2024 17th International Conference on Security of Information and Networks (SIN) Program

Time (Sydney)	Room-1	Room-2	Room-Break
Monday, December 2			
09:00 am-09:45 am	**K1**: *Opening & Keynote 1* Interplay of AI and Cybersecurity: How Will it Affect Us All?		
09:45 am-10:30 am	**K2**: *Keynote 2* Side channel Attacks, Remote Power Attacks and Countermeasures		
10:30 am-11:00 am			**B1**: *Break*
11:00 am-11:30 am	**S1.1**: *Network Security-1*	**D2.1**: *Invited Presentation* Autonomous UAVs for Wildfire Management: AI-Driven Solutions for Next-Generation Emergency Response	
11:30 am-12:30 pm		**D2.2**: *Drone Sense-AI Workshop 1*	
12:30 pm-01:30 pm			**B2**: *Break*
01:30 pm-03:00 pm	**S1.2**: *Network Security-2*	**D2.3**: *Drone Sense-AI Workshop 2*	
03:00 pm-03:30 pm			**B3**: *Break*
03:30 pm-05:00 pm	**S1.3**: *Machine Learning and Security*	**S2.3**: *Application Security 1*	
Tuesday, December 3			
09:00	**K3**: *Keynote 3* Establishing Trustworthy Data		

Time (Sydney)	Room-1	Room-2	Room-Break
am-09:45 am	Sharing and Use Frameworks		
09:45 am-10:30 am	**K4**: *Keynote 4* Election verification for computer scientists		
10:30 am-11:00 am			**B4**: *Break*
11:00 am-12:30 pm	**S1.4**: *Security and AI-1*	**S2.4**: *Security and Privacy-1*	
12:30 pm-01:30 pm			**B10**: *Break*
01:30 pm-03:00 pm	**S1.5**: *Security and AI-2*	**S2.5**: *Security and Privacy-2*	
03:00 pm-03:30 pm			**B5**: *Break*
03:30 pm-05:00 pm	**S1.6**: *IoT & Security*	**S2.6**: *Block-Chain and Security*	
Wednesday, December 4			
09:45 am-10:30 am	**K5**: *Keynote 5* Cloud Computing Security: Past, Present and Future		
10:30 am-11:00 am			**B6**: *Break*
11:00 am-12:30 pm	**S1.7**: *Security & Education*	**S2.7**: *Cloud*	
12:30 pm-01:30			**B7**: *Break*

Time (Sydney)	Room-1	Room-2	Room-Break
pm			
01:30 pm-03:00 pm	**S1.8**: *Other Topics in Security*	**S2.8**: *Application Security-2*	
03:00 pm-03:30 pm	**C1**: *Closing Ceremony and Best Paper Awards*		

Monday, December 2

Monday, December 2 9:00 - 9:45 (Australia/Sydney)

K1: Opening & Keynote 1

Interplay of AI and Cybersecurity: How Will it Affect Us All?

Atilla Elçi
Hasan Kalyoncu University, Türkiye

Room-1

Abstract: AI has come strong this time. It looks like it is here to stay and plays an increasingly decided role in all niches of our lives. We would be most concerned with the safety and security aspects where AI and cybersecurity interact. On the one hand, AI helps enhance cybersecurity, and just at the same stance, it equips adversaries to enhance their capabilities. Let's look at how AI interacts with cybersecurity- how each is indispensable for the other. We shall survey AI's part in cybersecurity, security's role in AI use, ethical issues, whether AI is what we expect it to be, and how organizations try to cope with the interplay.

Bio: Prof. Dr. Atilla ELÇI is a full Software Engineering professor at Hasan Kalyoncu University, Türkiye. He served as faculty and chairman in computer engineering and software engineering departments in several universities in Turkey and abroad. He started several BSc, MSc, and PhD programs. He has published over a hundred journal and conference papers and book chapters; co-authored The Composition of OWL-S based Atomic Processes (LAP Lambert, 2011); edited the Semantic Agent Systems (Springer, 2011), Theory and Practice of Cryptography Solutions for Secure Information Systems (2013), The Handbook of Applied Learning Theory and Design in Modern Education (2016), Metacognition and Successful Learning Strategies in Higher Education (2017), Contemporary Perspectives on Web-Based Systems (2018), Handbook of Research on Faculty Development for Digital Teaching and Learning (2019), Artificial Intelligence Paradigms for Smart Cyber-Physical Systems (2021), Challenges and Applications of Data Analytics in Social Perspectives (2021), Future of Digital Technology and AI in Social Sectors (2024), Cutting-Edge Technologies for Business Sectors (2024), Multifaceted Uses of Cutting-Edge Technologies and Social Concerns all by IGI Global, 2024), and the proceedings of SIN Conferences 2007-20 (ACM) and 2021-24 (IEEE), ESAS 2006-24 (IEEE CS). He initiated and ran ESAS workshops and SIN Conferences. He delivers keynote speeches at international conferences on educational technology, web semantics, machine learning, knowledge representation and ontology, and information security.

Monday, December 2 9:45 - 10:30 (Australia/Sydney)

K2: Keynote 2

Side channel Attacks, Remote Power Attacks and Countermeasures

Prof. Sridevan Parameswaran
The University of Sydney, Australia

Room-1

Abstract Deep devastation is felt when privacy is breached, personal information is lost, or property is stolen. Now imagine when all of this happens at once, and the victim is unaware of its occurrence until much later. This is the reality, as an increasing number of electronic devices are used as keys, wallets and files. Security attacks targeting embedded systems illegally gain access to information or destroy information. Advanced Encryption Standard (AES) is used to protect many of these embedded systems. While mathematically shown to be quite secure, it is now well known that AES circuits and software implementations are vulnerable to side channel attacks. Side-channel attacks are performed by observing properties of the system (such as power consumption, electromagnetic emission, etc.) while the system performs cryptographic operations. In this talk, differing power-based attacks are described, and various countermeasures are explained. A countermeasure titled Algorithmic Balancing is described in detail. Implementation of this countermeasure in hardware and software is described. Since process variation impairs countermeasures, we show how this countermeasure can be made to overcome process variations. In the next part of the talk, Remote power attacks are described, and novel sensors are demonstrated which enable stealthy deployment of attacks on Cloud based FPGAs (such as the Amazon Cloud FPGA).

Bio Sri Parameswaran is the Head of School of Electrical and Computer Engineering at the University of Sydney. Prior to that he was a Professor in the School of Computer Science and Engineering at the University of New South Wales. He also served as the Program Director for Computer Engineering. His research interests are in System Level Synthesis, Low power systems, High Level Systems, Security, Genomic Systems and Network on Chips. He served as the Editor in Chief of the IEEE Embedded Systems Letters, and has served on the editorial boards of IEEE Transactions on Computer Aided Design, ACM Transactions on Embedded Computing Systems, the EURASIP Journal on Embedded Systems and the Design Automation of Embedded Systems. He has served on the Program Committees of Design Automation Conference (DAC), Design and Test in Europe (DATE), the International Conference on Computer Aided Design (ICCAD), the International Conference on Hardware/Software Code-sign and System Synthesis (CODES-ISSS), and the International Conference on Compilers, Architectures and Synthesis for Embedded Systems (CASES). Sri Parameswaran is a Fellow of the IEEE.

Monday, December 2 10:30 - 11:00 (Australia/Sydney)

B1: Break

Room-Break

Monday, December 2 11:00 - 11:30 (Australia/Sydney)

D2.1: Invited Presentation

Autonomous UAVs for Wildfire Management: AI-Driven Solutions for Next-Generation Emergency Response

A/Prof. Fatemeh Afghah
Clemson University.

Room-2

Abstract The deployment of unmanned aerial vehicles (UAVs) in wildfire management and disaster response represents a paradigm shift in leveraging intelligent systems for emergency operations. UAVs, equipped with advanced sensing capabilities such as thermal cameras and high-resolution imaging, are uniquely suited to perform rapid situational assessments in hazardous, inaccessible areas. These systems can detect and track wildfire dynamics, provide real-time data for fire progression modeling, and assist in prioritizing resource allocation for mitigation efforts. By minimizing the need for human exposure to dangerous environments, UAVs offer a safer and more effective alternative to traditional disaster response

approaches. Despite the potential of UAVs, current operational frameworks are often constrained by manual control paradigms, involving ground-based commanders or operators in manned aircraft. These configurations not only limit the scalability of UAV deployments but also expose operators to operational risks. Fully autonomous UAV systems present a transformative solution, capable of executing complex, large-scale missions with minimal human intervention. Autonomous drones can dynamically coordinate, communicate, and perform tasks such as fire perimeter monitoring, hotspot detection, and real-time mapping through the integration of cutting-edge AI and multi-agent collaboration algorithms. In this talk, we will present our recent advancements in autonomous UAV systems for wildfire management. This includes innovations in distributed communication protocols, cooperative path planning, decentralized task allocation, and AI-driven wildfire detection and mapping. We will also discuss the integration of these technologies into a scalable, low-cost framework for enabling intelligent, adaptive, and autonomous UAV fleets to address the multifaceted challenges of wildfire management in real-world scenarios.

Biography Fatemeh Afghah is an Associate Professor with the Electrical and Computer Engineering Department at Clemson University. Prior to joining Clemson University, she was an Associate Professor (2020-2021) and an Assistant Professor (2015-2020) with the School of Informatics, Computing and Cyber Systems, Northern Arizona University, where she was the Director of Wireless Networking and Information Processing (WiNIP) Laboratory. Her research interests include wireless communication networks, decision-making in multi-agent systems, radio spectrum management, UAV networks, security and artificial intelligence in healthcare. Her recent project involves autonomous decision-making in uncertain environments, using autonomous vehicles for disaster management and IoT security. Her research has been continuously supported by NSF, AFRL, AFOSR, NIH, and Arizona Board of Regents, where she has served in the role of PI or the sole PI for grants with a total of over $4.8M and in the role of Co-PI for grants with a value of $5M. She is the recipient of several awards, including the Air Force Office of Scientific Research Young Investigator Award in 2019, the NSF CAREER Award in 2020, NAU's Most Promising New Scholar Award in 2020, NSF CISE Research Initiation Initiative (CRII) Award in 2017, AFRL Visiting Research Faculty Award in 2016 and 2017. and NC Space grant's New Investigator award in 2015.

She is an inventor/co-inventor of 5 patents and an author/co-author of over 100 peer-reviewed publications. She served as the associate editor for several journals, including Elsevier Ad hoc Networks, Computer Network Journal, Springer Neural Processing Letters and Frontiers Aerial and Space Networks Journal. She is an IEEE Senior member and was the chair and organizer of the IEEE Communications and Signal Processing Chapter at the IEEE Central North Carolina Section. She served as the representative of IEEE regions R1-6 on the membership board standing committee for the IEEE Signal Processing Society (2016-18) and as Mentoring co-chair (2019-2021) and Advocate co-chair (2015-2016) for the N2W

Monday, December 2 11:00 - 12:30 (Australia/Sydney)

S1.1: Network Security-1

Room-1

11:00 ***Taxonomy of User-Centric Errors Leading to Cyber Attacks in LoRaWAN***

Indu Parajuli, Biplob Ray, Jahan Hassan and Michael Cowling (Central Queensland University, Australia)

In recent years, the use of the Internet of Things (IoT) has grown rapidly in smart cities, households, and smart industries environments due to the benefits of convenience and easy implementation. The Long-Range Wide Area Network (LoRaWAN) is a key technology driving this growth, which has seen significant adoption due to its scalability, long-range capabilities, low power consumption, lost cost and wide area coverage. As the use of LoRaWAN-enabled IoT environment has increased, the cyber-attacks related to it have also increased. About 95% of the cyber-attacks in IoT environment occurs due to the security vulnerabilities caused by the user's errors. However, much research in the LoRaWAN environment is highly focused on the security vulnerabilities due to technical errors, leaving gaps in identifying the security vulnerabilities that occur due to user errors. Therefore, this paper addresses these gaps by identifying user-centric errors which may lead to cyber-attacks in an LoRAWAN IoT environment. It builds a taxonomy based on a comprehensive literature review and maps these user errors to potential security vulnerabilities within LoRaWAN-enabled IoT environments.

