IoTBDS 2025

10th International Conference on Internet of Things, Big Data and Security

Final Program and Book of Abstracts

Porto, Portugal

6 - 8 April, 2025

https://iotbds.scitevents.org

SPONSORED BY

INSTICC

PAPERS AVAILABLE AT

SCITEPRESS DIGITAL LIBRARY

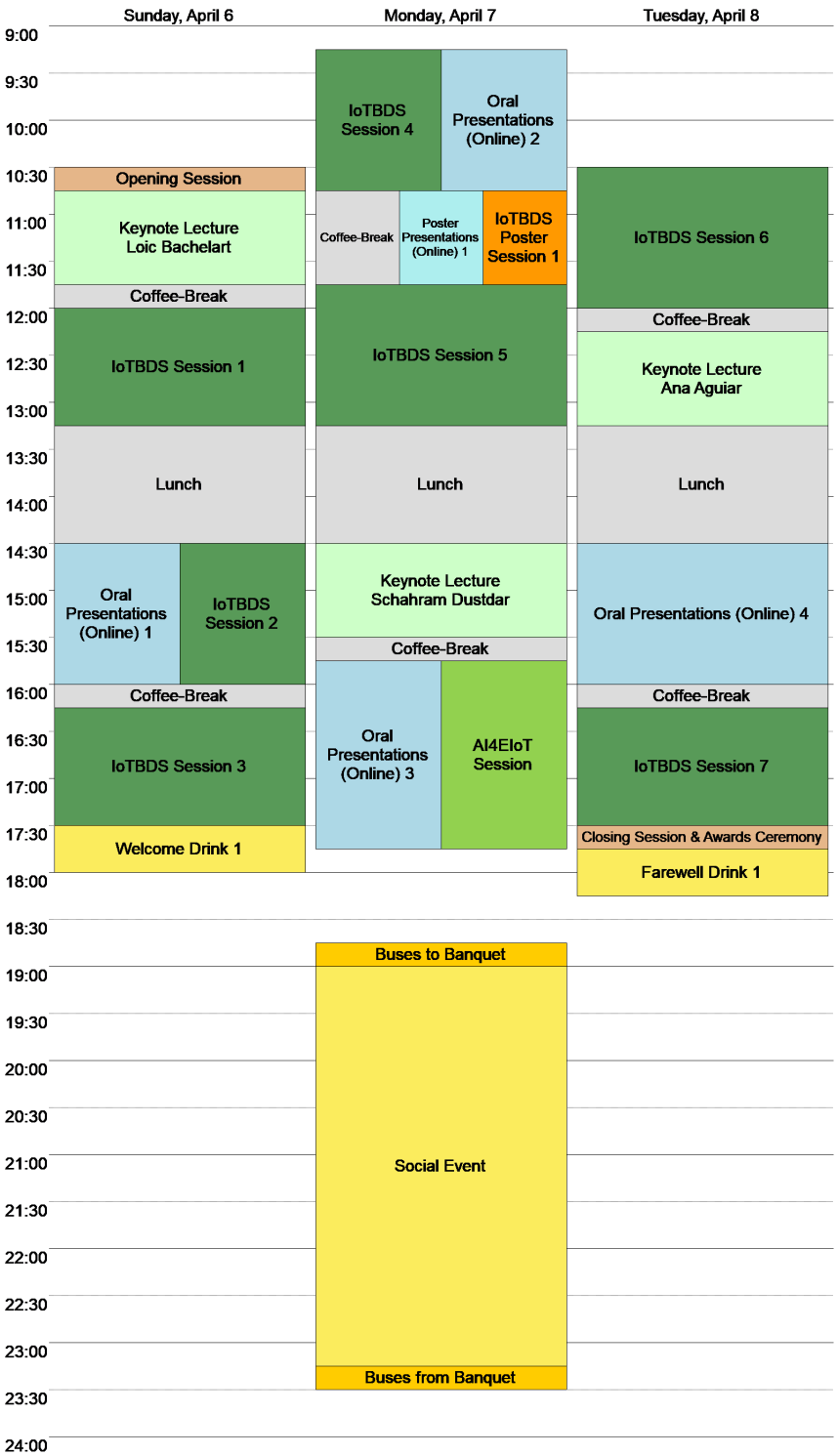
IoTBDS 2025
Final Program and Book of Abstracts

10th International Conference on Internet of Things, Big Data and Security

Porto - Portugal
April 6 - 8, 2025

Sponsored by
INSTICC - Institute for Systems and Technologies of Information, Control and Communication

Program Layout



Final Program and Book of Abstracts

Contents

Sunday Sessions: April 6

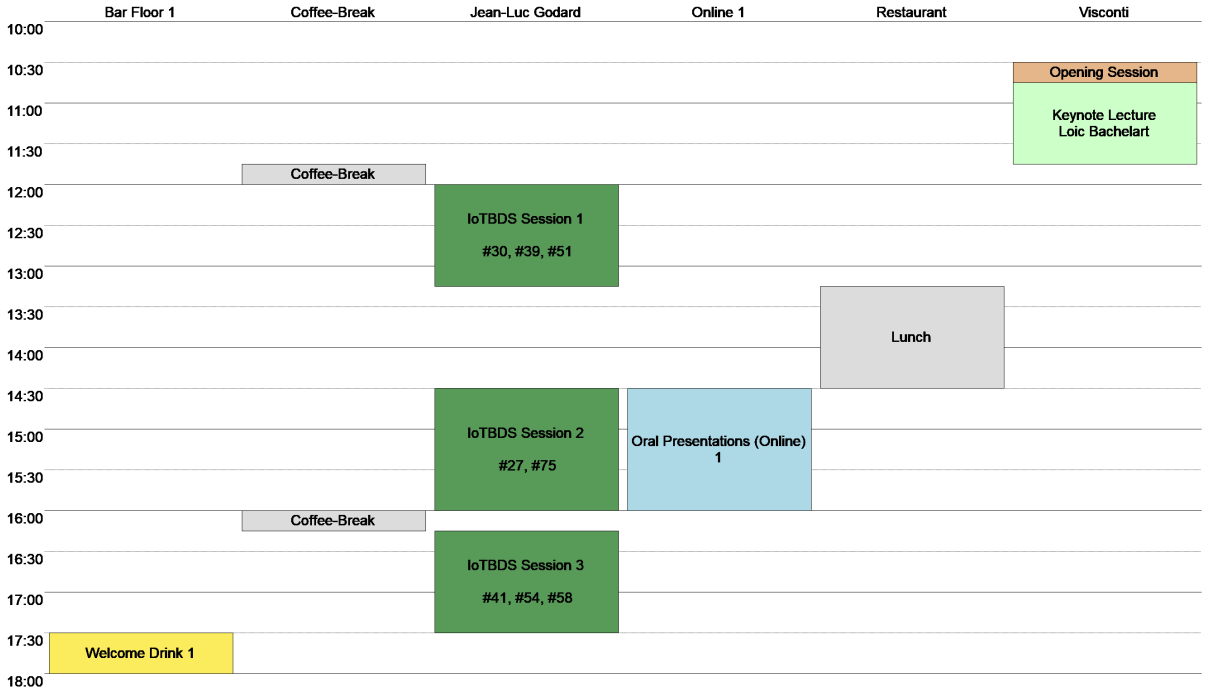
Monday Sessions: April 7

Contents

Tuesday Sessions: April 8

Sunday Sessions: April 6

Sunday Sessions: April 6 Program Layout



Opening Session	IoTBDS
10:30 - 10:45	Room Visconti

Keynote Lecture	IoTBDS
10:45 - 11:45	Room Visconti

Technological Adoption in the Era of Generative AI

Loic Bachelart
Microsoft, France

Abstract: Since ChatGPT became publicly available, each month brings another announcement of the stunning capabilities of generative AI technologies. Now capable of vision, full-duplex conversation, and autonomy with agents, generative AI promises to boost individual productivity, enhance processes, foster innovation in products and services, and therefore transform organizations and industries. However, the gap between the potential of the technology and the value realized by users and organizations has never been so big. And it looks like this gap will continue to grow given the specific challenges of generative AI adoption. By comparing the adoption of generative AI with past disruptive technologies and sharing learnings from real-life adoption engagements, this keynote will focus on the strategies European organizations can implement to harness the power of generative AI to drive innovation, productivity, and growth.

Session 1A	IoTBDS
12:00 - 13:15	Room Jean-Luc Godard
Security, Privacy and Trust	

Complete Paper #39

Information Flow Control for the Internet of Things

Gildas Kouko, Josée Desharnais and Nadia Tawbi
Université Laval, 2325 rue de l'Université, Québec, QC, G1V 0A6, Canada

Keywords: Internet of Things, Information Flow, Reachability Property, Safety Property, Model Checking.

