internet. It modifies responses from the Ethereum client to attract attackers, identifies malicious accounts and analyzes their behaviors. With the Internet-wide scan results from Shodan, we also detect suspicious Ethereum accounts that are registered on multiple nodes. Finally, we utilize Etherscan, a well-known blockchain explorer for Ethereum, to track and analyze the activities related to the detected accounts. Through the observation of 6 weeks, we observed 538 hosts trying to call JSON-RPC of our honeypots with 41 different types of methods, including 2 types of unreported attacks in the wild. We detected 16 malicious accounts from the honeypots and 64 suspicious accounts from Shodan scan results, 5 out of which are overlapped. Finally, from Etherscan, we collected records of activities related to the detected accounts, including transactions of 21.50 ETH and mining of 22.61 ETH (equivalent to 167,560 US$ at the rate of 2021/10/14). To an end, we provide a much brighter view of malicious activities on Ethereum.

4 ABSTRACT OF SESSION 2

Time & ID	Presentation
10:00-10:15 **CS019**	A Proactively Defensive Low-Level Decision Center Model of Endogenous Security ***Feilin Li**, Southeast University, China* Abstract—With the development of 5g and next-generation networks, shell-based defenses are becoming increasingly unsuitable and become a burden and obstacle to information systems. The endogenous security defense system based on the bionic mechanism has entered people's field of vision. On this basis, this paper proposes a spinal-like low-level decision center model in the endogenous security system. It uses fuzzy cognitive maps and trusted computing to comprehensively analyze the information of the system, and makes decisions based on the needs of applications and tasks. Some case studies and experimental results prove the effectiveness and efficiency of the model.
10:15-10:30 **CS013**	Context-based Adblocker using Siamese Neural Network ***Rui Ning**, School of Cybersecurity, Old Dominion University, USA* Abstract—This paper proposes a new content-based ad-blocker to minimize the amount of human effort required to effectively combat pushed advertisements. Current ad-blocker models are expensive to maintain and not always effective in identifying confusable images that may play different roles across diverse websites. We investigated the possibility of solving these problems with the introduction of a deep learning, content-based ad-blocker model. More specifically, the proposed ad-blocker identifies advertisement images by combining the contained information of a given image and the content of the website it originated from. The proposed solution was prototyped and applied to a diverse selection of popular websites, achieving a detection accuracy of 98%.
10:30-10:45 **CS020**	The Future Roadmap for Cyber Attack Detection ***Rasha Kashef**, Ryerson University, Canada* Abstract—Cyber-attacks can cause delays in world operations and substantial economic losses. Therefore, there is a greater interest in cyber-attack detection (CAD) to accommodate the exponential increase in the number of attacks. Various CAD techniques have been developed, including Machine Learning (ML) and Deep Learning (DL). Despite the high accuracy of the deep learning-based method when learning from large amounts of data, the performance drops considerably when learning from imbalanced data. While many studies have been conducted on imbalanced data, the majority possess weaknesses that can lead to data loss or overfitting. However, Generative Adversarial Networks can help solve problems such as overfitting and class overlapping by generating new virtual data similar to the existing data. This paper provides a comprehensive overview of the current literature in CAD methods, thus shedding light on present research and drawing a future road map for cyber-attack detection in different applications.

4 ABSTRACT OF SESSION 2

Time & ID	Presentation
10:45-11:00 **CS004**	Anonymity-driven Measures for Privacy ***Sevgi Arca**, Texas Tech University, USA* Abstract—In today's world, digital data are enormous due to technologies that advance data collection, storage, and analyses. As more data are shared or publicly available, privacy is of great concern. Having privacy means having control over your data. The first step towards privacy protection is to understand various aspects of privacy and have the ability to quantify them. Much work in structured data, however, has focused on approaches to transforming the original data into a more anonymous form (via generalization and suppression) while preserving the data integrity. Such anonymization techniques count data instances of each set of distinct attribute values of interest to signify the required anonymity to protect an individual's identity or confidential data. While this serves the purpose, our research takes an alternative approach to provide quick privacy measures by way of anonymity especially when dealing with large-scale data. This paper presents a study of anonymity measures based on their relevant properties that impact privacy. Specifically, we identify three properties: uniformity, variety, and diversity, and formulate their measures. The paper provides illustrated examples to evaluate their validity and discusses the use of multi-aspects of anonymity and privacy measures.
11:00-11:15 **CS011**	A Class of Software-Layer DoS Attacks in Node.js Web Apps ***Tuong Phi Lau**, University of Information Technology, Ho Chi Minh, Vietnam* Abstract—Application-level DoS attacks are occurring more frequently and raise more serious threats. Such attacks can be performed advantageously in node.js web apps, as these apps are built by third-party npm packages. Adversaries may inject malicious data into its client requests and submit them to a victim server. It then may manipulate program states to pass the malicious input to sensitive APIs as long-running operations which are resided in npm packages required in the node.js web app. Once the sensitive APIs (e.g. pattern matching) can be called with hard-to-match input string, it can cause degradation of the worker pool's throughput of the web server to interrupt web services accessed by Internet users. This attack vector is defined as Module-driven DoS (MDoS).