11:22 ***Comprehensive Security of SDN Controllers in NFVI-BASED 5G Network***

Asad Faraz Khan and Priyadarsi Nanda (University of Technology Sydney, Australia)

In the present world, Software-Defined Networks (SDN) is the developing technological environment that allows integrated control and splits the control plane from the data plane. It is essential to classify the attacks in SDN-based networks to improve security. Concomitantly, SDN-related networks are vulnerable to numerous attacks especially Distributed Denial of Service (DDoS) attacks which interrupt the data transmission and network data. To resolve this issue, various traditional researchers have attempted to attain attack detection, however, there is a lack in computational cost, accuracy rate, and Packet Delivery Ratio. To overcome the limitations, the proposed hybrid model employs a system creation model for encrypting data using ELGAMAL and ECC algorithms to strengthen data security. Furthermore, the present hybrid model incorporates the wrapper-based approach Sine Cosine hybrid optimization algorithm with Modified Particle Swarm Optimization (SCMPSO) for feature selection which is intended to improve the performance of the classification. Furthermore, it utilizes the XG Boost-Light Gradient-Boosting Machine (GBM) algorithm for attack classification. Accordingly, Extreme Gradient-Boosting (XG Boost) can handle the missing data, and the ensemble nature of XG Boost with multiple Decision trees (DT) combinations makes it challenging to finalize the prediction. To overcome the limitations of the XG Boost algorithm, the proposed model uses Light GBM. Correspondingly, the present method created a dataset using the Mininet tool. The efficacy of the proposed hybrid model is calculated with several evaluation metrics to analyze the performance. The proposed method is intended to contribute to SDN-based network development and is envisioned to contribute to attack detection mechanisms.

11:45 ***Dynamic Network Slicing and Deep Learning Based Intrusion Detection System With Virtual Load Balancing in Edge Enabled SDN/NFV Based 5G Networks***

Asad Faraz Khan and Priyadarsi Nanda (University of Technology Sydney, Australia)

In current times, network slicing in a 5G context is a significant study field. But it might be difficult to meet network slice requests' requirements. Network slices need to share limited resources; therefore energy efficiency and security are crucial. Additionally, it is essential to establish secured network slicing for Software-Defined Network/Network Function Virtualization (SDN/NFV). As attackers have developed to become more skilled and frequently use different attacking approaches, security is a crucial problem in network slicing. We address security, ineffective network slicing, and overloading using load balancing and Deep Learning (DL) based network slicing algorithms in edge enabled SDN/NFV assisted 5G settings in this research. Here, we mainly concentrate on secure and efficient network slicing in SDN/NFV assisted 5G systems. Initially, slicing of network is performed based on UniqueNet which includes lightweight convolutional layers that reduce the processing time and increase accuracy. For authentication of users, we employ the Improved Mersenne Twister (IMT) algorithm and role-based access control is performed using Improved Deep Q Network (ImDQN) algorithm for authorization purpose. Clustering is done by using k-means clustering (KMC) algorithm. Here, Cluster Head (CH) performed intrusion detection using Enhanced Bidirectional Generative Adversarial Network (E-BiGAN) algorithm. After detected intrusions, the Kangaroo-based IDS (KIDS) jump and send the notification to all the nodes in the CH. For efficient load balancing, we perform optimal switch selection using Dove Swarm Optimization (DSO). The performance of the suggested framework is then evaluated in terms of different metrics and compared with existing approaches to prove the efficacy of the proposed system.

12:07 ***A Novel Key Management Framework for Secure and Scalable Decentralized Identity Systems***

Mert Yıldız and Serif Bahtiyar (Istanbul Technical University, Turkey)

The rise of decentralized identity systems has posed significant challenges in the secure and scalable management of keys, especially in large-scale national identity programs. In this paper, we propose a new secure and scalable framework for cryptographic keys management that may be applied in a national digital identity system. The proposed framework provides a hierarchical structure for efficient key generation and isolation, while hardware security modules provide a secure environment for key storage and operations. Key wrapping is implemented to enable secure

external storage of large volumes of keys. In our work, we present a comprehensive security analysis. Our analysis demonstrates the resilience of the framework against various threat vectors and its ability to address key management challenges such as complexity, scalability, security isolation, recovery and secure delegation. The proposed framework provides a promising solution for security and scalability of national-level identity systems.

Monday, December 2 11:30 - 12:30 (Australia/Sydney)

D2.2: Drone Sense-AI Workshop 1

Room-2

11:30 ***Spatial Prediction of UAV Position Using Deep Learning***

Márton Bertalan Limpek (Budapest University of Technology and Economics & Ericsson, Hungary); Géza Szabó (Ericsson Research, Hungary); László Hévizi (Ericsson Hungary, Hungary); István Gódor (Ericsson Research, Hungary)

This paper presents a deep learning approach for drone navigation aimed at accurately estimating a drone's position based on RSS in a simulated environment. A predefined route is established, and the drone collects RSS and IMU data while traversing it multiple times. This dataset serves as the foundation for training various neural network architectures. We create multiple training and test datasets to compare different models and identify the most effective approach for predicting the drone's location. After training, the neural networks are evaluated using distinct test data, showing that deep learning models can reliably predict a drone's position in simulation. The developed predictive models enhance the accuracy and reliability of autonomous drone operations in real-world scenarios.

11:50 ***Bushfire Severity Prediction Optimization: Feature Combination Study With XGBoost Regression and Satellite-Derived Data***

Pirunthavi Wijikumar (University of Vavuniya, Sri Lanka); Shouthiri Partheepan (Central Queensland University & Eastern University, Australia); Jahan Hassan, Farzad Sanati and Biplob Ray (Central Queensland University, Australia)

Bushfire severity prediction plays a vital role in mitigating the catastrophic effects of bushfires on ecosystems, human life, and property. Accurate prediction models enable timely interventions and informed decision-making, which are crucial for effective fire prevention and response strategies. This study aims to develop an efficient bushfire severity prediction model by leveraging satellite-derived data, specifically from Landsat 8, which includes spectral indices, topographical and climatic features. The primary objective of this study is to assess the impact of different feature combinations on model performance using the XGBoost regression model with dNBR as the target variable. Eighteen tests were conducted, ranging from single-feature indices like NDVI to more complex multi-feature sets. The findings revealed that a 21-feature combination achieved the highest accuracy of 90.09%, with a MSE of 0.0008, a computational time of 1201.86 seconds, and a memory usage of 106.28 MB. However, adding more features did not always result in proportional improvements and often led to increased computational demands. In contrast, tests with fewer features demonstrated that high precision could be achieved with reduced resource consumption, offering a favourable trade-off between performance and efficiency. The results underscore the importance of strategic feature selection and optimization to enhance model accuracy while minimizing computational overhead. This study provides valuable insights for creating effective, high-performance fire severity prediction models, especially in resource-constrained settings.

12:10 ***Implementation of Natural Language UAV Control Using OpenAI's ChatGPT in a Simulated University Environment***

Yulduz Muradova, Jennifer C Amachree and Louis Henry (Georgia State University, USA); Anu G Bourgeois (GSU, USA)

This study looks at how Microsoft AirSim and OpenAI's Natural Language Processing capabilities

may be used to enable drone navigation in a campus simulation. The project uses Unreal Engine to create a 3D simulation of Georgia State University's campus to investigate the use of language-based drone control. Three current technologies are combined in our implementation: (1) Microsoft's AirSim platform for simulating drone physics, (2) OpenAI's ChatGPT API for natural language interpretation and command processing, and (3) a comprehensive campus environment integrated into Unreal Engine. This integration replaces traditional drone control interfaces by allowing users to operate simulated drones through natural language instructions. By converting user commands into drone navigation directions, this technology demonstrates the practical applications of language models. Our findings show that this approach can enhance campus navigation simulations and provide a secure environment for testing drone operations in urban areas. Our study highlights the potential of combining language processing with drone control systems, particularly within educational simulations.

Monday, December 2 12:30 - 1:30 (Australia/Sydney)

B2: Break

Room-Break

Monday, December 2 1:30 - 3:00 (Australia/Sydney)

D2.3: Drone Sense-AI Workshop 2

Room-2

Monday, December 2 1:30 - 3:00 (Australia/Sydney)

S1.2: Network Security-2

Room-1

1:30 *CDCEF: A Cloud-Based Data Volatility & CSP Reliance Eradication Framework*

Pankaj Hariom Sharma and Priyanka Singh (The University of Queensland, Australia)

Cloud computing has become a significant part of people's daily lives over the last decade due to its cost-effective services, such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). As a result, the cloud environment contains a massive amount of sensitive and confidential data, thus becoming a crucial target for attackers. Additionally, cloud forensics over the cloud environment has become complex and difficult due to the cloud's several challenges. These challenges include collecting volatile data, dependency on cloud service providers (CSPs), secure logs storage, and more. This paper proposes a Cloud-Based Data Volatility and CSP Reliance Eradication Framework (CDCEF) to mitigate data volatility and dependency on CSP in cloud forensics in IaaS. We also performed experiments on the Amazon Web Service (AWS) Lightsail - a widely used cloud platform by people globally, based on hypothetical cybercrime scenarios to support our framework. The significant benefits of this framework for investigators are that it allows them to collect volatile data without losing the integrity of the evidence and eradicates CSP reliance. Additionally, the framework provides another benefit of minimizing the usage of forensic tools.

2:00 *5G Slice Mutation to Overcome Distributed Denial of Service Attacks Using Reinforcement Learning*

Amir Javadpour (University of Oulu, Finland); Forough Ja'fari (Sharif University

of Technology, Iran); Tarik Taleb (Ruhr University Bochum, Germany); Chafika Benzaid (University of Oulu, Finland & University of Sciences and Technology Houari Boumediane (USTHB), Algeria)

5G slices are vulnerable to indirect Distributed Denial of Service (DDoS) attacks, by which a flooded traffic is sent toward a target and makes it unavailable. When a DDoS attack is launched against a single slice, the other slices with shared infrastructure with the target are also affected. Most existing mitigation techniques require a detection phase, which is insufficient for unknown and complex attacks. Moving Target Defense (MTD) is a security mechanism that invalidates the adversary's collected information, and it can be deployed without the detection phase. In this paper, we propose a Slice Mutation technique based on Reinforcement Learning (SMRL) that reduces the impact of DDoS attacks on 5G slices while keeping the number of allocated slices acceptable. SMRL proposes a general RL model that considers ternary and ranking numbers to improve learning performance. We tested a new system, SMRL, on computer networks that were attacked by a real botnet called Mirai. We evaluated the system using different measures, including a new way of looking at how the system works. The reported results show that SMRL reduces the number of slices affected by a DDoS attack and improves the distribution of the slices among infrastructure resources by 46% and 20%, respectively.