Abstract: The Internet of Things (IoT) refers to devices and applications that interact and connect the physical and digital worlds. Unfortunately, their interactions often lead to information leaks and safety issues. Controlling their autonomous behavior related to events and actions in their environment is therefore important. This is the key to uncovering conflicts between user-defined expectations. To control these conflicts, we propose to verify IoT information-flow according to the principles of model checking. We propose a model based on an abstraction of the information flow induced by device and application operations and interactions in an IoT network. More precisely, the model is independent of any functional and technical heterogeneity. This abstraction is the result of an information flow analysis carried out, a priori, for all the involved devices, as well as for all the applications controlling them. A transition system is constructed from these abstractions enabling us to transform the information flow control into reachability and safety properties verification. We express these properties using a modal logic inspired by Timed Computation Tree Logic (TCTL) (Baier and Katoen, 2008). We illustrate our approach with an example and adapt the language and the model to an existing model checker.

Complete Paper #30

A Technology Review of Zero Knowledge Proof Techniques

Seyed Mohsen Rostamkolaei Motlagh[1], Claus Pahl[1], Hamid Barzegar[1] and Nabil El Ioini[2]
[1] *Free University of Bozen-Bolzano, 39100 Bolzano, Italy*
[2] *University of Nottingham, 43500 Semenyih, Malaysia*

Keywords: ZKP, Authentication, Distributed Systems, Technology Review.

Abstract: Distributed systems, particularly in IoT, require robust privacy-preserving authentication mechanisms to address increasing concerns about data security and integrity. Zero-Knowledge Proofs (ZKPs) have emerged as a promising solution to balance security, privacy, and efficiency. This paper reviews and compares state-of-the-art ZKP protocols, focusing on their suitability for decentralized, resource-constrained environments. We propose a comprehensive evaluation framework and apply it to zk-SNARK, zk-STARK, and Bulletproof protocols, analyzing metrics such as scalability, efficiency, and proof size. Our findings provide actionable insights into the trade-offs between these protocols, offering guidance for their application in IoT systems.

Complete Paper #51

Automating the Assessment of Japanese Cyber-Security Technical Assessment Requirements Using Large Language Models

Kento Hasegawa[1], Yuka Ikegami[2], Seira Hidano[1], Kazuhide Fukushima[1], Kazuo Hashimoto[2] and Nozomu Togawa[2]
[1] *KDDI Research, Inc., 2-1-15, Ohara, Fujimino-shi, Saitama, Japan*
[2] *Waseda University, 3-4-1, Okubo, Shinjuku-ku, Tokyo, Japan*

Keywords: Internet of Things, Security, Large Language Models, Retrieval-Augmented Generation, JC-STAR.

Abstract: Several countries, including the U.S. and European nations, are implementing security assessment programs for IoT devices. Reducing human effort in security assessment has great importance in terms of increasing the efficiency of the assessment process. In this paper, we propose a method of automating the conformance assessment of security requirements based on Japanese program called JC-STAR. The proposed method performs document analysis and device testing. In document analysis, the use of rewrite-retrieve-read and chain of thought within retrieval-augmented generation (RAG) increases the assessment accuracy for documents that have limited detailed descriptions related to security requirements. In device testing, conformance with security requirements is assessed by applying tools and interpreting the results with a large language model. The experimental results show that the proposed method assesses conformance with security requirements with an accuracy of 95% in the best case.

Session 2A **IoTBDS**
14:30 - 16:00 **Room Jean-Luc Godard**
IoT Services and Applications

Complete Paper #27

Real-Time Manufacturing Data Quality: Leveraging Data Profiling and Quality Metrics

Teresa Peixoto[1], Bruno Oliveira[1], Óscar Oliveira[1] and Fillipe Ribeiro[2]

[1] *CIICESI, School of Management and Technology, Porto Polytechnic, Portugal*

[2] *JPM Industry, Portugal*

Keywords: Data Quality, Data Profiling, Real-Time Data Analysis, Smart Manufacturing Environments, Industry 4.0.

Abstract: Ensuring data quality in decision-making is essential, as it directly impacts the reliability of insights and business decisions based on data. Data quality measuring can be resource-intensive, and it is challenging to balance high data quality and operational costs. Data profiling is a fundamental step in ensuring data quality, as it involves thoroughly analyzing data to understand its structure, content, and quality. Data profiling enables teams to assess the state of their data at an early stage, uncovering patterns, anomalies, and inconsistencies that might otherwise go unnoticed. In this paper, we analyze data quality metrics within Industry 4.0 environments, emphasizing various critical aspects of data quality, including accuracy, completeness, consistency, and timeliness, and showing how typical data profiling outputs can be leveraged to monitor and improve data quality. Through a case study, we validate the feasibility of our approach and highlight its potential to improve data-driven decision-making processes in smart manufacturing environments.

Complete Paper #75

EV-Connect: Energy Efficient & Incentive Cost Based Model for Range Anxious EVs with Multi-Hop Socially Assisted V2V Charging

Srishti Sharma and Rahul Thakur

Computer Science and Engineering, Indian Institute of Technology Roorkee, India

Keywords: Electric Vehicle (EV), Vehicle-to-Vehicle (V2V), Social Internet of Vehicles (SIoV), Incentive Cost, Bipartite Matching.

Abstract: With an increasing demand for a sustainable environment, there has been a rapid shift from internal combustion engines (ICEs) to battery-powered engines (BPEs), which are installed in electric vehicles (EVs). With the increasing need and demand for electric vehicles (EVs), the need for charging stations (CS) is also increasing. However, the paradigm shift is slow regarding CSs because of their high installation costs. Thus, there is still the non-ubiquity of CSs in cities, highways, and remote areas, which causes EV users to experience range anxiety. In this context, vehicle-to-vehicle (V2V) charging could be a promising solution recently gaining prominence. In this paper, we have proposed the incentive-based socially connected V2V charging model for EVs where the excess charge of EVs acts as an alternate charging option for other EVs. We have used the maximum bipartite matching algorithm to map the EVs experiencing range anxiety with available CSs and other EVs with surplus charge. The results of our model have shown the trend that the number of EV users who were experiencing range anxiety is less than the only CS-dependent users. Also, the trend of results indicates that there could be a significant reduction of load on the power grid in that particular area, especially during peak hours.

Oral Presentations (Online) 1 **IoTBDS**
14:30 - 16:00 **Room Online 1**
Internet of Things, Big Data and Security

Complete Paper #13

Internet of Things Devices Management for Smart Cities

Nilson Sousa[1,2], George Pinto[1,2] and Cassio Prazeres[1]

[1] *Institute of Computing, Computer Science Department, Federal University of Bahia (UFBA), Salvador, Bahia, Brazil*

[2] *Federal Institute of Bahia, Brazil*

Keywords: Internet of Things, Smart City, Management, Device.

Abstract: In this work, we address the critical challenge of managing IoT devices within Smart City infrastructures. We propose a comprehensive solution tailored to the specific requirements of IoT device management, different from traditional network device management. Our approach integrates hundreds of devices across urban areas, leveraging telecommunications and information technologies (ICT) to improve urban services and citizens' quality of life. We reviewed existing architectures and platforms and developed a prototype to demonstrate the practical application of our solution. Our prototype ensures consistent service availability and efficient resource management. The insights gained from our work provide valuable guidance for future developments and implementations of IoT device management strategies in Smart Cities.

Complete Paper #17

Bridging the Cost Gap: A Comprehensive Analysis of CAPEX and OPEX for Smart Home Transition from a Provider's Perspective

Nilton Seixas, Adriano Maia, George Pinto, Dhyego M. da Cruz, Bruno Santos, Ivan Machado, Eduardo Almeida, Frederico Durao, Maycon Peixoto, Gustavo Figueiredo and Cassio Prazeres

Institute of Computing, Computer Science Department, Federal University of Bahia (UFBA), Salvador, Bahia, Brazil

Keywords: IoT, Smart Homes, Smart Grids, CAPEX, OPEX.

Abstract: The urgency of addressing global warming has driven global efforts to enhance energy efficiency and transform energy acquisition methods. In this context, the adoption of smart technologies has gained relevance across various domains, including smart cities and smart homes. While smart cities are often promoted through government initiatives, transforming conventional homes into smart homes largely depends on consumer adoption. However, there is a significant gap in the literature regarding the implementation costs and benefits of this transition, with many studies focused on unrealistic scenarios tailored to the average American consumer profile. This study aims to fill that gap by proposing a methodology to estimate the conversion of conventional homes into smart homes, accounting for both capital expenditures (CAPEX) and operational expenditures (OPEX). The proposed approach seeks to enable an affordable transition for a wider range of consumer profiles. Four case studies are presented to demonstrate how smart systems can be integrated into homes, maximizing economic and environmental benefits

for end-users. Additionally, the paper analyzes the commercial relationship between manufacturers and smart environment providers, exploring acquisition and operational cost models. As an alternative to the traditional device-based business model, the study suggests a subscription-based system, supported by the continuous delivery of smart solutions, promoting greater customer retention and scalability.

Complete Paper #12

Dynamic Obfuscation for Secure and Efficient Multi-Cloud Business Processes

Amina Nacer[1] and Mohammed Abdmeziem[2]

[1] *M'hamed Bougara University, 35000 Boumerdes, Algeria*

[2] *National School of Computer Science, 16000 Oued Smar, Algiers, Algeria*

Keywords: Business Process, Cloud Computing, Data Obfuscation, Obfuscation Methods, Cost-Effective Solution.