4 ABSTRACT OF SESSION 2

Time & ID	Presentation
11:15-11:30 **CS002**	Teleporting Qubits Between Participants by Third-Party Center ***Abdulbast Ali Abushgra**, Utica College, USA* Abstract—As many applied and theoretical challenges are still facing the quantum computing in general and quantum cryptography in specific. Teleporting a qubit from a participant to another has been catching most of the recent concentration in this field. Quantum Key Distribution is a method as in the classical system that provides secret keys to secure the communication channels between legitimate participants by different mechanisms. In this paper, a quantum key exchange protocol is designed to carry qubits from a trusted third party to both communicators. The Third-Party Center (TPC) initiates secure exchanges between the sender (Alice) and the receiver (Bob). The legitimate parties only share indexes with TPC, where the TPC cannot forge the communication parameters. These parameters include photons applied under an EPR Paradox environment. Therefore, the legitimate parties can share data securely by using a third-party without any restrictions.
11:30-11:45 **CS014**	IoTProtect: A Machine-Learning Based IoT Intrusion Detection System ***Mohammed M. Alani**, Seneca College of Arts and Technology, Canada* Abstract—The rapid growth in IoT adoption in various dailylife applications, combined with the lack of proper patching and securing, has made IoT an easy target for malicious actors. As we notice the increase in the utilization of IoT devices in conducting security attacks around the world, research needs to catch up and protect IoT devices. In this paper, we present IoTProtect; a machine-learning based intrusion detection system utilizing the TON IoT dataset in training and testing. Testing the proposed system showed 99.999% detection accuracy with 0.001% false-positive, and 0% falsenegative with excellent timing performance.

4 ABSTRACT OF SESSION 3

Session 3: Information Network and Information Management Session Chair: Dr. Li Li, Peking University, China	**Time: 13:00-15:00 // Room B: 973 4517 2118** Meeting Link: https://zoom.us/j/97345172118

Time & ID	Presentation
13:00-13:15 **CS037**	A Two-Stage Out-Of-Box Method for Detecting Side-Channel Attacks in Cloud Computing ***Jiangyong Shi**, National University of Defense Technology, China* Abstract—In this paper, we proposed a two-stage out-of-box method for detecting side-channel attacks in cloud computing. The method detects side-channel attacks from outside of the virtual machine, utilizing hardware support of performance events and hypervisor's ability to introspect the virtual machine, which is robust and stealthy to attackers. By utilizing information of hardware performance counters to train a classification model, we can quickly locate the suspicious attacking virtual machine with 96.7% of precision and 95% of recall rate. By adjusting the sampling duration and interval, we can get a F1-score of 98.9%. By utilizing virtual machine introspection method to extract syscall information of suspicious virtual machine, we can precisely locate the suspicious process. Experiments demonstrate our method's effectiveness in detecting cache side-channel attacks.
13:15-13:30 **CS030**	Spectrum-based Fingerprint Extraction and Identification Method of 100M Ethernet Card ***Jiaqi Liu**, Southeast University, China* Abstract—In the local area network (LAN) system, most terminals are connected to edge switches through fast or gigabit Ethernet connections. The terminal access security problem has always been a key concern. This paper proposes a method of Ethernet card fingerprint extraction and identification based on spectrum characteristics, which solves the problem of illegal terminal access with counterfeit media access control (MAC) addresses. The extracted Ethernet card fingerprint is used as the identity of the terminal, which is unique and difficult to be counterfeited. The frequency-domain features of the signals can be extracted by analyzing the Ethernet card signals of wired terminals received by the switch. The dimension of these features is reduced to obtain their Ethernet card fingerprints, which can be effectively classified and identified. In the classification and recognition experiments on 7 Ethernet cards of 100M produced by the same manufacturer, 26 Ethernet cards by different manufacturers, and 65 Ethernet cards by mixed manufacturers, all Ethernet cards can achieve an accuracy of 100%. This method can be widely used for identity authentication during the access and connection of terminals and provides a secure access control scheme.