Presenter bio: Amir Javadpour Biography Amir Javadpour received his MSc degree in 2014 in Medical Information Technology Engineering from University of Tehran, Iran. He is a Ph.D. holder of Computer Science / Mathematics from Guangzhou University, China. His research interests include Cloud computing, Software-Defined Networking (SDN), Big Data, Intrusion detection systems (IDS), the Internet of Things (IoT), Machine Learning. Furthermore, he has published several papers in several domains with his colleagues in highly ranked journals and several ranked conferences. He has been the reviewer for many peer-reviewed journals such as IEEE Transactions, ACM Transactions on Sensor Networks, IEEE Transactions on Mobile Computing, Computer Networks, The Journal of Supercomputing, etc. He also served in academic works such as reviewing IEEE communication magazine, Springer, TPC of several conferences, and so on.

2:30 ***A Zero-Trust Framework Based on Machine Learning for Industrial Internet of Things***

Adel Atieh and Priyadarsi Nanda (University of Technology Sydney, Australia); Manoranjan Mohanty (Carnegie Mellon University, Qatar)

Controlling access to data is essential in ensuring data is only accessed by authorised and trusted users. For these reasons, zero-trust frameworks have been in the centre of interest in the past few years. Zero-Trust frameworks assume that users and systems have been compromised and deal with them as untrusted entities that requires multiple levels of authorisation and security attributes to be compliant in order to be considered trusted. The most used zero trust frameworks use static thresholds to grant levels of access to systems which could introduce false positives and incorrect access privileges to systems/networks. This research paper proposes a machine- learning (ML)-based zero-trust framework that utilises an anomaly detection algorithm. The output of the anomalous detection would inform the observers the trustworthiness of systems in their environments. Moreover, performance, complexity and impact of our proposed scheme is compared against a static threshold zero-trust framework.

Monday, December 2 3:00 - 3:30 (Australia/Sydney)

B3: Break

Room-Break

Monday, December 2 3:30 - 5:00 (Australia/Sydney)

S1.3: Machine Learning and Security

Room-1

3:30 ***A Token-Level Adversarial Example Attack Method for Machine Learning***

Based Malicious URL Detectors

Qisheng Chen and Kazumasa Omote (University of Tsukuba, Japan)

To detect malicious URLs more timely, machine learning based malicious URL detection methods have replaced traditional blacklist methods. These studies aim to improve the accuracy and speed of detection from various aspects such as URL segmentation, URL embedding methods, machine learning models, etc. However, the security issues inherent in these machine learning based malicious URL detection methods have been overlooked. Adversarial example attacks are one of the security issues faced by machine learning based malicious URL detectors. In this paper, we proposed a new adversarial example attack method against malicious URL detection based on machine learning and it has better performance than existing methods. Besides, we compared the robustness of different URL embedding methods and machine learning models with our attack methods and existing attack methods. At last, we analyzed the reasons why our proposed method performs better and the reasons why the context-considered embedding method has high resistance to adversarial example attacks.

4:00 ***Enhancing AI-Generated Image Detection With a Novel Approach and Comparative Analysis***

Stuart Weir, Muhammad Shahbaz Khan and Naghmeh Moradpoor (Edinburgh Napier University, United Kingdom (Great Britain)); Jawad Ahmad (Prince Mohammad Bin Fahd University, Saudi Arabia)

This study explores advancements in AI-generated image detection, emphasizing the increasing realism of images, including deepfakes, and the need for effective detection methods. Traditional Convolutional Neural Networks (CNNs) have shown success but face limitations in generalization and accuracy, particularly with newer technologies like Diffusion Models. With the evolution of AI image generation models, from CNNs to Generative Adversarial Networks (GANs) and Diffusion Models, detecting synthetic images has become more challenging. Issues include dataset diversity, adversarial attacks, and inconsistencies in pre-processing methods. While state-of-the-art models like CNNs, Vision Transformers (ViTs), and hybrid approaches exist, their accuracy in detecting increasingly sophisticated fake images remains suboptimal. This research proposes a novel hybrid detection model combining CNNs and ViTs with an additional attention mechanism layer. This structure aims to improve the interaction between local and global features, enhancing detection accuracy. The model was trained using the CIFAKE dataset, which contains 120,000 real and AI-generated images. The added attention mechanism enhances feature extraction, addressing limitations in existing models when faced with next generation synthetic images. The hybrid CNN/ViT+Attention model demonstrated improved detection accuracy, achieving 99.77%, surpassing previous methods. This research lays a foundation for stronger AI-generated image detection, helping to mitigate the risks of synthetic image fraud.

4:30 ***Experimental Study on Impact of Appliance ID-Based Normalization on SimDataset for Anomalous Power Consumption Classification***

Rajesh Nayak (National Institute of Technology Karnataka Surathkal, India); Jaidhar CD (National Institute of Technology, India)

In terms of annual worldwide energy consumption, buildings use more energy than any other sector. Enhancing buildings' energy efficiency and ensuring security of the appliances requires identifying abnormal power usage. Identifying anomalous power usage is essential for energy conservation. This study suggests an experimental analysis of SimDataset used for detecting micro-moment-based abnormal power usage. Five machine learning-based classifiers-Random Forest (RF), Support Vector Machine (SVM), K Nearest Neighbors (KNN), Naive Bayes (NB), and Decision Tree (DT)-are used to detect unusual consumption of electricity. The SimDataset has undergone binary and multi-class classification. Effect on the performance of the classifiers after the inclusion of new features is examined. Computational complexity of the classifiers is also analyzed. Experimental results showed, the binary and multi-class classification using the RF model with the original dataset, with Min-Max Normalized Power feature and Appliance Id-based Normalized Power feature, produced identical and maximum accuracy, precision, recall, and F1-Score.

Monday, December 2 3:30 - 5:00 (Australia/Sydney)

S2.3: Application Security 1

Room-2

3:30 *ECG-PPS: Privacy Preserving Disease Diagnosis and Monitoring System for Real-Time ECG Signals*

Beyazit B Yuksel and Ayşe Yılmazer-Metin (Istanbul Technical University, Turkey)

This study introduces the development of a stateof-the-art, real-time ECG monitoring and analysis system, incorporating cutting-edge medical technology and innovative data security measures. Our system performs three distinct functions: real-time ECG monitoring and disease detection, encrypted storage and synchronized visualization, and statistical analysis on encrypted data. At its core, the system uses a three-lead ECG preamplifier connected through a serial port to capture, display, and record real-time ECG data. These signals are securely stored in the cloud using robust encryption methods. Authorized medical personnel can access and decrypt this data on their computers, with AES encryption ensuring synchronized real-time data tracking and visualization. Furthermore, the system performs statistical operations on the ECG data stored in the cloud without decrypting it, using Fully Homomorphic Encryption (FHE). This enables privacypreserving data analysis while ensuring the security and confidentiality of patient information. By integrating these independent functions, our system significantly enhances the security and efficiency of health monitoring. It supports critical tasks such as disease detection, patient monitoring, and preliminary intervention, all while upholding stringent data privacy standards. We provided detailed discussions on the system's architecture, hardware configuration, software implementation, and clinical performance. The results highlight the potential of this system to improve patient care through secure and efficient ECG monitoring and analysis. This work represents a significant leap forward in medical technology. By incorporating FHE into both data transmission and storage processes, we ensure continuous encryption of data throughout its lifecycle while enabling real-time disease diagnosis. Our entire architecture is available as open-source, encouraging further research and development in this vital field.

3:52 *Demystifying Trajectory Recovery From Ash: An Open-Source Evaluation and Enhancement*

Nicholas D'Silva, Toran Shahi, Øyvind T. D. Husveg and Adith Sanjeeve (University of New South Wales, Australia); Erik Buchholz (University of New South Wales, CSIRO's Data61, Cyber Security CRC, Australia); Salil S Kanhere (University of New South Wales, Australia)

Once analysed, location trajectories can provide valuable insights beneficial to various applications, including urban planning, market analysis, and public health surveillance. However, such data is also highly sensitive, rendering them susceptible to privacy risks in the event of mismanagement, for example, revealing an individual's identity, home address, or political affiliations. Hence, ensuring that privacy is preserved for this data is a priority. One commonly taken measure to mitigate this concern is aggregation. Previous work by Xu et al. in [Trajectory Recovery From Ash: User Privacy Is NOT Preserved in Aggregated Mobility Data (2017)] shows that trajectories are still recoverable from anonymised and aggregated datasets. However, the study lacks implementation details, obfuscating the mechanisms of the attack. Additionally, the attack was evaluated on commercial non-public datasets, rendering the results and subsequent claims unverifiable. This study reimplements the trajectory recovery attack from scratch and evaluates it on two open-source datasets, detailing the preprocessing steps and implementation. Results confirm that privacy leakage still exists despite common anonymisation and aggregation methods but also indicate that the initial accuracy claims may have been overly ambitious. We release all code as open-source to ensure the results are entirely reproducible and, therefore, verifiable. Moreover, we propose a stronger attack by designing a series of enhancements to the baseline attack. These enhancements yield higher accuracies by up to 16%, providing an improved benchmark for future research in trajectory recovery methods. Our improvements also enable online execution of the attack, allowing partial attacks on larger datasets previously considered unprocessable, thereby furthering the extent of privacy leakage. The findings emphasise the importance of using strong privacy-preserving mechanisms when releasing aggregated mobility data and not solely relying on aggregation as a

means of anonymisation.

4:15 ***Mathematical Models of Security Information Systems Based on the Generalized Multiplicative Knapsacks***

Valeriy Osipyan, Eman Algarib, Arseniy Sergeevich Zhuck and Kirill Litvinov (Kuban State University, Russia)

This paper shows the objective necessity of improving the security information systems (SIS) under the development of information and telecommunication technologies. In contrast to existing multiplicative knapsack security information systems based on standard (binary) multiplicative knapsacks KMS, this work, first of all, is about generalization of classic multiplicative knapsack problem to KMG, and, secondly, in the work, mathematical models MMG of security information systems, based on the generalized multiplicative knapsacks AMG, are offered. Necessary and sufficient conditions at which generalized multiplicative knapsack vector is injective over Zp, p≥2 is established.

4:37 ***Incident Response Adaptive Metrics Framework***

Muntathar Abid and Priyadarsi Nanda (University of Technology Sydney, Australia); Manoranjan Mohanty (Carnegie Mellon University, Qatar)

This paper introduces a novel, multi-dimensional approach to address the evolving challenges in cybersecurity incident response. Our proposed framework uniquely integrates adaptive metrics with a layered security model, providing organisations with a dynamic and context-sensitive tool for building robust response capabilities. We present an innovative integration of proactive threat hunting, real-time threat intelligence, and AI/ML analysis within a cohesive, adaptable structure-a combination not previously explored in incident response literature. This approach not only serves as a comprehensive baseline for managing and responding to incidents but also offers a comparative measure for organisations to continuously evaluate and enhance their cybersecurity postures. Through practical implementation scenarios and future prospects analysis, we demonstrate the framework's unique ability to adapt to the rapidly changing digital landscape, addressing critical gaps in current incident response strategies.

Tuesday, December 3

Tuesday, December 3 9:00 - 9:45 (Australia/Sydney)

K3: Keynote 3

Establishing Trustworthy Data Sharing and Use Frameworks

Dr. Ian Oppermann, University of Technology Sydney

Room-1

Abstract: Data is the lifeblood of the modern economy. It impacts, enables and personalises how we work, play and engage socially and is also crucial for the operation of government and the economy. Banks and financial services companies can be described as data and digital services organisations with some bricks and mortar operations. Value comes from creating, using, protecting and sharing data. Use of data is a very wide and vague topic, incorporating analysis, storage, aggregation, dissemination and deletion. The value of data is unleashed through sharing. The challenge within any sharing or use relationship is "can I trust the data or data product you have tried to share with me?". When that data product is a chart or an analytical insight, it is easier to apply tests on source of origin, governance and methods of analysis. When the data product is the output of complex AI systems, there is little in the way of frameworks to test the image, video, voice message or other generated result. This keynote seeks to outline frameworks which help answer important questions about data and products derived from data: How can I determine if data is fit for the purposes, I plan to use it for? How can I provide guidance / restrictions / prohibitions for future

uses of the products I create from this data? How can I enforce restrictions / prohibitions for future uses of the products I create from data? How can I determine if a data product has been manipulated in ways that I did not expect?