Abstract: Organizations increasingly outsource complex business processes to the cloud, but concerns about exposing business strategies persist. While existing solutions split processes across multiple cloud providers, they don't fully address the risk of information leakage. Our approach leverages random obfuscation techniques at each execution to safeguard sensitive data, offering a lightweight alternative to encryption. In multi-cloud environments, where processes are distributed across providers, obfuscation reduces leakage risks with lower computational overhead, making it ideal for resource-constrained scenarios compared to more expensive cryptographic solutions.

Complete Paper #60

L2C: Learn to Clean Time Series Data

Mayuresh Hooli and Rabi Mahapatra

Texas A&M University, College Station, U.S.A.

Keywords: Data Cleaning, Machine Learning, Time Series Analysis, Outlier Detection, Data Imputation, Internet of Things (IoT), Support Vector Regression (SVR).

Abstract: In today's data-driven economy, where decisions hinge on vast amounts of data from diverse sources such as social media and government agencies, the accuracy of this data is paramount. However, data complexities including errors from missing information and outliers challenge its integrity. To address this, we introduce a novel machine learning framework, L2C (Learn to Clean), specifically designed to enhance the cleanliness of time series data. Unlike existing methods like SVR and ARIMA that are limited to handling one or two types of outliers, L2C integrates techniques from SVR, ARIMA, and Loess to robustly identify and correct for all three major types of outliers—global, contextual, and collective. This paper marks the first implementation of a framework capable of detecting collective outliers in time series data. We demonstrate L2C's effectiveness by applying it to air quality sensor data sampled every 120 seconds from wireless sensors, showcasing superior performance in outlier detection and data integrity enhancement compared to traditional methods like ARIMA and Loess.

Session 3A **IoTBDS**
16:15 - 17:30 **Room Jean-Luc Godard**
Machine Learning & Artificial Intelligence

Complete Paper #41

Smoke Segmentation Improvement Based on Fast Segment Anything Model with YOLOv11 for a Wildfire Monitoring System

Puchit Bunpleng[1], Puthtipong Thunyatada[1], Bhutharit Aksornsuwan[1], Kanokvate Tungpimolrut[2] and Ken Murata[3]

[1] *Sirindhorn International Institute of Technology, Thammasat University, Pathum Thani, Thailand*

[2] *NECTEC, National Science and Technology Development Agency, Pathum Thani, Thailand*

[3] *National Institute of Information and Communications Technology, Tokyo, Japan*

Keywords: Wildfire, Smoke Segmentation, Machine Learning, YOLOv11, FastSAM, Gradient Boosting, Deep Learning.

Abstract: Forests and wildlife are crucial parts of our ecosystem. Wildfires occurring in dry and hot regions represent a significant threat to these areas, particularly in ASEAN countries during the dry season. While human observers are often employed to detect wildfires, their scarcity and limited availability highlight the need for automated solutions. This study explores the use of machine learning, specifically computer vision, to enhance wildfire detection by segmenting smoke, an approach which potentially gives information regarding the size and the direction of the spread of the smoke, aiding mitigation efforts. We extend prior work by proposing a model to predict the errors and performance of segmentation masks without access to the ground truth, with the aim of facilitating iterative self-improvement of segmentation models. The FireSpot dataset is used to fine-tune a YOLOv11 model to predict bounding boxes of smoke successfully; subsequently, the outputs of this model are used as a prompt to refine a FastSAM model designed to segment the image into a proposed mask containing the smoke. The proposed mask and the corresponding original image are then used to train a machine learning model where the targets are metrics regarding the error rates of the masks. The results show that a gradient boosting model achieves good prediction performance in predicting some error metrics like the IoU (denoted TPP in this paper) between the proposed and actual segmentation masks with an MSE of 0.03 and R2 of 0.46, as well as the proportion of false positives over the union of the proposed and actual masks (denoted FPP in our paper) with an MSE of 0.0002 and R2 of 0.95, while a pre-trained deep learning model fails to learn the distribution, achieving considerably lower performance for IoU with an MSE of 0.05 and R2 of 0.06 and FPP with an MSE of 0.0002 and R2 of -1.15. These findings open the way to future work where the results of the error prediction model can be used as feedback to improve the prompts and hyperparameters of the segmentation model.

Complete Paper #54

Generating Realistic Cyber Security Datasets for IoT Networks with Diverse Complex Network Properties

Fouad Al Tfaily[1,2], Zakariya Ghalmane[1], Mortada Termos[1,2], Mohamed-el-Amine Brahmia[1], Ali Jaber[2] and Mourad Zghal[1]

[1] *CESI LINEACT UR 7527, Strasbourg, France*

[2] *Computer Science Department, Faculty of Sciences, Lebanese University, Beirut, Lebanon*

Keywords: Complex Networks, Internet of Things, Artificial Intelligence, Cyber Security, Federated Learning, Network Properties, Intrusion Detection.

Abstract: In the cybersecurity community, finding suitable datasets for evaluating Intrusion Detection Systems (IDS) is a challenge, particularly due to limited diversity in complex network properties. This paper proposes a dual-purpose approach that generates diverse datasets while producing efficient, compact versions that maintain detection accuracy. Our approach employs three techniques - community mixing modification, centrality-based modification, and time-based modification - each targeting specific network property adjustments while achieving significant dataset size reductions (up to 81.5%). Our approach is validated on real-world datasets, including NF-UQ-NIDS, CCD-INID-V1, and TON-IoT, demonstrating its ability to generate realistic datasets while preserving network properties, attack patterns, and structural integrity. The generated datasets exhibit diverse complex network properties, making them particularly useful for IDS technique evaluation that incorporates complex network measures. The reduced size and preserved accuracy (96.4%) make these datasets especially valuable for resource-constrained environments. Moreover, our approach facilitates the construction of homogeneous datasets required for federated learning situations where data distribution similarity across clients is essential. This contribution helps address both dataset scarcity and computational efficiency challenges while ensuring that the generated datasets retain the characteristics of real-world network traffic.

Complete Paper #58

Anomalous IoT Behavior Detection by LSTM-Based Power Waveform Prediction

Ryusei Eda and Nozomu Togawa

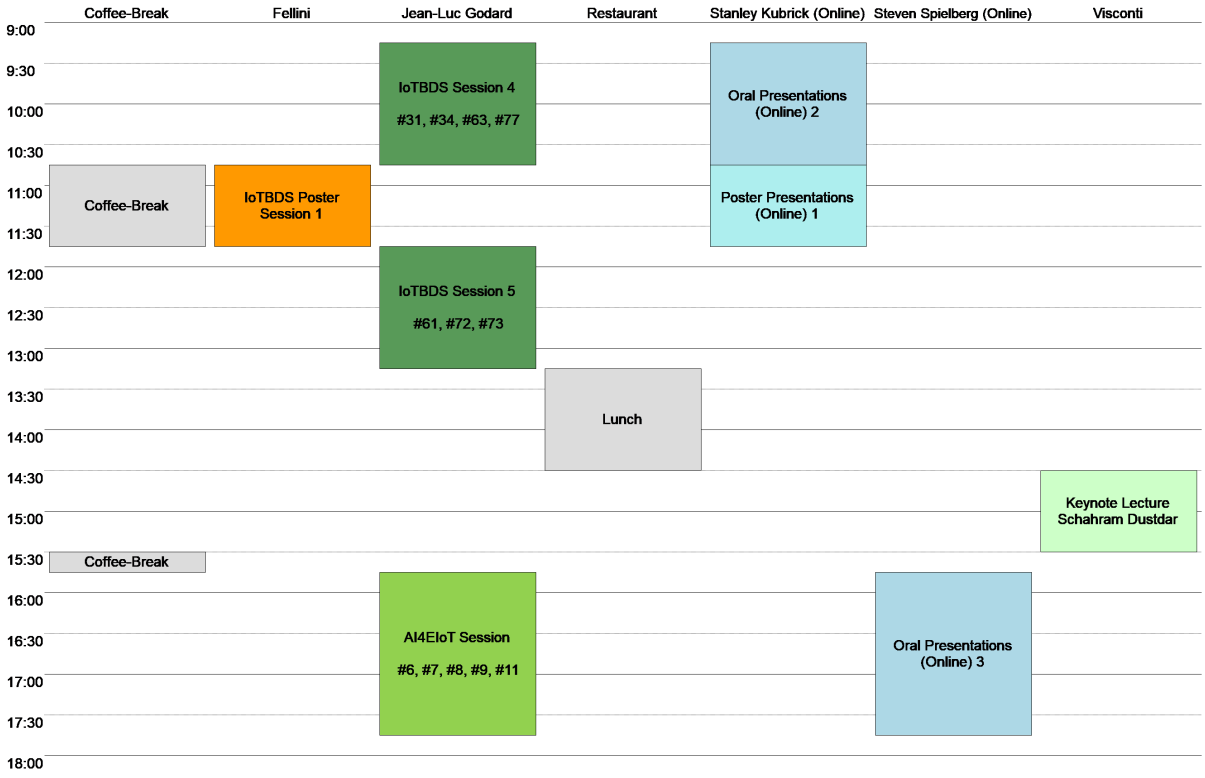
Department of Computer Science and Communications Engineering, Waseda University, Japan

Keywords: Hardware Trojan, Power Analysis, Anomalous Behavior Detection, LSTM.