4 ABSTRACT OF SESSION 3

Time & ID	Presentation
13:30-13:45 **CS034**	Convex Hull Convolutive Non-negative Matrix Factorization Based Speech Enhancement For Multimedia Communication ***Dongxia Wang**, Tianjin University of Technology and Education, China* Abstract—In this paper, an effective speech enhancement method is proposed for the next generation multimedia communication system. The priori knowledge of the enhancement stage is obtained by the modified Convex Hull Convolutive NMF with less information loss. To deal with the difficulty of its optimal gain estimation, an iterative algorithm is then introduced to update the coefficient matrix. The experimental results under different types of noise environment show that the proposed algorithm can reduce the signal distortions dramatically, and provide better enhancement performance than the benchmark algorithms simultaneously, especially under adverse conditions.
13:45-14:00 **CS036**	An approach to construct feedforward clock-controlled sequence with high linear complexity ***Yangpan Zhang**, Peking University, China* Abstract—In practical applications, people tend to use feedforward clock control structures to construct stream ciphers. However, it is difficult to estimate the linear complexity lower bound for stream ciphers constructed in this way. This paper proposes a clock-controlled sequence construction method with provably high linear complexity. For a control sequence with period m, the complexity of proof is O(m2), independent of the controlled sequence period size.
14:-00-14:15 **CS001**	Analysis of the Propagation of Miner Botnet ***Yuxi Cheng**, Southeast University, China* Abstract—Miner Botnet, a new type of botnet that perform digital cryptocurrency mining by invading and implanting malware programs in normal noncooperative user terminals, and occupy their computational resource, has been widely propagated with the soaring price of crypto currencies and become one of the major threats to the security of today's cyber-space. Since the rapid spread of miner botnet mainly relies on the vulnerabilities in the computer system, the security of the computer system will be greatly improved if the vulnerability exploitation tactics of miner botnet can be predicted. In this paper, we study the exploitation history of the vulnerabilities exploited by miner botnets, build a new set of attributes on the basis of CVSS3.0 and use the knowledge graph as the framework to model the relationship between miner botnet, vulnerabilities and vulnerability attributes, and propose a method, combined with Apriori, Fast-Unfolding and a reasoning algorithm based on the knowledge structure, to predict the vulnerability exploitation tactics of miner botnet. Thereby we can prejudge the exploitation of miner botnets with historical data of vulnerability exploitation. The experimental results also show that the algorithm has a certain predictive effect on the vulnerability exploitation tactics of miner botnets. The algorithm can help security personnel respond to the attacker's behavior in advance and reduce the loss .

4 ABSTRACT OF SESSION 3

Time & ID	Presentation
14:15-14:30 **CS039**	Blockchain based Smart Parking System using Ring Learning with Error based Signature ***Jihan Lailatul Atiqoh***, *Telkom University, Indonesia* Abstract—Recently, placing vehicles in the parking area is becoming a problem. A smart parking system is proposed to solve the problem. Most smart parking systems have a centralized system, wherein that type of system is at-risk of single-point failure that can affect the whole system. To overcome the weakness of the centralized system, the most popular mechanism that researchers proposed is blockchain. If there is no mechanism implemented in the blockchain to verify the authenticity of every transaction, then the system is not secure against impersonation attacks. This study combines blockchain mechanism with Ring Learning With Errors (RLWE) based digital signature for securing the scheme against impersonation and double-spending attacks. RLWE was first proposed by Lyubashevsky et al. This scheme is a development from the previous scheme Learning with Error or LWE.
14:30-14:45 **CS021**	The AILA Methodology for Automated and Intelligent Likelihood Assignment ***Cristian Daniele***, *Radboud University, Italy* Abstract—Risk assessment is core to any institution's evaluation of risk, notably for what concerns people's privacy. The assessment often relies on information stated in a policy shaped as a text document. The risk assessor, or analyst in brief, is called to understand documentation that can be long, unclear or incomplete, hence subjectivity or distraction may strongly influence the process, particularly for identifying each relevant asset and for the assignment of the likelihood value of a given threat to an identified asset. The aim of this paper is to reduce the influence of subjectivity and distraction through risk assessment by means of our methodology for the Automated and Intelligent Likelihood Assignment (AILA). While the analyst's role cannot be emptied, it is facilitated through entities identification and likelihood assignment to threats for assets. The methodology adopts Natural Language Processing for summarisation and entity recognition, it tailors fully-supervised Machine Learning over policy documents and it leverages an existing tool supporting risk assessment, PILAR, in order to gain a more objective likelihood assignment. The paper demonstrates AILA over three real-world case studies from the automotive domain, culminating with the risk assessment exercises over the privacy policies of Toyota, Mercedes and Tesla.
14:45-15:00 **CS005**	RippleSign: Isogeny-Based Threshold Ring Signatures with Combinatorial Methods ***Li Li***, *Peking University, China* Abstract—Threshold ring signature schemes are widely used in blockchains and cryptocurrencies. Isogeny-based signature schemes benefit from short public key and signature sizes. In this paper, by using trapdoor commitments in ring signatures, we propose a decentralized post-quantum threshold ring signature scheme, RippleSign, based on isogenies between supersingular elliptic curves. Our scheme enjoys perfect anonymity and is unforgeable under a chosen-message attack. In terms of practicality, our threshold scheme has signature size of 187 KB with 100 participants at the 128-bit security level. In addition, our scheme takes about 2 seconds to produce (2,3)-threshold ring signature.