Bio: Dr Ian Oppermann is a Digital Economy thought leader, a highly-cited researcher, and a regular speaker about big data, broadband enabled services and the impact of technology on society. Ian is an Associate Industry Professor in the Faculty of Engineering & IT at UTS and the co-founder of ServiceGen. From 2015 to 2023, Ian was the NSW Government's Chief Data Scientist working within the Department of Customer Service, where he chaired the 11-member NSW Artificial Intelligence Advisory Committee that is advising the State Government on how it should use the technology. The committee also developed a world-first AI assurance framework for government projects. Ian has nearly 30 years' experience in the Information and Communication Technology sector and has led large organizations that deliver products and services that have reached millions of people around the world. He has held senior management roles in Europe and Australia, including Director for Radio Access Performance at Nokia, Global Head of Sales Partnering (network software) at Nokia Siemens Networks, and Divisional Chief and Flagship Director at the CSIRO. He has contributed to six books and co-authored more than 120 papers, which have been cited more than 4000 times. Ian is a Fellow of the Institute of Engineers Australia, the IEEE, the NSW Royal Society, the Australian Academy of Technological Sciences and Engineering, and is a Fellow and past President of the Australian Computer Society. He is also a graduate member of the Australian Institute of Company Directors, president of the Australia National Committee of the IEC, and president of the JTC1 strategic advisory committee in Australia.

Ian has an MBA from the University of London and a PhD in Mobile Telecommunications from the University of Sydney.

Tuesday, December 3 9:45 - 10:30 (Australia/Sydney)

K4: Keynote 4

Election verification for computer scientists

Dr. Vanessa Teague, CEO, Thinking Cybersecurity Pty. Ltd

Room-1

Abstract: In this talk we will discuss some good ideas for election verification and evidence, as well as some recent examples of practical failures. We'll discuss the state of election security in Australia, and possibly the USA, and think about what technologists can do to improve the situation.

Bio: Dr Vanessa Teague is an Associate Professor (Adjunct.) at the ANU College of Engineering, Computing and Cybernetics. Dr Teague is a cryptographer living and working on Wurundjeri land in southeastern Australia (near Melbourne). She is interested in cryptographic protocols that support a free and democratic society. She works on openly-available research and open-source software for supporting democratic decision making and empowering ordinary people to make choices about their own data. Dr Teague's research focuses primarily on cryptographic methods for achieving security and privacy, particularly for issues of public interest such as election integrity and the protection of government data. She was part of the team (with Chris Culnane and Ben Rubinstein) who discovered the easy re-identification of doctors and patients in the Medicare/PBS open dataset released by the Australian Department of Health. Joint work with Andrew Conway has identified several errors in deployed official Australian STV vote counting software, most of which was corrected as a consequence. She has co-designed numerous protocols for improved election integrity in e-voting systems, and co-discovered serious weaknesses in the cryptography of deployed e-voting systems in New South Wales, Western Australia and Switzerland.

Tuesday, December 3 10:30 - 11:00 (Australia/Sydney)

B4: Break

Room-Break

Tuesday, December 3 11:00 - 12:30 (Australia/Sydney)

S1.4: Security and AI-1

Room-1

11:00 ***FakeFaceDiscriminator: Discrimination of AI-Synthesized Fake Faces***

Xufeng Liu and Hoan Quoc Vu (University of Queensland, Australia); Priyanka Singh (The University of Queensland, Australia)

In recent years, the rapid improvement of deep learning technologies, particularly Generative Adversarial Networks, has led to the proliferation of high-quality synthetic facial images and videos, commonly known as deepfakes. This study aims to evaluate and compare the performance of three prominent deep learning models - ResNet, EfficientNet, and Xception - in detecting synthetic faces. Using the Deepfake Detection Challenge and FaceForensics++ datasets, we systematically assess each model's capability to handle diverse and challenging scenarios, including blurred and dark images. Data augmentation techniques, such as random blurring, brightness adjustment, and contrast enhancement, were employed to improve the models' robustness. Additionally, we applied model-specific optimizations, including the integration of Squeeze-and-Excitation blocks in ResNet, compound scaling in EfficientNet, and multi-scale feature fusion in Xception. These enhancements significantly improved the models' accuracy and resilience against low-quality synthetic data. Our results indicate that EfficientNet and Xception outperform ResNet in both general and adverse conditions, with EfficientNet excelling in high-resolution image processing and Xception showing superior performance in fine-grained feature extraction. Furthermore, the introduction of pre-trained weights, multitask learning frameworks, and dynamic learning rate adjustments during training contributed to the models' enhanced performance.

11:22 ***Prompt Engineering Adversarial Attack Against Image Captioning Models***

Hiep K Vo and Shui Yu (University of Technology Sydney, Australia); Xi Zheng (Macquarie University & School of Computing, Australia)

This work presents a highly effective strategy for attacking image captioning models through the use of prompt engineering. The objective of this approach is to deliberately guiding the output of LLMs and introduce dynamic noise into the original clean image captions, causing them to be categorized as a different class. Consequently, when the image captioning model is fine-tuned using adversarial captions, it will deteriorate and produce inaccurate captions for clean photos. The novelty of this attack is that it does not require the attacker to perform any model training and only require to prompt the LLMs to generate only a small amount of captions for the attack to be effective. Comprehensive experiments using GPT-3.5 indicate that with only 100 captions created by LLMs with malicious intent can significantly worsen picture captioning model performance by up to over 50% in BLEU metric and over 25% in ROUGE-L and METEOR scores.

11:45 ***Adversarial Attack Vectors Against Near-Real-Time AI xApps in the Open RAN***

Azadeh Arnaz (University of Technology, Sydney, Australia); Justin Lipman (University of Technology, Sydney (UTS), Australia); Mehran Abolhasan (University of Technology Sydney, Australia)

Ultra-Reliable Low Latency Communications (URLLC) and OpenRAN are transforming wireless telecommunications. However, concerns regarding security pose significant challenges to their widespread adoption. This paper conducts a series of systematic experiments to uncover hidden vulnerabilities such as performance degradation, potential impact on Quality of Service (QoS) or Quality of Experience (QoE). The experiments are designed to carry out strategic attacks on a Handover AI xApp using four different methods, each with its own unique attack strategy. Our research demonstrates that current policies are inadequate, as URLLC xApps are vulnerable to various types of attacks. This highlights the potential for malicious actors to carry out strategic attacks.

12:07 ***Leveraging BERT and AraBERT With Bi-LSTM and Attention for Cross-Lingual Sentiment Analysis***

Wael G Jefry (University Of Technology Sydney, Australia); Faris AL-Doghman and Farookh Khadeer Hussain (University of Technology Sydney, Australia)

Cross-lingual sentiment analysis has developed as a significant area of research in linguistics, especially for languages having diverse syntactic and morphological structures. The objective of this study emphasizes on creating a sophisticated sentiment analysis model that connects English and Arabic datasets, two languages with distinct linguistic problems. Using cutting-edge transformer architectures, we utilize pre-trained models-BERT for English and AraBERT for Arabic-to address the challenges of morphologically rich but resource-limited languages such as Arabic. The foundation of this study is the IMDB movie review dataset, which is similarly structured and large for both languages. To find the best deep learning architecture, we conducted extensive experiments using Long Short-Term Memory (LSTM), Bidirectional LSTM (BiLSTM), and attention methods. While LSTM-based models produced competitive results, transformer-based models that included bidirectional and attention layers outperformed them substantially, particularly on Arabic and English data.

Tuesday, December 3 11:00 - 12:30 (Australia/Sydney)

S2.4: Security and Privacy-1

Room-2

11:00 ***EncPDS: Encrypted Personal Data Stores via Key-Aggregate ID-Based Proxy Re-Encryption***

Kaisei Kajita and Go Ohtake (Japan Broadcasting Corporation, Japan)

Personal data stores (PDSs) are gaining attention as an alternative to the current systems used by tech giants to manage users' data. PDSs centrally manage user logs and data across services and enable data to be passed on to service providers in accordance with the user's own intentions. Using cloud servers to manage personal information is a natural choice from the perspectives of convenience and cost. Therefore, security is highly important in the PDS model. However, to the best of our knowledge, not enough research on encrypting PDS data has been conducted. This is because merely using conventional encryption schemes could compromise the functionality of PDSs. In this study, we developed a key-aggregate identity-based proxy re-encryption (KA-IB-PRE) scheme combining a key-aggregate cryptosystem technique with an identity-based proxy re-encryption scheme. We demonstrated the syntax and specific configuration of KA-IB-PRE and conducted security proofs. Our approach is highly compatible with PDSs, and a system using KA-IB-PRE called EncPDS can construct a privacy-preserving model that meets their requirements. In particular, it offers advantages in privacy protection compared with existing methods, allowing for selective re-encryption of any data through key aggregation while keeping information about which data to re-encrypt hidden from the cloud.

11:18 ***Unsupervised Learning for Insider Threat Prediction: A Behavioral Analysis Approach***

Rahat Mehmood (University of Hertfordshire, Australia); Priyanka Singh (The University of Queensland, Australia); Zoe Jeffrey (University of Hertfordshire, United Kingdom (Great Britain))

Most of the devastating cyber-attacks are caused by insiders with access privileges inside an organization. The main reason of insider attacks being more effective is that they don't have many security barriers before they get into the critical resources of the system. Different machine learning techniques have been previously utilized to identify insider threats within cybersecurity domain whereas research done in predicting insider attacks is not significant. Moreover, machine learning models used for prediction and detection face a critical limitation as they require training on labeled datasets, rendering them less effective for real-time data streams which lack threat presence indicators. This work presents an unsupervised machine learning approach that predicts insider threat using behavior analysis for real-time threat data. Patterns are identified in user behavior, to make predictions about benign and malicious insiders. Features are selected by analyzing activities performed. Selected features are utilized to feed machine learning model which extracts anomalous behavior among users, using anomalies in their activity patterns followed by learning methods for threat detection. A dataset that contains selected features from CERT r4.2 is used to make predictions. The performance of Isolation Forest (iForest) is compared with other algorithms of the same category including One-class SVM, Local Outlier Factor (LOF) and DBSCAN to evaluate the new approach. The iForest shows the best performance accuracy 80 percent and recall 84.2 percent.

11:36 ***Recommendation System Model Ownership Verification via Non-Influential Watermarking***

Xiaocui Dang, Priyadarsi Nanda, Heng Xu and Haiyu Deng (University of Technology Sydney, Australia); Manoranjan Mohanty (Carnegie Mellon University in Qatar, Qatar)

While deep learning-based recommendation systems have achieved great success, recommendation system models are also at serious risk of intellectual property infringement. Current model watermarking research faces significant challenges in terms of fidelity, invisibility, and efficiency. Additionally, existing model watermarking techniques are predominantly applied to image data, with limited applicability to tabular data. In this paper, we introduce an innovative watermarking framework designed to safeguard the ownership of recommendation system models. Specifically, we verify recommendation system model ownership by embedding a type of backdoor watermark into the training dataset, which does not affect model performance. We have conducted experiments on several classical datasets to validate the reliability and effectiveness of our approach.