Abstract: Internet of Things (IoT) devices have very rapidly spread out in recent years. In IoT devices where applications run on operating system (OS), the power consumption of the OS and the power consumption of the applications overlap, resulting in complex power waveform. Previous methods need to explicitly extract the application power waveform from the multiple signal sources in the measured power waveform, which often fail to detect anomalous behaviors. In this paper, we propose a method to detect anomalous behaviors by using LSTM (Long Short Term Memory). The proposed method learns power waveform containing multiple signal sources and compares the predicted waveform and the actual one. Then, we can successfully detect anomalous behaviors, even though the measured power waveform is composed of multiple signal sources. Experimental results show that anomalous behavior can be successfully detected from an IoT device built with Raspberry Pi4.

Monday Sessions: April 7

Monday Sessions: April 7 Program Layout



Session 4A **IoTBDS**
09:15 - 10:45 **Room Jean-Luc Godard**
Internet of Things

Complete Paper #31

Toward a More Realistic Energy Consumption Model for IoT Nodes in Extreme-Edge Computing Environments

Hassan Hammoud[1,2], Frédéric Weis[2], Melen Leclerc[1] and Jean-Marie Bonnin[3]

[1] *IGEPP, INRAE, Le Rheu, France*

[2] *IRISA, Rennes University, Rennes, France*

[3] *IRISA, IMT Atlantique, Rennes, France*

Keywords: IoT, Extreme-Edge Computing, Power Consumption, Energy Efficiency, Sensors, Memory Operations, Low-Power Networks, Energy Model, Wireless Sensor Networks (WSNs).

Abstract: As Internet of Things (IoT) networks grow, accurately modeling the energy consumption of individual IoT nodes has become essential for understanding and managing energy use in diverse applications. In extreme-edge computing scenarios, where processing is pushed as close to the device as possible to support local data manipulation, memory operations play a substantial role in power consumption. However, existing models in the literature primarily focus on communication, processing, and sensing, often overlooking the contribution of memory operations to overall energy use. This paper presents an extended energy model for IoT nodes, incorporating memory-related energy usage alongside traditional factors. Results show that addressing memory usage within the energy model provides a more comprehensive understanding of consumption patterns, supporting more effective management strategies for IoT applications. Furthermore, we propose an approach that optimizes power consumption by implementing data management techniques that efficiently handle data retrieval and storage.

Complete Paper #34

Analysis and Design of Smart Components in Digital Energy Twins

Katharina Legler, Muhammad Jajja and Klaus Volbert

Faculty of Computer Science and Mathematics, Ostbayerische Technische Hochschule (OTH) Regensburg, Germany

Keywords: Digital Twins, Internet of Things, Machine Learning Models, Data Visualization.

Abstract: The energy crisis, energy demand growth, and dependence on fossil fuels worldwide have made urgent action necessary for us to seek sustainability in energy production and use. Digital technologies, especially Digital Energy Twins, have immense potential to reduce energy consumption, thereby reducing environmental impacts, particularly in the building sector. This paper presents the development of a digital energy twin that supports sustainable energy consumption analysis and optimization. Our study begins with a comprehensive analysis of the energy consumption data, the weather data, and the building plans as a solid basis for the analysis. We identify key energy consumption trends and patterns across different timescales and device-specific details that could be optimized, such as base load consumption and device-specific inefficiencies. A key part of our work is forecasting energy consumption using time series models, such as the ARIMA model, which promises to be useful in identifying patterns for improving energy efficiency. Overall, our study provides valuable insights into energy optimization and could form the base for further advances in digital energy twins at OTH Regensburg, helping to contribute to its sustainable development goals and smart campus initiatives.

Complete Paper #63

Enhancing Scalability in Wi-Fi IoT Networks with Logical Data Plane Segregation Using SDN Principles

Gabriel Vieira, Ana Ortigoso, Daniel Fuentes, Luis Frazão, Nuno Costa and António Pereira

Computer Science and Communication Research Centre, Polytechnic University of Leiria, Portugal

Keywords: Data Plane Segregation, IoT, Wi-Fi 6, ESP-NOW, SDN, Scalability.

Abstract: The increasing demand for wireless connectivity, with IoT devices projected to exceed 20 billion by 2025, reinforces Wi-Fi as the dominant technology. However, the standard star topology limits coverage for widely dispersed IoT devices. While mesh networking extends coverage, most IoT endpoints lack native mesh support, posing scalability and security challenges. This study proposes an IoT architecture leveraging a dual-stack and dual logical data plane approach based on SDN principles. It separates control and data traffic into three planes: IoT data, Wi-Fi extension, and control. The control plane employs ESP-NOW for mesh optimisation, while Wi-Fi ensures compatibility and expanded functionality. A prototype using ESP32-C6 DevKitC-1 modules demonstrates cost-efficiency, supporting stable connectivity with performance degradation beyond 50 metres. Experimental results confirm the architecture's ability to establish a self-organising, resilient mesh network with dynamic reconfiguration, offering a scalable and flexible solution for IoT mesh networks.

Complete Paper #77

Design of an IoT-Driven Software Architecture for an Automated Robotic Fueling System in Open-Pit Mining

Carlos Vilchez Pascual[1], Brian Pajares Correa[2] and Felix Santos López[2]

[1] *School of Science and Engineering, Pontifical Catholic University of Peru, Lima, Peru*

[2] *Department of Engineering, Pontifical Catholic University of Peru, Lima, Peru*

Keywords: IoT, ADD, Mining, Fueling, Robotic Arm.

Abstract: The fueling process for haul trucks in open-pit mining operations is traditionally manual, leading to inefficiencies, operational delays, and increased costs. This paper presents the design of an automated robotic fueling system aimed at optimizing fueling operations by automating key tasks such as fuel nozzle positioning, authorization, and process monitoring. The proposed system leverages Internet of Things (IoT) technology and a cloud-based architecture to enable real-time monitoring and seamless integration with existing mine infrastructure. The physical design of the system follows the German Guideline VDI 2206 methodology, while the cloud platform is structured using the Attribute Driven Design (ADD) 3.0 methodology to ensure scalability and adaptability. Additionally, interface prototypes were developed, including an Human-Machine Interface (HMI) and a responsive web application, to provide real-time data visualization and operational control. The results of this study

demonstrate the potential of automation to improve fueling efficiency, enhance safety, and reduce downtime in mining operations.

Oral Presentations (Online) 2 **IoTBDS**
09:15 - 10:45 **Room Stanley Kubrick (Online)**
Internet of Things, Big Data and Security

Complete Paper #23

PatSimBoosting: Enhancing Patient Representations for Disease Prediction Through Similarity Analysis

Yuzheng Yan, Ziyue Yu and Wuman Luo
Faculty of Applied Sciences, Macao Polytechnic University, China

Keywords: Electronic Health Records, Similarity, Patient Representation Learning, Disease Prediction.

Abstract: Patient representation learning based on electronic health records (EHR) is crucial for disease prediction. So far, various deep learning-based methods have been proposed and have made great progress. In particular, recent research has shown that trends and variations of dynamic features are of great importance in patient representation learning. However, these methods ignored the similarity between the patients. Although a number of similarity-based methods have been proposed for patient representation learning, they regarded each dynamic feature as a whole in similarity detection and failed to utilize the important fine-grained characteristics of each feature. To address this issue, we propose a Patient Similarity-Based Representation Boosting framework (PatSimBoost) to enhance patient representation for disease prediction based on EHR. Our proposed framework consists of four modules: Frequency Extraction Module (FEM), Similarity Calculation Module (SCM), Patient Representation Learning Module (PRLM), and Prediction Module (PM). FEM extracts trends and variations of dynamic features, while SCM employs Dynamic Time Warping (DTW) to assess the similarity between patients. PRLM learns patient representations, and the PM utilizes the representation of the most similar patient, along with the current patient's representation, to perform disease prediction. Experimental results on two real-world public datasets demonstrate that PatSimBoost outperforms existing state-of-the-art methods in terms of F1-score, AUROC, and AUPRC.

Complete Paper #40

Pseudorandom Number Generators, Perfect Learning and Model Visualization with Neural Networks: Expanding on LFSRs and Geffe

Sara Boancă
Babeş-Bolyai University, Cluj-Napoca, Romania

Keywords: Pseudorandom Number Generators, Neural Networks, Visualization, Linear Feedback Shift Registers, Geffe.

Abstract: The present paper explores the use of Artificial Neural Networks in the context of Pseudorandom Number Generators such as Linear Feedback Shift Registers and Geffe. Because of their hardware efficiency, variations of these generators may be used by IoT devices for security purposes. Testing to ensure security is essential, but it was observed that traditional test suites are too slow for the task. Machine Learning models, on the other hand, represent a faster alternative. While Artificial Neural Networks have been able to learn from these generators, improvements are still needed in terms of optimization and lowering domain knowledge. For that, the present paper focuses on the manner in which state of the art neural network approaches scale for a wider variety of Linear Feedback Shift Registers, including some of degree ≥ 100 and discusses the challenges that arise. Moreover, it proposes a novel Geffe learning approach that produces up to 100% testing accuracy and, based on that, promotes an additional optimization by capitalizing on model visualization and the ability of neural networks to learn deterministic functions to perfection. A comparative analysis is performed in order to show the superiority of the approach and an in-depth discussion is conducted on the possibility and implications of neural network perfect learning, particularly when coupled with model visualization. The obtained results can be regarded as incremental advances towards the creation of more robust neural network models to perform PRNG security evaluation for IoT devices.