5 CONFERENCE COMMITTEE 2022

Advisory Committees
Gang Qu, University of Maryland, USA
Josep Domingo Ferrer, Universitat Rovira i Virgili, Spain

Conference Local Organizing Chair
Genghuang Yang, Tianjin University of Technology and Education, China

Program Chairs
Xiaofeng Wang, Xi'an University of Technology, China
Rose Shumba, Bowie State University, USA
Yanqiu Che, Tianjin University of Technology and Education, China
Chunxiao Han, Tianjin University of Technology and Education, China
Jian Dong, Tianjin University of Technology and Education, China

Conference Chair
Bing Yan, Tianjin University of Technology and Education, China

Conference Co-Chair
Shuangbao Wang, Morgan State University, USA

Publicity Chair
Xiangyang Hao, Information Engineering University, China

Local Oragnizing Committee
Yujun Cai, Tianjin University of Technology and Education, China
Jihua Cao, Tianjin University of Technology and Education, China
Liguo Tian, Tianjin University of Technology and Education, China
Fengjie Zhai, Tianjin University of Technology and Education, China
Shilong Zhang, Tianjin University of Technology and Education, China
Li Zhao, Tianjin University of Technology and Education, China
Zhiliang Chen, Tianjin University of Technology and Education, China
Min Li, Tianjin University of Technology and Education, China

5 CONFERENCE COMMITTEE 2022

Technical Committees

Abdulbast Ali Abushgra, Utica College, USA

Almas Abbasi, International Islamic University Islamabad, Pakistan

Ashraf Darwish, Helwan University, Russia

Carlos Guardado da Silva, University of Lisbon, Portugal

Dra. Cristina Freitas, University of Coimbra, Portugal

Eric Sakk, Morgan State University, USA

Farah Afianti, Telkom University, Indonesia

Gabriela MOGOS, Xi'an Jiaotong-Liverpool University, China

Haleh Shahzad, Telus, Canada

Hung-Yu Chien, National Chi Nan University, China

Jaouhar Fattahi, Laval University, Canada

Jorge Sequeira, LABS: Lisbon Accounting and Business School Polytechnic University, Portugal

Li Li, Peking University, China

Luís Corujo, University of Lisbon, Portugal

Jiangyong Shi, National University of Defense Technology, China

Meghana Kshirsagar, University of Limerick, Ireland

Min-Shiang Hwang, National Chung Hsing University, China

Paulo Batista, CIDEHUS.UÉ - Interdisciplinary Center of History, Cultures and Societies of the University of Évora, Portugal

Priteshkumar Prajapati, Chandubhai S. Patel Institute of Technology, India

Rika Butler, Stellenbosch University, South Africa

She Kun, University of Electronic Scinece and Technology China, China

Sherali Zeadally, University of Kentucky, USA

Thelma Palaoag, University of the Cordilleras, Philippines

Wei Li, Beijing Jinghang Computation and Communication Research Institute, China

Xiaochun Cheng, Middlesex University, UK

Yang Liu, Harbin Institute of Technology (Shenzhen), China

If you have any questions, please feel free to contact us any time.

CSP
WWW.ICCSP.ORG

CSP 2022
E-mail: iccsp_conf@126.com
Tel: +86-137-3111-1131
Web: www.iccsp.org