11:54 ***Critical Behavior Sequence Monitoring for Early Malware Detection***

Tarun Bisht, Sarath Babu and Virendra Singh (Indian Institute of Technology Bombay, India)

The widespread use and the immense user base make Windows systems a prime target for attackers seeking to exploit vulnerabilities and maximize impact. Modern obfuscation techniques enable malware to evade detection tools, allowing it to intrude on systems and carry out malicious activities. Thus, to prevent potential harm to the victim's system, it is crucial to detect malware at the early execution stage and initiate adequate action. However, there is often a trade-off between accuracy and earliness in malware detection, as detecting threats at earlier stages may sometimes come at the cost of reduced detection accuracy. We introduce an early malware detection framework to balance trade accuracy and earliness. Our proposed framework iteratively constructs API call prefix subsequences and applies security-sensitive embedding. The causal sequence encoder transforms these sequences into contextual vectors, which are then classified by a multilayer perceptron. The proposed framework outperforms the state-of-the-art early detection method CTIMD and the early detection method EarlyMalDetect. The proposed framework is able to detect the malicious activity on or before executing 3% of the actual malware sequence.

12:12 ***SMAKAP: Secure Mutual Authentication and Key Agreement Protocol for RFID Systems***

Shayesta Naziri, Xu Wang, Guangsheng Yu, Jian Xu, Sudhir Shrestha and

Christy Jie Liang (University of Technology Sydney, Australia)

Radio Frequency Identification (RFID) is a crucial technology in the Internet of Things (IoT), enabling seamless wireless communication and data exchange. However, these technologies can pose significant security challenges if not implemented with proper attention to security protocols-especially in communication, where pre-shared keys are not used between active tags and readers for device authentication. Some recent authentication protocols rely solely on a hash function, nonce, and single public kay agreement, which can lead to failure to implement robust security and proper authentication or ineffective for high security application environments. To effectively address these challenges this paper proposes a secure Elliptic Curve Cryptography (ECC) based lightweight mutual authentication protocol utilizing a hybrid key agreement protocol between active tag and reader for secure communication in RFID-enabled devices in the IoT environments. The informal analysis demonstrates a secure communication environment for data privacy and flexibility through effective key management.This protocol is adaptable to various applications by addressing specific requirements and limitations.

Tuesday, December 3 12:30 - 1:30 (Australia/Sydney)

B10: Break

Room-Break

Tuesday, December 3 1:30 - 3:00 (Australia/Sydney)

S1.5: Security and AI-2

Room-1

1:30 ***Building Resilient AI: A Solution to Data and Model Poisoning Prevention***

Ghazaleh Keshavarzkalhori (Autonomous University of Barcelona, Spain); Cristina Pérez-Solà (UAB, Spain); Guillermo Navarro-Arribas (Universitat Autonoma de Barcelona, Spain); Jordi Herrera-Joancomarti (Autonomous University of Barcelona, Spain)

In many machine learning scenarios, training occurs outside the control of the model sponsor or the entity using the model. A growing concern in such settings revolves around model poisoning and data poisoning-how training is conducted and which data contributes to the process. This paper introduces a protective scheme against model and data poisoning attacks. Leveraging cryptographic primitives such as hashes, signature schemes, and zero-knowledge proofs, the scheme ensures the integrity of the training process. Hashing maintains the continuity of data from authenticated sensors, while signatures validate the data. In the end, zero-knowledge proofs verify the correct model computation by the entity carrying out the training process. By adopting this approach, model sponsors can securely delegate training tasks, guaranteeing the authenticity of the results. Implementation and testing demonstrate the scheme's feasibility, effectively countering data and model poisoning threats.

1:52 ***Contextualized AI for Cyber Defense: An Automated Survey Using LLMs***

Christoforus Yoga Haryanto (RMIT University & ZipThought Pty Ltd, Australia); Anne Maria Elvira, Trung Duc Nguyen and Minh Hieu Vu (RMIT University, Australia); Yoshiano Hartanto (University of Technology Sydney, Australia); Emily Lomempow (ZipThought Pty Ltd, Australia); Arathi Arakala (RMIT University, Australia)

This paper surveys the potential of contextualized AI in enhancing cyber defense capabilities, revealing significant research growth from 2015 to 2024. We identify a focus on robustness, reliability, and integration methods, while noting gaps in organizational trust and governance frameworks. Our study employs two LLM-assisted literature survey methodologies: (A) ChatGPT 4

for exploration, and (B) Gemma 2:9b for filtering with Claude 3.5 Sonnet for full-text analysis. We discuss the effectiveness and challenges of using LLMs in academic research, providing insights for future researchers.

2:15 ***Cybersecurity Revolution via Large Language Models and Explainable AI***

Jamshaid Iqbal Janjua (University of Engineering & Technology, Lahore, Pakistan)

Integrating Groundbreaking advancements in AI, like language models, interpretable AI, and machine learning, opens up a world of exciting new possibilities. Machine Learning algorithms hold the potential to enhance threat detection & response. The Evolving face of cybersecurity and Modern cyber threats are complex and well crafted; hence, conventional cybersecurity mechanisms show difficulty in staying relevant. LLMs, especially based on Transformer architecture will noticeably increase the accuracy and speed of detecting threats. Transparency and trust are increased by XAI approaches like SHAP and LIME, which offer facts about ML model predictions. This paper explores the literature that demonstrates the integration between XAI and LLMs in cybersecurity, exemplifying how this trinity of models has the potential to help attenuate errors producing Reduced false positives and improve how we detect threats. Thinking about the possibilities the challenges including performance Explainability trade-offs, the need for common evaluation metrics, and the black-box nature of AI Models, remain in place. Solving these will help to enhance AI-driven solutions in cybersecurity.

2:37 ***Discoverable Hidden Patterns in Water Quality Through AI, LLMs, and Transparent Remote Sensing***

Asif Ahamed (Westcliff University, USA); Jamshaid Iqbal Janjua (University of Engineering & Technology, Lahore, Pakistan)

Clean water is a basic human need and necessary for environmental sustainability, particularly in rural areas with limited supplies of water where basic methods for monitoring water quality are seriously impeded. Combining explainable artificial intelligence (XAI) and large language models (LLMs) with remote sensing offers a possible solution. In this review, we examine an innovative framework that leverages satellite and UAV data to assess water quality through pioneering AI techniques. The proposed framework strongly emphasizes using LLMs for better data processing and Perspective formation, with XAI techniques to ensure trust at both stakeholder level and model visibility. Application of this approach could significantly improve real-time monitoring and notably valuable outcomes to conserve water supplies in resource-constrained environments. The framework is designed to be scalable and flexible to fit the specific environmental context of either rural environments or socioeconomic variables to ensure any water quality-monitoring program remains sustainable over time. This analysis shows how we can combine such emergent technology as AI with remote sensing to tackle large-scale water quality problems and open up new ways of monitoring our precious aquatic resources.

Tuesday, December 3 1:30 - 3:00 (Australia/Sydney)

S2.5: Security and Privacy-2

Room-2

1:30 ***Simulation of Pre-Ransomware Attacks on Active Directory***

En Jie Tan, Kowit Tan, Royce Yu Feng Chong, Xingxing Chen, Yi Ching Tan, Liming Lu and Huaqun Guo (Singapore Institute of Technology, Singapore)

Active Directory is adopted by many organizations today. However, not many know how to securely implement it. This is concerning, particularly with the increasing prevalence of ransomware attacks. A ransomware attack inevitably affects organizations' business operations, data loss, and causes financial loss. Our approach aims to enable analysis of technical routes and behavioral aspects of attackers' "pre-ransomware" actions in an AD network, while taking their capabilities and attack

surfaces into account for realistic scenarios. By integrating simulations of vulnerable AD networks with an SIEM server, we demonstrate how AD attacks are carried out, with the goal of collecting raw data on such attacks for future study for improvement of organizational detection capabilities.

1:48 *The Bell-LaPadula (BLP) Enterprise Security Architecture Model Vs Inference Attacks*

Dominic Ayamga and Priyadarsi Nanda (University of Technology Sydney, Australia); Manoranjan Mohanty (Carnegie Mellon University in Qatar, Qatar)

Protecting information flow, data and assets is paramount to every establishment. Therefore, enterprise security architecture design is essential in achieving this protection as it directly implements enterprise security policies. Existing research revealed that researchers have made little effort to investigate inference security challenges to enterprise security architecture design and to assess how the existing security architecture models fare against inference attacks. It was also discovered that existing security architecture models are too old and susceptible to inference attacks. Hence, this research explores a novel solution for designing effective enterprise security architecture and addressing inference attacks.

2:06 *Performance Evaluation of Quantum-Secure Symmetric Key Agreement*

Amin Rois Sinung Nugroho and Muhammad Ikram (Macquarie University, Australia); Mohamed Ali Kaafar (Macquarie University & Optus Macquarie University Cyber Security Hub, CSIRO Data61, Australia)

Quantum-safe public key exchange protocols face significant challenges, both in hardware-based and software-based approaches. Quantum key distribution, which relies on specialized quantum hardware, presents a significant barrier to widespread adoption due to its high cost and limited scalability. Conversely, software-based solutions using post-quantum algorithms introduce their complications, such as increased resource demands and larger ciphertexts. Furthermore, the security of these post-quantum algorithms remains relatively untested, which has led to the emerging trend of hybrid deployment, combining classical and quantum-resistant techniques to hedge against potential vulnerabilities.

In this work, we address these problems by proposing a novel quantum-safe symmetric key agreement (SKA) protocol that is both lightweight and scalable. Our approach involves a hybrid mechanism, leveraging secret strings distributed through a combination of classical and quantum public key pairs during the initial key exchange. This hybrid approach enhances security by utilizing both quantum-resistant algorithms and classical methods, mitigating the risks associated with the nascent nature of post-quantum cryptography. After the initial key exchange, the protocol completes the process using a quantum-safe AES symmetric key, ensuring both security and efficiency. All communications are securely authenticated over classical TLS, making our solution compatible with existing infrastructure.

The contributions of this work are threefold. \textit{First}, we demonstrate that our protocol incurs minimal performance overhead, with only 99ms for purely quantum SKA and 199ms for the hybrid version, compared to classical SKA protocol. \textit{Second}, our SKA protocol remains robust under various network conditions, including delays, packet losses, and bandwidth variations, maintaining small and consistent overheads. \textit{Third}, we show that our solution is highly scalable, with an overhead of only one second for every additional five concurrent users, and that performance improves significantly with increased computational resources-achieving a 50-60% improvement when scaling from two to four CPUs. Additionally, our security evaluations confirm that the protocol provides consistent and sufficient randomness throughout the key agreement process, ensuring quantum-resistance at every stage.

Presenter bio: Amin is doing MRes and PhD in Cyber Security at Macquarie since January 2024. He has more than 15 years experience in cyber security management, big data processing, and solutions architecting. He has a B.S. in Statistical Computing from Institute of Statistics Jakarta, Indonesia and an M.S. in Computer Science from University of Arkansas, United States. Since July 2024, he is also working part-time at Macquarie: • to support Cyber Range Training Center (CRTC) operation as System Engineer and Security Engineer (https://crtc.mq.edu.au/). • he is also teaching practical classes for Master level Cyber Security courses as Sessional Academics at Macquarie: COMP8320 – Data and Information Security and Privacy, COMP8260 Advanced System and Network Security. On the side, he is also the CEO of PT Data Cerdas Indonesia (https://datacerdas.id/) which offers various technology services. In addition, he is also the CTO of Poddium (https://poddium.com.au/) which offers an AI Powered Storytelling Platform for Authors Community.