Complete Paper #14

A Highly Nonlinear Survival Network for Hospital Readmission Prediction of Cardiac Patients

Yuejing Zhai[1], Yiping Li[2], Lihua He[1] and Wuman Luo[1]
[1] *Macao Polytechnic University, Macao, China*
[2] *Macau University of Science and Technology, Macao, China*

Keywords: Survival Network, Hospital Readmission, Cardiac Patients.

Abstract: Hospital readmission prediction of cardiac patients is an increasingly important survival analysis problem these days. So far, three groups of methods for cardiac readmission have been proposed: statistical-based, machine learning-based and deep learning-based. However, the assumptions of the statistical-based methods limit their practicality in real-world applications. The traditional machine learning-based methods suffer from the problem of over-reliance on feature engineering. Deep learning-based methods can be further classified into two groups in terms of how they deal with first hitting times: discrete strategy-based and continuous strategy-based. It is nontrivial for the discrete strategy-based methods to find the optimal granularity of output time intervals. The continuous strategy-based methods assume nonlinear proportional hazards condition, which often limits the model performance in practical applications. Besides, existing deep learning-based methods still have room for improvement in calculating the mean value of fitted dropout models. To address these issues, in this paper, we propose a highly nonlinear survival network called Environment-Aware Max-out Deep Survival Neural Network (EMaxSurv) to predict the risk value of hospital readmission of cardiac patients. EMaxSurv is based on a key observation that environmental conditions have a significant impact on the health of cardiac patients. The basic idea of EMaxSurv is to adopt maxout deep networks combined with environmental information to better capture the relationship between covariates and the distribution of the first-hitting times. To evaluate the proposed model, we conduct extensive experiments on three real world datasets. The experimental results show that EMaxSurv outperforms the other baselines in all three datasets.

Complete Paper #74

Intelligent Anomaly Detection for Context-Oriented Data Brokerage Systems

Rawaa Al-Wani and Mays Al-Naday

School of Computer Science and Electronic Engineering, The University of Essex,Colchester, U.K.

Keywords: Internet of Things, Publish/Subscribe, FIWARE, Context-Awareness, Anomaly Detection, Machine Learning.

Abstract: Applications of the Internet of Things (IoT) face challenges related to interoperability and heterogeneity due to variations in data representation formats and the absence of connectivity standards across wireless networks. This has led to the emergence of context-oriented data brokering frameworks, with FIWARE being the most widely adopted. However, such frameworks are not able to differentiate malicious from benign data. Consequently, challenges related to data quality persist, and brokering overlays are susceptible to exploitation for the distribution of malicious data assets. We propose a novel Artificial Intelligence (AI) anomaly detection service that communicates with the FIWARE broker via the Fast Application Programming Interface (FastAPI). The system also uses the Publish/Subscribe (Pub/Sub) model of FIWARE to allow networking between brokers to validate data assets before disseminating them. This is to analyze the overhead that anomaly detection introduces as a cost of the solution. The results show that the solution can detect around 95% malicious data, with an approximate overhead of 12% increase in response time.

Poster Presentations (Online) 1 **IoTBDS**
10:45 - 11:45 **Room Stanley Kubrick (Online)**

Complete Paper #18

DLT-Based Approach for Secure and Cyber Resilient Resource Constrained IoT Devices: A Survey on Recent Advances

Sthembile Mthethwa[1], Moses Dlamini[2] and Edgar Jembere[1]

[1] *School of Mathematics, Statistics and Computer Science, University of KwaZulu-Natal, Durban, Westville, South Africa*

[2] *Defence and Security, Council for Scientific and Industrial Research (CSIR), Pretoria, South Africa*

Keywords: Resource Constrained, IoT Devices, DLTs, Security, Cyber Resilient.

Abstract: Distributed Ledger Technologies (DLTs) are advancing various fields such as the financial sector, supply chain management, Internet of Things (IoTs), etc. Through its characteristics, DLTs have the potential to solve some of the challenges encountered by IoT devices as the number of connected devices continues to grow tremendously. These characteristics includes but not limited to decentralisation, traceability, security, transparency, immutability, non-repudiation, etc. There has been an increase in the body of knowledge in relation to the convergence of DLTs and IoTs. This paper examines how DLTs can enhance the security of resource-constrained IoT devices, which have limitations that prevent the implementation of traditional security measures like encryption due to size and computational power. This paper consolidates existing research by comparing techniques, technologies used, and results achieved over the years. Finally, the research identifies knowledge gaps for future exploration.

Complete Paper #20

Implementation of Rank Attack and Its Mitigation in RPL-Based IoT Networks

Madhu Yadav and Rajbir Kaur

Department of CSE, The LNMIIT, Jaipur, 302031, Rajasthan, India

Keywords: IoT, LLN, RPL, Rank Attacks.

Abstract: The burgeoning interest in the Internet of Things (IoT) has led to the widespread deployment of Low-power and Lossy Networks (LLNs). The Routing Protocol for Low-Power and Lossy Networks (RPL) is a standard protocol designed for networks with resource-constrained devices and high packet loss rates. However, RPL is vulnerable to various attacks, particularly rank attacks, which can disrupt network performance and compromise security. This paper addresses this gap by implementing rank attacks in RPL using the Cooja Simulator in Contiki OS and analyzing their impact on network performance. While rank attacks are extensively dis-cussed in the literature, practical implementations remain limited. To mitigate these attacks, we propose a novel trust-based mitigation strategy that integrates seamlessly with resource-constrained IoT devices. Our approach dynamically computes trust metrics to detect and isolate malicious nodes, thereby improving network security, reducing power consumption, and ensuring reliable packet transmission. Comparative analysis demonstrates the superiority of our approach over existing techniques, offering enhanced scalability and adaptability for secure IoT deployments.

Complete Paper #26

Inventory Management System Through the Integration of RPA and IoT to Enhance Processes in SMEs Within Peru's Automotive Sector

Tadashi Buitron, Enzo Peña and Pedro Castañeda

Facultad de Ingeniería de Sistemas de Información, Universidad Peruana de Ciencias Aplicadas (UPC), Lima, Peru

Keywords: IoT, RPA, Inventory Management, SMEs, Automation, Real-Time Monitoring, Operational Efficiency, Automotive Sector, Supply Chain Optimisation.

Abstract: This paper presents the design and implementation of an inventory management system that integrates Robotic Process Automation (RPA) and Internet of Things (IoT) technologies to enhance operational efficiency in small and medium-sized enterprises (SMEs) within Peru's automotive sector. The system addresses common challenges faced by SMEs, such as inaccurate inventories and inefficient stock management, through automated processes and real-time monitoring. By streamlining repetitive tasks and enabling continuous inventory updates, the solution reduces operating costs and improves record-keeping accuracy. Initial results show a 30% reduction in management time and a 25% decrease in operational costs, highlighting the transformative potential of RPA and IoT technologies in inventory management. The project offers a practical model that can be scaled and replicated across other sectors, contributing to the long-term competitiveness of SMEs.

Poster Session 1 **IoTBDS**
10:45 - 11:45 **Room Fellini**

Complete Paper #21

Agri-Guard: IoT-Based Network for Agricultural Health Monitoring with Fault Detection

Kushagra Singh, Kafil Momin, M. Nishal, Chinmay Sultania and Madhav Rao

Dept. of Electronics and Communication Engineering, International Institute of Information Technology Bangalore, Karnataka, India

Keywords: Precision Agriculture, Gas Sensors, ESP8266, IoT Devices, Thermal Imaging, Sustainable Farming, Crop Productivity.

Abstract: Agricultural sector is increasingly adopting advanced technologies to enhance crop productivity and sustainability. Precision agriculture leverages IoT devices, sensors, and data analytics to monitor and manage various environmental parameters, addressing challenges such as global food demand, climate change, and resource optimization. Previous research has demonstrated the efficacy of wireless sensor networks (WSNs) and remote sensing technologies in improving irrigation efficiency and early disease detection. However, these systems often assume that all components continue to operate, thereby offering an incomplete view. This study presents an advanced agricultural monitoring system referred to as Agri-Guard that integrates a wide array of sensors to measure temperature, humidity, soil moisture, and gases like CO_2, methane and ammonia. By utilizing an ESP8266 microcontroller and IoT connectivity, the system ensures seamless data transmission and real-time processing. Additionally, a centralized hub, equipped with a Raspberry Pi 5 and a thermal camera, enhances the detection of crop anomalies, and an inoperative sensor hub. The sensor hub in the form of a cone is optimally designed to detect environmental parameters besides being rainproof. The proposed Agri-Gaurd setup clearly demonstrated the lack of manure and water from the sensors' data, whereas thermal imaging showcased the classification of 92.7% between a dead and alive plant. The anomaly between an operating and non-operating Agri-cone was found to be in complete agreement (100%). The proposed system represents a significant improvement over existing solutions, empowering farmers with precise data and faulty hub detection, leading to quick recovery and more sustainable farming practices.