2:24 *IRIS-SAFE: Privacy-Preserving Biometric Authentication*

Devi Listiyani and Priyanka Singh (The University of Queensland, Australia)

Biometric authentication systems have become an inseparable part of society. This popularity is owing to the fact that biometric traits are immutable. However, applications using these sensitive biometric traits must treat this crucial information carefully. Otherwise, their leakage can threaten the security and privacy of an individual. This paper proposes a privacy-preserving biometric authentication system based on iris data. In the proposed framework, the homomorphic properties are exploited to process data while it is encrypted. There is no leakage of sensitive data throughout the entire process, even when utilizing the services of third-party cloud service providers (CSPs). Authentication is carried out fully within the encrypted domain. Experiments have been conducted to validate the robustness of the proposed framework. Additionally, the time complexity of the proposed framework is minimized compared to other state-of-the-art approaches.

2:42 *Assessing Perceptual Hash Algorithms for Publicly Evaluatable Framework*

Yaser Saei (Urmia University of Technology, Iran); Jafar Tahmoresnezhad (Urmia University of Technology); Sima Jafarikhah and Hossein Siadati (University of North Carolina Wilmington, USA)

The development of a publicly evaluatable perceptual hash framework enables various applications, including private image search resilient to image alterations. Despite the potential of such a framework, little research has systematically analyzed the performance of various perceptual hash algorithms within it. In this paper, we assess the performance of several leading perceptual hash methods, including aHash, pHash, dHash, wHash, and DCT, across five diverse image datasets, and examine how cryptographic techniques impact the effectiveness of the algorithms.

Tuesday, December 3 3:00 - 3:30 (Australia/Sydney)

B5: Break

Room-Break

Tuesday, December 3 3:30 - 5:00 (Australia/Sydney)

S1.6: IoT & Security

Room-1

3:30 *Enhancing LoRaWAN Security: Protection Against Bit Flipping Attacks in IoT Networks*

Jay Dave and Nikumani Choudhury (BITS Pilani Hyderabad Campus, India); Dantu Havishteja and Katuri Revanth (BITS Pilani, Hyderabad Campus, India)

The prominence of the Internet of Things (IoT) has surged in recent years due to technological advancements, increased connectivity, and the widespread adoption of smart devices. Currently, IoT solutions are pervasive across various sectors, including smart homes, wearable devices, healthcare, transportation, and industrial automation. The Long Range Wide Area Network (LoRaWAN) is a wireless communication protocol designed to provide reliable connection over long distances, spanning many kilometers, using low-power and wide-area networks (LPWANs) often used in IoT applications. However, LoRaWAN is vulnerable to bit-flipping attacks, where transmitted data is intercepted and maliciously altered by flipping specific bits in the message payload. Such attacks have the potential to undermine the trustworthiness and dependability of the system. In this paper, we propose a novel security enhancement for LoRaWAN. Our scheme incorporates a hash digest along with the end device's payload, enabling the application server to detect any malicious alterations in the received content using the hash value. We analyze the security of the proposed scheme against bit-flipping attacks and measure its performance through experiments in a real

testbed. Our observations indicate that the proposed mechanism not only secures communication against these attacks but also incurs minimal overhead in terms of power consumption, transmission overhead, and latency.

3:48 *EV-IRP Manager: An Electric Vehicle Incident Response Playbook Manager and Visualizer Toolkit*

Kerem Alpdag (University of Greenwich, United Kingdom (Great Britain)); Naghmeh Moradpoor (Edinburgh Napier University, United Kingdom (Great Britain)); Ny Hasina Andriambelo (University of Antananarivo, Madagascar); Paul Wooderson (HORIBA MIRA, United Kingdom (Great Britain)); Leandros A. Maglaras (Edinburgh Napier University, United Kingdom (Great Britain))

In the rapidly evolving realm of electric vehicle technology, safeguarding the cybersecurity of both electric vehicles and their charging infrastructure has become fundamental. The integration of electric vehicles and their charging stations into the broader grid introduces complex cybersecurity challenges, necessitating robust incident response strategies. Traditional cybersecurity playbooks often fall short in addressing the unique vulnerabilities associated with electric vehicles and their charging systems. The lack of publicly available community playbooks tailored to these needs leaves the electric vehicle ecosystem vulnerable to cyber threats that could compromise user privacy, vehicle functionality, and grid stability. In response to this, the project undertakes the creation of a foundational playbook for electric vehicle and electric vehicle charging station incident response, addressing a significant void in current cybersecurity practices. This paper introduces a Playbook Manager and Visualizer application, called EV-IRP, designed to enable users to upload, manage, and visualize electric vehicle and electric vehicle charging station incident response playbooks efficiently. Utilizing Python, Tkinter for GUI development, SQLite for database management, and Graphviz for visualization, the application facilitates a dynamic and responsive approach to maintaining upto- date incident response strategies. The application is expected to streamline the management of incident response playbooks through procedure visualization, enhancing the cybersecurity posture of electric vehicle infrastructure. By converting textual playbook procedures into easily understandable diagrams, it facilitates a clearer understanding of response steps among users, thereby enhancing the overall efficiency and efficacy of incident response practices. Additionally, the research and development process, informed by a comprehensive literature review, contributes to the academic and practical understanding of cybersecurity best practices for electric vehicle technologies.

4:06 *Comparative Analysis of Intrusion Detection Schemes in Internet of Things(IoT) Based Applications*

Farag El Zegil (University of Technology, Sydney, Australia); Priyadarsi Nanda (University of Technology Sydney, Australia); Manoranjan Mohanty (Carnegie Mellon University, Qatar); Majed Alzahrani (University of Technology, Sydney Australia, Australia)

Due to massive growth in IoT devices in recent years, security of these devices is a major concern. IoT applications span across a number of fields including but not limited to smart cities, intelligent agriculture systems, and the innovative industry. Despite its benefits, cybersecurity challenges have increased significantly in IoT environments. The lack of resource capacity and sophisticated security measurement exposes IoT devices to large number of recent attacks. A strong intrusion detection system (IDS) is the best way to secure IoT devices. Various studies have shown that the current IDS fails to detect modern malware in IoT environments. Some datasets do not have complex scenarios of attack. There are limitations of current datasets, or heterogeneous data of the IoT environment, such as KDD99, NLS_KDD, and UNSW_NB15. In addition, these datasets do not include an operating system and network monitoring audits. This paper comprehensively compares five machine-learning models on the recent EDGE-IIoT dataset. We examine these machine learning methods on Binary and Multiclass class IDS and the security challenges in managing current and future attacks in an IoT environment.

4:24 *A Lightweight Hybrid Signcryption Scheme for Smart Devices*

Lanlan Pan (University of Science and Technology of China, China); Ruonan

Qiu and Minghui Yang (Guangdong OPPO Mobile Telecommunications Corp. Ltd., China)

With the widespread of smart devices, a massive number of messages are sent through message applications every day. Currently, most message applications have been designed for single-receiver and group-receiver scenarios. Moreover, the sender device may send messages to multiple-receiver devices selected from the group device set. In this paper, we propose a lightweight hybrid signcryption scheme supporting the single-receiver and multiple-receiver scenarios, which are compatible with the group-receiver scenario. The formal verification results show that our scheme can offer confidentiality and authentication and is resistant to key-compromise impersonation (KCI) attacks. The evaluation results show that it provides an efficient solution with lower compute time and smaller payload size, which is suitable for lightweight message delivery.

Presenter bio: Lanlan Pan is a cybersecurity expert with a Master's degree in Information Security from University of Science and Technology of China. She is currently serving as cybersecurity expert at Shenzhen Kaihong Digital Industry Development Co., Ltd. Corporation, focuses on ensuring the security of the OpenHarmony operating system. Her research interests span critical areas of cybersecurity, including mobile security, automotive security, cryptographic protocols, and broader cybersecurity challenges.

4:42 ***Towards Weaknesses and Attack Patterns Prediction for IoT Devices***

Carlos Alberto Rivera Alvarez and Arash Shaghaghi (UNSW Sydney, Australia); Gustavo Batista (University of New South Wales, Australia); Salil S Kanhere (UNSW Sydney, Australia)

As the adoption of Internet of Things (IoT) devices continues to rise in enterprise environments, the need for effective and efficient security measures becomes increasingly critical. This paper presents a cost-efficient platform to facilitate the pre-deployment security checks of IoT devices by predicting potential weaknesses and associated attack patterns. The platform employs a Bidirectional Long Short-Term Memory (Bi-LSTM) network to analyse device-related textual data and predict weaknesses. At the same time, a Gradient Boosting Machine (GBM) model predicts likely attack patterns that could exploit these weaknesses. When evaluated on a dataset curated from the National Vulnerability Database (NVD) and publicly accessible IoT data sources, the system demonstrates high accuracy and reliability. The dataset created for this solution is publicly accessible.

Tuesday, December 3 3:30 - 5:00 (Australia/Sydney)

S2.6: Block-Chain and Security

Room-2

3:30 ***A Secure Contact Tracing Method Using Blockchain for Criminal Investigation***

Mizuki Tsuchida and Kazumasa Omote (University of Tsukuba, Japan)

The global outbreak of new coronavirus infections has increased the demand for smartphone-based contact tracing. In particular, much research has been conducted on contact tracing using blockchain, which is decentralized and hard to tamper with data. However, contact tracing requires the centralized collection of information for tracing users, and this essence remains the same even when using blockchain. In this study, we propose a blockchain-based contact tracing method that mitigates the centralized information collection and considers user privacy so that the administrator cannot trace the information. In this scheme, only the application knows the wallet address corresponding to the user, so even the trust authority cannot determine the user's identity from the wallet address. This method is capable of notifying users who may be witnesses at a crime scene by using smart contracts. Users can also prove their innocence if suspected of a crime. Furthermore, we will demonstrate the effectiveness of this method by conducting a demonstration experiment using an Ethereum testnet and two smartphones.

3:48 ***A Blockchain-Based System for Dynamic Redundancy in IoT***

Communications

Liang Liu and Kazumasa Omote (University of Tsukuba, Japan)

The rapid growth and widespread application of Internet of Things (IoT) devices have resulted in a significant increase in the demand for data transmission. However, IoT devices often operate in unstable environments and are constrained by their limited computing and communication capabilities, which makes stable and reliable data transmission a major challenge. Due to the diversity and complexity of IoT platforms, existing systems struggle to provide flexible and scalable solutions. To address these issues, we propose a system based on blockchain and smart contracts that enhances data transmission redundancy by integrating external collaborative devices, thereby ensuring both transmission stability and security. The proposed system achieves efficient identity verification through the use of certificates and smart contracts, while also promoting the participation of temporary devices through incentive mechanisms. Compared to existing methods, our system not only enhances security but also optimizes resource utilization and reduces operational costs.