Complete Paper #29

A Comparative Evaluation of Zero Knowledge Proof Techniques

Seyed Mohsen Rostamkolaei Motlagh[1], Claus Pahl[1], Hamid Barzegar[1] and Nabil El Ioini[2]

[1] *Free University of Bozen-Bolzano, 39100 Bolzano, Italy*

[2] *University of Nottingham, 43500 Semenyih, Malaysia*

Keywords: ZKP, Authentication, Distributed Systems, Bulletproof, zk-STARK, Experimental Comparison.

Abstract: Common to many distributed systems such as the Internet-of-Things (IoT) is decentralisation, often with a growing number of devices with diverse computational capabilities and security requirements. If integrated into critical applications, ensuring secure communication and data integrity is critical. In particular, privacy and security concerns are growing with the rise of these architectures. Zero-Knowledge Proof (ZKP) techniques are solutions to improve security without compromising on privacy. While the advantages of ZKP techniques are well-documented, it is important to consider the inherent limitations of these distributed environments, such as restricted processing power, memory capacity, and energy constraints, when aiming to solve security concerns. Here, we select two prominent ZKP techniques, Bulletproof and zk-STARK, and experimentally compare a number of their variants for a set of architecture-specific assessment criteria.

Complete Paper #32

Making Use of Design Patterns in IoT Middleware Implementation

Lasse Harjumaa, Ilkka Kivelä, Petri Jyrkkä and Ismo Hakala

Kokkola University Consortium Chydenius, University of Jyväskylä, Kokkola, Finland

Keywords: Internet of Things, Design Patterns, Scalability, Maintainability, Software Design, Wireless Sensor Networks.

Abstract: This paper describes the usage of object-oriented and microservice design patterns to enhance system maintainability. The project involved bringing together data from multiple sensor networks and providing single endpoint for client applications. The middleware consists of purpose-specific components, databases and various off-the-shelf IoT components. Key lessons learned include the role of design patterns in simplifying complex system interactions and improving understandability. The importance of a modular approach, where design patterns provide a structured framework that promote reuse of proven solutions and reduce technical complexity becomes clear during the implementation of the middleware.

Complete Paper #38

IoT-Driven Livestock Monitoring: Leveraging LoRaWAN for Behavior Analysis and Enhanced Farm Management

Khadijah Febriana, Rahul Thakur and Sudip Roy

Indian Institute of Technology Roorkee, India

Keywords: Livestock Monitoring, IoT, Sensors, LoRaWAN.

Abstract: Cattle play a crucial role in farming by providing essential resources such as milk, meat, leather, and labor, contributing significantly to both economic and social stability in rural areas of India. This work develops an energy-efficient IoT system based on LoRaWAN to monitor and analyze livestock behavior. The system employs an MPU6050 sensor and TTGO T-Beam microcontroller to capture livestock's movement and positional data. This data is continuously transmitted via a mesh network, utilizing The Things Network and ThingSpeak for remote analytics. A neural network with two hidden layers and ReLU activation functions is trained with sparse categorical cross-entropy loss. Validation on a 20% subset of the training data demonstrates high accuracy in classifying complex animal behaviors. Classification results, including F1-scores, precision, and recall metrics, highlight the model's strong capability in behavior differentiation. Overall, this system enhances animal health and welfare, improves farm productivity, promotes environmental sustainability, and strengthens India's food security.

Complete Paper #50

Automated Test Input Generation Based on Web User Interfaces via Large Language Models

Kento Hasegawa[1], Hibiki Nakanishi[2], Seira Hidano[1], Kazuhide Fukushima[1], Kazuo Hashimoto[2] and Nozomu Togawa[2]

[1] *KDDI Research, Inc., 2-1-15, Ohara, Fujimino-shi, Saitama, Japan*

[2] *Waseda University, 3-4-1, Okubo, Shinjuku-ku, Tokyo, Japan*

Keywords: Internet of Things, Cybersecurity, Large Language Models, Fuzzing, User Interfaces.

Abstract: The detailed implementation of IoT devices is often opaque, necessitating the use of a black-box model for verification. A challenge in fuzzing for the diverse types of IoT devices is generating initial test inputs (i.e., initial seeds for fuzzing) that fit the specific functions of the target. In this paper, we propose an automatic test input generation method for fuzzing the management interfaces of IoT devices. First, the automated web UI navigation function identifies the input fields. Next, the test input generation function creates appropriate test inputs for these input fields by analyzing the surrounding information of each field. By leveraging these functions, we establish a method for automatically generating test inputs specifically for the web user interfaces of IoT devices. The experimental results demonstrate that test inputs that are suitable for the input fields are successfully generated.

Complete Paper #56

A Distributed Event-Orchestrated Digital Twin Architecture for Optimizing Energy-Intensive Industries

Nicolò Bertozzi[1], Anna Geraci[1], Letizia Bergamasco[1,2], Enrico Ferrera[1], Edoardo Pristeri[1] and Claudio Pastrone[1]

[1] *Fondazione Links, Via Pier Carlo Boggio 61, 10138 Turin, Italy*

[2] *Department of Control and Computer Engineering, Politecnico di Torino, Corso Duca degli Abruzzi 24, 10129 Turin, Italy*

Keywords: Distributed Microservices Architecture, Digital Twin, Event-Based Orchestration, Interoperability, Energy Optimization, Industry, Computing Continuum.

Abstract: This paper presents a novel distributed architecture designed to spawn digital twin solutions to improve energy efficiency in energy-intensive industrial scenarios. By executing user-defined workflows, our platform enables the implementation of real-time monitoring, forecasting, and simulation microservices to enhance decision-making strategies for optimizing industrial processes. Leveraging a stateless centralized orchestration mechanism built around an Apache Kafka-based backbone, the platform ensures scalability, fault tolerance, and efficient handling of heterogeneous data. Key features include intuitive workflow configuration, asynchronous communication for streamlined workflow execution, and API-driven scheduling for dynamic, event-based task management. This platform will be deployed and validated in several energy-intensive industrial scenarios, supporting the management of energy systems of different plants, to prove its effectiveness across a wide range of energy management challenges.

Complete Paper #62

PacketZapper: A Scalable and Automated Platform for IoT Traffic Collection and Analysis

Mathias Hedberg, Jia-Chun Lin and Ming-Chang Lee

Department of Information Security and Communication Technology, Norwegian University of Science and Technology (NTNU), Gjøvik, Norway

Keywords: IoT Traffic Analysis, Automated Traffic Collection, Scalable Data Processing, Smart Homes, IoT.

Abstract: The increasing adoption of IoT devices in home environments has raised significant concerns about security and privacy. Analyzing real IoT traffic is essential for understanding these implications, yet the process poses challenges for researchers, requiring expertise in hardware selection, data collection, storage, and analysis. To address these challenges, we introduce PacketZapper, an automated and scalable platform for IoT traffic collection, processing, and analysis. PacketZapper combines existing open-source tools with custom components to streamline research workflows. It follows a four-stage solution structure—collect, parse, store, and process—ensuring modularity and future extensibility. The platform supports the collection of Zigbee and 433MHz traffic using commercial USB dongles, with the potential to integrate additional IoT protocols. Data is stored in Elasticsearch, enabling efficient querying and exploration, while Apache Airflow automates task orchestration through Directed Acyclic Graphs (DAGs). A case study evaluation demonstrated PacketZapper's capability to infer devices in a smart home and to facilitate effective data exploration. The platform provides a robust foundation for reproducible IoT traffic research, addressing critical gaps in IoT traffic analysis. It offers researchers an extensible, automated, and scalable solution for conducting diverse experiments.

Complete Paper #68

A Study of Anomalous Communication Detection for IoT Devices Using Flow Logs in a Cloud Environment

Yutaro Iizawa[1], Norihiro Okui[2], Yusuke Akimoto[1], Shotaro Fukushima[1], Ayumu Kubota[2] and Takuya Yoshida[3]

[1] *ARISE Analytics Inc., 2-21-1, Shibuya, Shibuya, Tokyo, Japan*

[2] *KDDI Research, Inc., 2-1-15, Ohara, Fujimino, Saitama, Japan*

[3] *TOYOTA Motor Corporation, 1-6-1, Otemachi, Chiyoda, Tokyo, Japan*

Keywords: Aomalous Communication Detection, IoT, IPFIX, VPC Flow Logs.

Abstract: Research on network-based anomaly detection has been conducted as a countermeasure against cyberattacks from IoT devices. Specifically, anomaly detection based on flow data, such as IPFIX, has garnered increasing attention to address the rising communication volume. In these studies, obtaining flow data from the communication data sent and received by IoT devices is necessary; however, obtaining these data can be difficult when the IoT system is already built in a cloud environment. In this study, we investigated an anomalous communication detection method using VPC Flow Logs, which can be obtained via AWS. VPC Flow Logs record only the number of packets and bytes in a single direction, resulting in less information than that obtained via flow data. For example, session information is divided into multiple records according to the time window. To increase the precision of anomalous communication detection using VPC Flow Logs data, we developed a methodology for the effective conversion of multiple VPC Flow Logs into bidirectional data. The efficacy of this approach was assessed by evaluating its performance on public

datasets.