4:06 ***Lightweight Blockchain Prototype for Food Supply Chain Management***

Alexey Rusakov and Naghmeh Moradpoor (Edinburgh Napier University, United Kingdom (Great Britain)); Aida Akbarzadeh (Norwegian University of Science and Technology, Norway)

The modern food supply chain often involves multiple layers of participants spread across different countries and continents. This complex system offers significant benefits to businesses worldwide; however, it also presents several challenges. One major problem is the inability to trace the product flow back to its origin, a critical issue in many industries. Another issue is the lack of trust among supply chain participants. Blockchain technology can help address these and other challenges faced by the supply chain industry. However, it is surprising that, globally, there are still not many examples of the technology's adoption, with most projects remaining in the pilot stage. This paper explores the field of custom blockchain design tailored to specific applications, with a focus on supply chain operations in the food industry. It includes the development of a lightweight yet fully featured Python prototype for a decentralized blockchain system. In addition to common features like block validation and state updates, the prototype includes a newly designed type of transaction tailored specifically for supply chain operations. These transactions eliminate the need for smart contracts, making the system more lightweight compared to general-purpose blockchain platforms such as Ethereum and less prone to security vulnerabilities. The prototype is designed as a public blockchain network, with Proof of Work selected as the consensus algorithm. The novelty of this research work lies in advancing the concept of a custom blockchain solution for the food industry. The key elements of the prototype have been unit tested. The overall evaluation was completed using a Python script that simulates product flow through an example supply chain, allowing product provenance to be determined by tracing the product flow back to its origin.

4:24 ***Enhancing Security and Privacy in Federated Learning for Connected Autonomous Vehicles With Lightweight Blockchain and Binius Zero-Knowledge Proofs***

Ny Hasina Andriambelo (University of Antananarivo, Madagascar); Naghmeh Moradpoor (Edinburgh Napier University, United Kingdom (Great Britain))

This The rise of autonomous vehicles (AVs) brings with it the need for secure and privacy-preserving machine learning models. Federated learning (FL) allows AVs to collaboratively train models while keeping raw data localized. However, traditional FL systems are vulnerable to security threats, including adversarial attacks, data breaches, and dependency on a central aggregator, which can be a single point of failure. To address these concerns, this paper introduces a peer-to-peer decentralized federated learning system that integrates lightweight blockchain technology and Binius Zero-Knowledge Proofs (ZKPs) to enhance security and privacy. In this system, Binius ZKPs ensure that model updates are cryptographically verified without exposing sensitive information, guaranteeing data confidentiality and integrity during the learning process. The lightweight blockchain framework secures the network by creating an immutable, decentralized record of all model updates, thus preventing tampering, fraud, or unauthorized modifications. This decentralized approach eliminates the need for a central aggregator, significantly enhancing system resilience to attacks and making it suitable for dynamic environments like AV networks. Additionally, the system's design includes Byzantine resilience, providing protection against adversarial nodes and ensuring that the global model aggregation process remains robust even in the presence of malicious actors. Extensive performance evaluations demonstrate that the system achieves low-latency, scalability,

and efficient resource usage while maintaining strong security and privacy guarantees, making it an ideal solution for real-time federated learning in autonomous vehicle networks. The proposed framework not only ensures privacy but also fosters trust among participants in a fully decentralized environment.

4:42 *Secure Communication for MUM-T: a Blockchain and Lightweight Cryptography Framework*

Halimcan Yaşar and Serif Bahtiyar (Istanbul Technical University, Turkey)

Manned-Unmanned Teaming (MUM-T) systems integrate manned aircraft and unmanned aerial vehicles (UAVs) to enhance mission effectiveness, allowing a single pilot to coordinate multiple UAVs for tasks like reconnaissance, communication, and targeting. However, the complexity and operational demands of MUM-T systems introduce significant security challenges, particularly for mission-critical data integrity and real-time communication. In this paper, we propose a new framework for adaptive blockchain cryptography that combines Proof of Authority (PoA)-based blockchain with XOR-based lightweight authentication. The blockchain component, with the manned aircraft that serves as the sole validator, ensures tamper-resistant logging of key mission data. Additionally, it supports accountability and traceability through an efficient PoA consensus algorithm. In parallel, XOR-based lightweight authentication secures control and telemetry signals with minimal computational overhead that enables low-latency and a real-time communication. Analyses results show that the proposed framework achieves a better transaction throughput with acceptable latency, which meets the stringent security and performance requirements of MUM-T operations. The proposed framework offers a scalable and resilient solution for secure communications in complex military environments.

Wednesday, December 4

Wednesday, December 4 9:45 - 10:30 (Australia/Sydney)

K5: Keynote 5

Cloud Computing Security: Past, Present and Future

Professor Willy Susilo, University of Wollongong

Room-1

Abstract: Cloud computing is considered as one of the most prominent paradigms in the information technology industry, since it can significantly reduce the costs of hardware and software resources in computing infrastructure. This convenience has enabled corporations to efficiently use cloud storage as a mechanism to share data and cloud computing as a mechanism to outsource computing. One of the most important works in the area of cloud computing is how to provide security protections. The work in the cryptography literature has been very rich in this area, as it has been studied in the past two decades. In this lecture, we will revisit the topics that researchers have been studying. Specifically, we will provide an overview on what research topic that was studied, and currently being studied in the literature. We provide a comprehensive understanding of cloud computing research based on the published papers spanning from 2007 to 2023. Furthermore, we also discuss the gap between theory and the implementation of the proposed solutions.

Bio: Willy Susilo is a Distinguished Professor at the School of Computing and Information Technology, Faculty of Engineering and Information Sciences at the University of Wollongong (UOW), Australia. He holds the most prestigious Australian Laureate Fellowship awarded by the Australian Research Council. He is the director of Institute of Cybersecurity and Cryptology, School of Computing and Information Technology, UOW. Recently, he was awarded the 2024 NSW Premier's Prizes for Science and Engineering due to his research work. He is an IEEE Fellow, an IET Fellow, an ACS Fellow, an AAIA Fellow and an AIIA Fellow. Previously, he was awarded the prestigious Australian Research Council Future Fellowship in

2009. He has published more than 500 papers in journals and conference proceedings in cryptography and network security. In 2016, he was awarded the ``Researcher of the Year'' at UOW, due to his research excellence and contributions. He is the Editor-in-Chief of the Information journal and the Special Content Editor of the Elsevier's Computer Standards and Interfaces. He is also serving as an Associate Editors in several international journals, including IEEE Transactions. He has also served as the program committee member of several international conferences.

Wednesday, December 4 10:30 - 11:00 (Australia/Sydney)

B6: Break

Room-Break

Wednesday, December 4 11:00 - 12:30 (Australia/Sydney)

S1.7: Security & Education

Room-1

11:00 *PATCH: Problem-Based Learning Approach for Teaching Cybersecurity and Ethical Hacking in Community Colleges*

Sajal Bhatia (Sacred Heart University, USA); Saaid Elhadad (Capital Community College, USA); Irfan Ahmed (Virginia Commonwealth University, USA)

Cybersecurity education incorporates a variety of teaching methods such as traditional lectures, lectures combined with hands-on exercises, and concept maps. One of the most well- known instructional methods is the use of lectures supplemented by hands-on activities. However, often these exercises either lack a strong connect with the lecture material or invariably lead students step-by-step in predetermined tasks, thereby hindering critical thinking and problem-solving skills. Hence, the instructional method falls short on providing students with a comprehensive understanding of complex and often associated cybersecurity concepts as encountered in real-world security incidents. The authors propose that a problem-based learning (PBL) approach can effectively address these gaps and improve cybersecurity education learning outcomes. This paper presents an application of PBL approach for teaching cybersecurity and ethical hacking in community colleges that play a crucial role in meeting the demand for cybersecurity professionals, but often face several challenges to effectively introduce cybersecurity concepts in their curriculum. Through this research, an existing course on ethical hacking is redesigned using the PBL pedagogy and offered to community college students. The course involves several PBL modules that are developed to cover all key aspects of ethical hacking and implemented using open-source software's. Each PBL module is based on a real-world cybersecurity incident and mapped to the MITRE ATT&CK framework. An external independent evaluation is conducted to assess the effectiveness of the proposed teaching methodology. Overall, the obtained results positively impact students' critical thinking, problem-solving, and communication skills, along with facilitating their understanding of key cybersecurity concepts. 100% of students reported that they enjoyed the PBL exercises. 75% of the students believed that PBL enhanced their learning of key concepts to a great extent, and remaining 25% believed that their learning of key concepts was somewhat enhanced.

Presenter bio: Dr. Sajal Bhatia is an Associate Professor (Cybersecurity) and Director of Cybersecurity programs within the School of Computing at Sacred Heart University, CT. His primary research interest revolves around Network Security - both in wired and wireless domain, in particular areas such as Distributed Denial-of-Service (DDoS) attacks synthetic traffic generation, critical infrastructure security, and intrusion detection. More recently he has been interested in exploring Intrusion Detection System (IDS) for Industrial Control Systems (ICS) and Cybersecurity Education. Prior to joining Sacred Heart, Sajal worked as Postdoctoral Research Scholar at Fordham University and at the Institute for Software Integrated System at Vanderbilt University. Sajal obtained his PhD from Queensland University of Technology, Brisbane,

Australia in 2013 and holds bachelor's degree in Communication and Computer Engineering awarded by the LNM Institute of Information Technology, India in 2008.

11:22 *Human-AI Collaboration and Cyber Security Training: Learning Analytics Opportunities and Challenges*

Kaie Maennel and Olaf M Maennel (University of Adelaide, Australia)

Cyber security is becoming more complex due to the exponential growth of interconnected systems and the global threat landscape. To mitigate those risks, there is a need for a skilled cyber security workforce that can navigate the complex decision-making in rapidly evolving cyberspace. Artificial intelligence (AI) is very fast adopted into cyber defence operations. However, we can not effectively train human-AI assisted cyber defence operators, without understanding the underlying learning theory and eco-systems. Cyber security exercises (CSXs) are popular teaching methods for cyber-readiness; however, applying learning analytics (LA) methods and AI-based approaches in an exercise design and implementation is still in the early stages. We propose a holistic Human-AI interaction model within the LA and CSX context. The model brings together elements and processes of human-AI interactions, but also cyber ranges, cyber security and LA tools and a wider lense of multimodal learning analytics, exercise life-cycle and overall pedagogical approach taken. We also discuss the opportunities and challenges for LA and AI in the context of cyber security training. We analyse the role of AI from the learning, instruction, and administration lens in cyber security training, specifically in the exercises. We aim to stimulate further discussions on the future of human-AI collaboration and how to enhance cyber security training with novel LA and AI capabilities.

11:45 *Security Situation Awareness Platform*

Charisee Zhi Ling Yip, Tee Kiat Chua, Clarabel Jinghui Teo, Jing Rui Goh, Brandon Jia Le Loo, Huaqun Guo, Liming Lu and Kan Chen (Singapore Institute of Technology, Singapore)

This paper presents the development of a security scoring platform, with the aim of enhancing the organization's defenses against ransomware attacks. The platform features a security score calculator that leverages on a customizable security scoring algorithm that evaluates the adequacy of the organization's security practices and measures, whilst also providing remediation measures for areas of improvement to allow security teams to quickly respond to threats. Users of the platform will also be able to manage assets, past historical scores and export data for comprehensive security assessments. This dual approach of real-time security scoring and predictive anomaly detection could fortify the organization's security posture in the evolving cyber threat landscape and allow for proactive, responsive measures to mitigate risks effectively.

12:07 *Ransomware Insight Analyzer*

Xin Lin Gan, Zhi Ren James Tan, Yu En Bernice Goo, Xin Ling Jocelyn Yeo, Vi Shean Lim, Yan Cong Boo and Huaqun Guo (Singapore Institute of Technology, Singapore)

This paper aims to analyze and provide insights on vulnerabilities being exploited by ransomware attacks. This paper offers users a comprehensive overview of exploited Common Vulnerabilities and Exposures (CVE). Our analysis includes displaying charts on various aspects such as the top ransomware gangs, the most frequently abused CVE IDs, comparative information before and after the year 2021, common attack vectors, and more. Key findings from our research show that the top ransomware gangs include Conti and Cerber. The most exploited CVE IDs are CVE-2021-34473 and CVE-2021-34523, which correspond to the Microsoft Exchange Server Remote Code Execution Vulnerability and the Microsoft Exchange Server Elevation of Privilege Vulnerability, respectively. Additionally, we identified common attack vectors such as network attacks, application attacks, and data breaches, with instance counts of 10,091, 7,087, and 1,115, respectively. These insights provide valuable information for understanding and mitigating ransomware threats.

Wednesday, December 4 11:00 - 12:30

(Australia/Sydney)

S2.7: Cloud

Room-2

11:00 ***Microsegmented Cloud Network Architecture Using Open-Source Tools for a Zero Trust Foundation***

Sunil Arora and John D. Hastings (Dakota State University, USA)

This paper presents a multi-cloud networking architecture built on zero trust principles and micro-segmentation to provide secure connectivity with authentication, authorization, and encryption in transit. The proposed design includes the multi-cloud network to support a wide range of applications and workload use cases, compute resources including containers, virtual machines, and cloud-native services, including IaaS (Infrastructure as a Service (IaaS), PaaS (Platform as a service). Furthermore, open-source tools provide flexibility, agility, and independence from locking to one vendor technology. The paper provides a secure architecture with micro-segmentation and follows zero trust principles to solve multi-fold security and operational challenges.

Presenter bio: Sunil Arora is a cybersecurity researcher and expert with over 18 years of work experience in the finance, healthcare, telecom, and technology services industries. His research interests are cybersecurity architecture, artificial intelligence, technology governance, technology impact on humans, and risk management. Sunil is a passionate cybersecurity advocate and an expert on cloud security, information security advising, secure design and architecture, and risk management. He is the Associate Director of Security Architecture at Humana Inc. while pursuing his PhD in Cyber Defense.

11:45 ***A Novel Biometric-Based Multi-Factor Authentication Protocol for EV Charging Infrastructures***

Akshitha K Subran (Amrita Vishwa Vidhyapeetham, India); Sriram Sankaran (Amrita University, India)

In the realm of modern transportation, Electric Vehicles (EVs) have emerged as a promising solution to address environmental concerns and reduce dependence on fossil fuels. However, the integration of advanced technologies and connectivity features in EVs makes their charging networks vulnerable to various cyber threats and vulnerabilities, potentially compromising their functionality, reliability, and security. In response to these challenges, our research proposes a novel security solution that leverages human biometrics, specifically fingerprint recognition, to safeguard against cyberattacks such as identity theft, man-in-the-middle attacks, and unauthorized access to EV charging stations. We conduct a brute force attack against the proposed Biometric Multi-Factor Authentication (MFA) method as well as the conventional authentication mechanism to demonstrate the reliability of our proposed mechanism. By combining biometric verification with existing authentication methods, our approach aims to strengthen the security of EV charging networks. To evaluate its effectiveness, we conduct a comparative analysis of our proposed method against current authentication techniques, based on certain criteria, such as success rate, time to breach, and power consumption. The conventional method showed a success rate of 35 %, with the initial breach occurring in just 5 seconds, underscoring a significant vulnerability. In contrast, the proposed biometric-based MFA method proved to be resistant to brute-force attack. Our findings demonstrate the feasibility and robustness of our biometric-based solution, offering a promising enhancement to the security framework of EV charging infrastructures.

Wednesday, December 4 12:30 - 1:30 (Australia/Sydney)

B7: Break

Room-Break

Wednesday, December 4 1:30 - 3:00 (Australia/Sydney)

S1.8: Other Topics in Security

Room-1

1:30 ***Exploiting the Vulnerabilities in MAVLink Protocol for UAV Hijacking***

Fei Du and Jinai Ge (Xi'an Jiaotong-Liverpool University, China); Wen Wang (Xi'an Jiaotong - Liverpool University, China); Yuwen Zou (Xi'an Jiaotong-Liverpool University, China); Sang-Yoon Chang (University of Colorado, USA); Wenjun Fan (Xi'an Jiaotong-Liverpool University, China)

The MAVLink protocol serves as the cornerstone for control communications between ground control systems (GCS) and unmanned aerial vehicles (UAVs), facilitating essential control communication. Despite its widespread adoption, the protocol's security mechanisms have raised significant concerns. This work focuses on the design vulnerabilities of the MAVLink protocol v2.0 including the deficiency in message authentication code (MAC) mechanism and lapses in sequence number verification. Also, this research reveals the implementation loopholes (as findings) in the well-known GCS software (Mission Planner) for updating the secret key and in the widely used UAV emulation (ArduPilot) for examining invalid timestamps. This breach paves the way for the injection of malicious messages, culminating in the potential hijacking of the UAV. In response to these issues, we propose several countermeasures including a solution using the public key-based signature. The efficacy of both the attack methods and the countermeasures is validated through a series of experiments conducted within a controlled testbed environment.

Wednesday, December 4 1:30 - 3:00 (Australia/Sydney)

S2.8: Application Security-2

Room-2

1:30 ***Enhancing Phishing Resilience in Academia: The Mediating Role of Anti-Phishing Tools on Student Awareness and Behavior***

Saleh Alqahtani (University of Technology Sydney, Australia & Saudi Electronic University, Saudi Arabia); Priyadarsi Nanda (University of Technology Sydney, Australia)

Phishing attacks are a significant threat to cybersecurity, particularly among university students who are frequent targets due to their extensive online activities and limited cybersecurity awareness. This study explores the impact of various factors, including threat susceptibility, phishing avoidance behavior, and the use of anti-phishing tools, on students' awareness of phishing attacks. Using a quantitative approach, data were collected from 715 university students worldwide through a structured questionnaire. The findings reveal that while students exhibit a moderate level of awareness about phishing attacks, their reliance on anti-phishing tools remains insufficient. The study identifies a significant positive relationship between the use of anti-phishing tools and increased phishing awareness and avoidance behaviors. Additionally, the research highlights the mediating role of anti-phishing tools in enhancing students' cybersecurity awareness. The results underscore the importance of integrating educational programs and advanced anti-phishing tools to improve students' resilience against phishing attacks. Recommendations for enhancing cybersecurity education and practices among university students are also provided.

1:48 ***Dilithium-Based Verifiable Timed Signature Scheme***

Erkan Uslu (ASELSAN Inc., Turkey & Middle East Technical University, Turkey); Oğuz Yayla (Middle East Technical University, Turkey)

Verifiable Timed Signatures (VTS) are cryptographic constructs that enable obtaining a signature at a specific time in the future and provide evidence that the signature is legitimate. This framework

particularly finds utility in applications such as payment channel networks, multiparty signing operations, or multiparty computation, especially within blockchain architectures. Currently, VTS schemes are based on signature algorithms such as BLS signature, Schnorr signature, and ECDSA. These signature algorithms are considered insecure against quantum attacks due to the effect of Shor's Algorithm on the discrete logarithm problem. We present a new VTS scheme called VT-Dilithium based on CRYSTALS-Dilithium Digital Signature Algorithm that has been selected as NIST's quantum-resistant digital signature standard and is considered secure against both classical and quantum attacks. Integrating Dilithium into the VTS scheme is a more challenging problem due to its complex mathematical operations (i.e. polynomial multiplications, rounding operations) and large module parameters such as polynomials, polynomial vectors, and matrices. This work aims to provide a comprehensive exposition of VT-Dilithium scheme.

2:06 *Effects of Personal Characteristics on Phishing Awareness, Anti-Phishing Tool Usage, and Phishing Avoidance Behavior: A Structural Equation Modeling Approach*

Saleh Alqahtani (University of Technology Sydney, Australia & Saudi Electronic University, Saudi Arabia); Priyadarsi Nanda (University of Technology Sydney, Australia)

Phishing attacks are among the most prevalent cyber threats, often leading to financial losses, reputational damage, and personal identity crises. This study investigates university students' behavior towards phishing attacks, focusing on the relationship between phishing Awareness and phishing avoidance behavior. Additionally, it examines the moderating effects of gender, age, and qualification on the use of anti-phishing tools, phishing avoidance behavior, and phishing Awareness. Data were collected from 715 university students through a structured questionnaire employing a quantitative approach. The results revealed a strong positive relationship between students' Awareness of phishing attacks and their phishing avoidance behavior. The mediation analysis showed that phishing awareness significantly mediates the relationship between using anti-phishing tools and phishing avoidance behavior. Furthermore, significant differences were observed in phishing Awareness, avoidance behavior, and the use of anti-phishing tools based on gender and age groups. These findings highlight the importance of tailored cybersecurity education programs considering these demographic factors to enhance students' resilience against phishing attacks. It is recommended to develop targeted cybersecurity education programs that focus on increasing phishing awareness and promoting the use of anti-phishing tools among university students, with particular emphasis on addressing demographic differences. The study's findings suggest that improving phishing awareness and tailoring interventions based on gender, age, and educational background can significantly enhance students' ability to avoid phishing attacks, strengthening cybersecurity resilience.

2:24 *Operational Technologies in Industrial Control System: Cybersecurity Perspectives and Research Trends*

Harshit Gupta (Indian Institute of Information Technology Allahabad India, India & University of Messina, Italy); Luca D'Agati, Francesco Longo and Antonio Puliafito (University of Messina, Italy); Giovanni Merlino (University of Messina & National Interuniversity Consortium for Informatics (CINI), Italy)

Operational technology (OT) and information technology (IT) are the backbones of modern industrial control systems (ICS). The coupling of IT and OT is significant as it provides various benefits that lead to higher manageability, efficiency, and productivity in industries. However, the presence of an IT network leads to cyber-security concerns in the OT networking system. Hence, in the emerging and growing field of Industry 4.0, making the system secure from cyber threats is very important. Therefore, the proposed work presents the multi-directional view of ICS concerning cyber-security by discussing possible cyber vulnerabilities and the methods to deal with cyber threats. It also discusses the various industrial protocols, standards, and ICS design frameworks. Last but not least, the work discusses various tools used for network monitoring, security analysis, and penetration testing.

2:42 *A Novel Framework for Attack Detection and Localization in Smart Cities*

Mehdi Houichi (High School of Communication TUNISIA, Tunisia)

As smart cities evolve, they integrate various applications such as intelligent transportation systems, energy management, healthcare, and public safety, all of which depend on interconnected networks. These applications rely on massive data exchanges between sensors, devices, and cloud services, making the system more efficient but also exposing it to cybersecurity challenges. Cyber threats, including data breaches, denial of service (DoS) attacks, and malware, can disrupt essential services, compromise privacy, and endanger lives. The complexity of smart city infrastructure amplifies vulnerabilities, making real-time detection and localization of attacks a critical necessity. In this paper, we propose a novel framework for attack detection and localization specifically designed for smart city environments. The framework integrates machine learning-based intrusion detection systems (IDS) with packet analysis techniques. Upon detection of an anomaly, detailed packet analysis is performed to extract crucial information, such as IP addresses, GPS coordinates, and other metadata. This enables precise localization of the attack's source, facilitating rapid response and mitigation. The combination of machine learning for anomaly detection with packet-level analysis ensures a comprehensive approach, significantly improving detection accuracy and localization precision. Extensive evaluations on real-world datasets demonstrate the efficacy of the proposed method in enhancing the security of smart city networks, while reducing false positives and improving real-time response capabilities. This framework represents a critical advancement in protecting smart cities from evolving cyber threats.

Wednesday, December 4 3:00 - 3:30 (Australia/Sydney)

C1: Closing Ceremony and Best Paper Awards

Room-1