Complete Paper #76

A Novel Wi-Fi Mesh Network Framework for Efficient Mobile Data Transmission

Yu-Jie Ou, Yan-Ming Chen and Chun-Chao Yeh

Department of Computer Science and Engineering, National Taiwan Ocean University, Keelung 202301, Taiwan

Keywords: Wi-Fi Mesh Networks, Mobile Data Transmission, QUIC.

Abstract: The current trend involves the use of robots and various IoT devices to assist in production and development. In the future, with the integration of AI technology, related applications will become even more widespread. Within this context, whether it is command transmission, equipment status reporting, or equipment condition monitoring, a stable network environment is essential. Presently, the technology can be mainly categorized into wired networks, wireless networks (Wi-Fi), and mobile networks. While wired networks are fast and stable, they are constrained by physical lines and cannot be used in environments requiring interlaced movement. Wireless networks face disconnection issues when crossing different APs. While mobile networks, particularly those using 5G, offer excellent real-time performance, the establishment of private networks is expensive and the signal sources are relatively singular. This study proposes the use of Wi-Fi technology combined with the UDP (User Datagram Protocol) and QUIC (Quick UDP Internet Connections) protocols to create a new type of multipath network system. This system aims to reduce the adverse effects of physical environmental changes and wireless access point (AP) device transitions, achieving a low-cost, high-speed, highly mobile, and secure network environment in specific settings. The proposed scheme leverages the encryption and security features of the QUIC protocol to protect data privacy while supporting the needs of high-mobility applications.

Session 5A **IoTBDS**
11:45 - 13:15 **Room Jean-Luc Godard**
Internet of Things (IoT) Fundamentals

Complete Paper #61

The Integration of Time Series Anomaly Detection into a Smart Home Environment

Eran Kaufman, Yigal Hoffner, Adan Fadila, Amin Masharqa and Nour Mawasi

Department of Software Engineering, Shenkar College, Israel

Keywords: Smart Home Architecture, Anomaly Detection Methods, Anomaly Management Process.

Abstract: Smart home IoT systems have become integral to modern households. To ensure security and safety, prevent hazards, accidents and health emergencies, optimize resource usage, and maintain system reliability, it is essential to have anomaly detection as an integral part of the home management system. Integrating anomaly detection into the smart home environment requires it to be extended to a comprehensive anomaly management process that can be broken down into several stages: data collection and aggregation, anomaly detection, anomaly assessment, decision-making, action-taking, logging and analysis of anomaly events and responses. Our work focuses on three key contributions. First, we explore anomaly detection algorithms to improve detection accuracy, improve classification, and provide users with detailed information on identified anomalies. Second, we present a step-by-step breakdown of the anomaly management process, highlighting how anomaly detection functions as its critical subprocess. Finally, we provide an in-depth explanation of how this management process is seamlessly integrated into a functional smart home environment, ensuring a cohesive and effective approach to anomaly handling.

Complete Paper #72

Clustering-Based Pattern Prediction Framework for Air Pollution Prediction

Athiruj Poositaporn[1,2] and Hanmin Jung[1,2]

[1] *University of Science and Technology, 217, Gajeong-ro, Yuseong-gu, Daejeon, Gyeonggi-do, Republic of Korea*

[2] *Korea Institute of Science and Technology Information, 245, Daehak-ro, Yuseong-gu, Daejeon, Republic of Korea*

Keywords: Internet of Things, Pattern Prediction, Prediction Framework, Pattern Analysis, K-means Clustering.

Abstract: Accurately predicting patterns from large and complex datasets remains a significant challenge, particularly in environments where real-time predictions are crucial. Despite advancements in predictive modeling, there remains a gap in effectively integrating clustering techniques with advanced similarity metrics to enhance prediction accuracy. This research introduces a clustering-based pattern prediction framework integrating Kmeans with our Overall Difference with Crossover Penalty (OD with CP) similarity metric to predict data patterns. In the experiment, we demonstrated its application in air pollution pattern prediction by comparing 15 different model-cluster combinations. We employed five predictive models: Euclidean Distance, Markov Chain, XGBoost, Random Forest, and LSTM to predict the next day's pollution pattern across three cluster sizes (K = 10, 20, and 30). Our aim was to address the limitation of traditional clustering methods in pattern prediction by evaluating the performance of each model-cluster combination to determine the most accurate predictions. The results showed that our framework identified the most accurate model-cluster combination. Therefore, the study highlighted the generalizability of our framework and indicated its adaptability in pattern prediction. In the future, we aim to apply our framework to a Large Language Model (LLM) combined with Retrieval Augmented Generation (RAG) to enhance in-depth result interpretation. Furthermore, we intend to expand the study to include client engagement strategy to further validate the effectiveness of our study in real-world applications.

Complete Paper #73

Towards Client Engagement Using RAG System with Pattern Prediction Framework

Hanmin Jung[1,2] and Athiruj Poositaporn[1,2]

[1] *University of Science and Technology, 217, Gajeong-ro, Yuseong-gu, Daejeon, Gyeonggi-do, Republic of Korea*

[2] *Korea Institute of Science and Technology Information, 245, Daehak-ro, Yuseong-gu, Daejeon, Republic of Korea*

Keywords: Client Engagement, Retrieval-Augmented Generation, Large Language Model, Q&A System.

Abstract: Client engagement refers to the process of companies and customers building and maintaining relationships through communication, personalized marketing, and value-added services. This often results in analysis reports, consulting services, and strategic planning documents. Tools like GPT-4o have significant potential to support these interactions in sectors such

as meteorological organizations. However, standalone generative models like GPT-4o face challenges in accessing external datasets and often produce generic outputs. To overcome these limitations, this study introduces a chat-based Retrieval-Augmented Generation (RAG) system integrated with a pattern prediction framework. We demonstrate our RAG system in analyzing air pollution pattern prediction results from our prior study and compare its generated answers with a standalone GPT-4o model. Experimental results show that the RAG system delivers actionable recommendations and contextually enriched outputs grounded in domain-specific data. In future work, we aim to explore the potential of RAG in real-world applications, such as improving client engagement by generating client-focused reports.

Keynote Lecture **IoTBDS**
14:30 - 15:30 **Room Visconti**

Active Inference for Distributed Intelligence in IoT and Edge Computing

Schahram Dustdar
Vienna University of Technology, Austria

Abstract: Modern distributed systems also deal with uncertain scenarios, where environments, infrastructures, and applications are widely diverse. In the scope of IoT-Edge-Fog-Cloud computing, leveraging these neuroscience-inspired principles and mechanisms could aid in building more flexible solutions able to generalize over different environments. A captivating set of hypotheses from the field of neuroscience suggests that human and animal brain mechanisms result from a few powerful principles. If proved to be accurate, these assumptions could open a deep understanding of the way humans and animals manage to cope with the unpredictability of events and imagination. In this talk, we will explore how Active Inference mechanisms can be utilized for Distributed Intelligence in the Computing Continuum. and in particular for IoT and Edge Computing.

Oral Presentations (Online) 3 **IoTBDS**
15:45 - 17:45 **Room Steven Spielberg (Online)**
Internet of Things

Complete Paper #57

A Comparative Study of Log-Based Anomaly Detection Methods in Real-World System Logs

Nadira Nipa, Nizar Bouguila and Zachary Patterson
Concordia Institute for Information and Systems Engineering, Concordia University, Montreal, Quebec, Canada

Keywords: Anomaly Detection, Log Analysis, Machine Learning, Deep Learning, Log Parser.

Abstract: The reliability and security of today's smart and autonomous systems increasingly rely on effective anomaly detection capabilities. Logs generated by intelligent devices during runtime offer valuable insights for monitoring and troubleshooting. Nonetheless, the enormous quantity and complexity of logs produced by contemporary systems render manual anomaly inspection impractical, error-prone, and laborious. In response to this, a variety of automated methods for log-based anomaly detection have been developed. However, many current methods are evaluated in controlled environments with set assumptions and frequently depend on publicly available datasets. In contrast, real-world system logs present greater complexity, lack of labels, and noise, creating substantial challenges when applying these methods directly in industrial settings. This work explores and adapts existing machine learning and deep learning techniques for anomaly detection to function on real-world system logs produced by an intelligent autonomous display device. We conduct a comparative analysis of these methods, evaluating their effectiveness in detecting anomalies through various metrics and efficiency measures. Our findings emphasize the most efficient approach for detecting anomalies within this specific system, enabling proactive maintenance and enhancing overall system reliability. Our work provides valuable insights and directions for adopting log-based anomaly detection models in future research, particularly in industrial applications.

Complete Paper #16

RAM-IoT: Risk Assessment Model for IoT-Based Critical Assets

Kayode Adewole[1,2], Andreas Jacobsson[1,2] and Paul Davidsson[1,2]
[1] *Department of Computer Science and Media Technology, Malmö University, Malmö, Sweden*
[2] *Internet of Things and People Research Center, Malmö University, Malmö, Sweden*

Keywords: Internet of Things, Risk Assessment, Threat, Vulnerability, Fuzzy AHP, Security and Privacy.

Abstract: As the number of Internet of Things (IoT) devices continues to grow, understanding and mitigating potential vulnerabilities and threats is crucial. With IoT devices becoming ubiquitous in critical sectors like healthcare, transportation, energy, and industrial automation, identifying and addressing risks is increasingly important. A comprehensive risk management approach enables IoT stakeholders to safeguard user data and privacy, as well as system integrity. Existing risk assessment frameworks focus on qualitative risk analysis methodologies, such as operationally critical threat, asset, and vulnerability evaluation (OCTAVE). However, security risk assessment, particularly for IoT ecosystem, demands both qualitative and quantitative risk assessment. This paper proposes RAM-IoT, a risk assessment model for IoT-based critical assets that integrates qualitative and quantitative risk assessment approaches. A multi-criteria decision making (MCDM) approach based on fuzzy Analytic Hierarchy Process (fuzzy AHP) is proposed to address the subjective assessment of the IoT risk analysts and their corresponding stakeholders. The applicability of the proposed model is illustrated through a use case connected to service delivery in the IoT. The proposed model provides a guideline to researchers and practitioners on how to quantify the risks targeting assets in IoT, thereby providing adequate support for protecting IoT ecosystems.

Complete Paper #59

Measuring Fall Risk Using the Internet-of-Things Chair

Alexander Lee[1], Melissa Lee[1], Chelsea Yeh[2] and Kyle Yeh[3]
[1] *Chino Premier Surgery Center, Chino, CA 91710, U.S.A.*
[2] *Yale University, New Haven, CT, 06520, U.S.A.*
[3] *Brown University, Providence, RI, 02912, U.S.A.*

Keywords: Lower Extremity Strength, Leg Strength, Falls, 30 Second Chair Stand Test, 5 Times Sit-to-Stand Test, Internet of Things, Automatic Chair, Wireless Chair, Clinical Study.

Abstract: Falls are one of the leading causes of injuries and deaths for U.S. adults ages 65 and older. People can fall because

of imbalance and leg weakness. Fall risks are evaluated by standardized tests, including the 30-Second Chair Stand Test (30CST) and 5x Sit-to-Stand Test (5xSST). These tests are conducted by visual observation of the participant and manual counting, which can be inaccurate and tedious. This study clinically tested an Internet of Things Chair (IoT) on how well it performed on the 30CST and 5xSST. A clinical study was performed on 224 participants. The results of the IoT Chair were found to be similar to the traditional, visually observed method. The IoT Chair required less manual work and provided information that was not obtainable with the observer method. The IoT Chair was able to calculate the weight exerted on the individual chair legs, rate of weight change, lag time between each sit-stand cycle, the amount of time spent standing during each cycle, and the amount of time each sit-stand cycle required. This additional information can allow for a better understanding of a person's leg strength and improves the prediction for falls, which can save lives and lower healthcare costs.

Complete Paper #64

A Multilevel Graph-Based Recommender System for Personalized Learning Paths in Archaeological Parks: Leveraging IoT and Situation Awareness

Mario Casillo[1], Francesco Colace[2], Angelo Lorusso[2], Domenico Santaniello[1] and Carmine Valentino[2]

[1] *DISPAC, University of Salerno, Fisciano (SA), Italy*

[2] *DIIN, University of Salerno, Fisciano (SA), Italy*

Keywords: Internet of Things, Bayesian Network, Situation Awareness, Ontology, Cultural Heritage.

Abstract: Enhancing Cultural Heritage relies on innovative technologies to improve user interaction with cultural assets. The advent of the Internet of Things (IoT) has made integrating smart devices with educational methodologies possible, enabling a combination of cultural engagement, heritage promotion, and learning. This study aims to introduce a Recommender System capable of suggesting personalized learning paths for users visiting archaeological parks, leveraging a multilevel graph-based approach. The method is grounded in Situation Awareness (SA) and structured into three main levels: perception, comprehension, and prediction. The perception level is ensured through data acquisition from sensors deployed in the field; the comprehension level utilizes semantic and contextual graph approaches for domain representation; and the prediction level is developed using predictive algorithms based on Bayesian Networks. A preliminary experimental campaign conducted across three archaeological parks allowed for testing the effectiveness of the proposed approach, demonstrating its predictive capabilities and potential in creating tailored cultural experiences. The findings highlight how advanced technologies can enrich users' educational experiences and significantly contribute to the valorization of cultural heritage.

Complete Paper #66

Anomaly Detection on Univariate Time Series Data Using Exponentially Weighted Moving Average (AnEWMA)

Jalaa Hoblos

Computer Science Department, Stony Brook University, Stony Brook, NY, U.S.A.

Keywords: Anomaly Detection, EWMA, Time Series, Exponentially Weighted Moving Average, Control Limits.

Abstract: Anomaly detection in time series data is a critical task with wide-ranging applications in industries such as finance, cybersecurity, healthcare, and manufacturing. It involves the identification of data points or patterns that deviate significantly from the expected behavior, thereby ensuring the integrity and reliability of data analysis and decision-making processes. Several methods have been developed to address this challenge, each offering unique advantages and addressing different aspects of the problem, ranging from statistical methods, to machine learning techniques, and dynamic time warping methods. In this work, we present a novel Anomaly Detection approach (AnEWMA) able to identify anomalies through the application of the Exponentially Weighted Moving Average (EWMA). AnEWMA leverages the responsiveness of EWMA to subtle shifts in data trends, enabling the detection of anomalies in a lightweight and computationally efficient manner. AnEWMA adjusts the control limits of the monitoring system using tuned heuristic multipliers. Traditional methods often rely on fixed control limits, which can lead to a high rate of false positives or missed anomalies, especially in the presence of noisy or non-stationary data. The proposed AnEWMA algorithm shows promising results when compared with state-of-the-art unsupervised and semi-supervised anomaly detection methods using stream data from popular Benchmarks.

Special Session - Session **AI4EIoT**
15:45 - 17:45 **Room Jean-Luc Godard**
Artificial Intelligence for Emerging IoT Systems:Open Challenges and Novel Perspectives

Complete Paper #8

eXplainable Artificial Intelligence Framework for Structure's Limit Load Extimation

Habib Imani[1], Renato Zona[2], Armando Arcieri[3], Luigi Piero Di Bonito[4], Simone Palladino[2] and Vincenzo Minutolo[2]

[1] *Department of Engineering and Architecture, Università degli Studi di Catania,Via S.Sofia 64, Catania (CT), Italy*

[2] *Department of Engineering, Università della Campania Vanvitelli,Via Roma 29, Aversa (CE), Italy*

[3] *Independent Researcher, Italy*

[4] *Dipartimento di Ingegneria Chimica, dei Materiali e della Produzione Industriale, Università degli Studi di Napoli "Federico II", Naples, Italy*

Keywords: Machine Learning, Finite Element, Limit Analysis, Virtual Twin, Vulnerability.

Abstract: The recent advancements in machine learning (ML) and deep learning (DL) have significantly expanded opportunities across various fields. While ML is a powerful tool applicable to numerous disciplines, its direct implementation in civil engineering poses challenges. ML models often fail to perform reliably in real-world scenarios due to lack of transparency and explainability during the decision-making process of the algorithm. To address this, physics-based ML models integrate data obtained through a finite element procedure based on the lower bound theorem of limit analysis, ensuring compliance with physical laws described by general nonlinear equations. These models are designed to handle supervised learning tasks while mitigating the effects of data shift. Widely recognized for their applications in disciplines such as fluid dynamics, quantum mechanics, computational resources, and data storage, physics-based ML is increasingly being explored in civil engineering. In this work, a novel methodology that combines machine learning and computational mechanics to evaluate the seismic vulnerability of existing buildings is proposed. Interesting and affordable results are reported in the paper concerning the predictability of limit load of structure through ML approaches. The aim is to provide a practical tool for professionals, enabling efficient mainte-

nance of the built environment and facilitating the organization of interventions in response to natural disasters such as earthquakes.

Complete Paper #9

Towards a Digital Twin of the Cardiovascular System

Ciro Nespolino, Roberta De Fazio, Laura Verde and Stefano Marrone

Dipartimento di Matematica e Fisica, Università degli Studi della Campania "Luigi Vanvitelli", viale Lincoln 5, Caserta, Italy

Keywords: Human Digital Twins, Heartbeat Modelling, Ordinary/Partial Differential Equations, Cardiovascular System, Recurrent Neural Network.

Abstract: As medicine aims to become smarter, more pervasive, and more personalised, the concept of the Digital Twin has become a cornerstone of the entire base and applied research. The advantages of having Digital Twins to understand, predict and communicate complex mechanisms and functionalities have become of paramount importance in modern and future medicine. This paper presents an approach for the construction of a Digital Twin for the cardiovascular system. The approach, with the objective of being as lightweight and explainable as possible, is based on the integration of partial differential equation models and of realistic data. This integration can overcome both the rigidity of traditional model-based methods and the computational demands of modern deep learning approaches. A technical integration of a smart backend with a frontend based on virtual reality visor is presented in the paper.

Complete Paper #7

An AI-Driven Methodology for Patent Evaluation in the IoT Sector: Assessing Relevance and Future Impact

Lelio Campanile[1], Renato Zona[2], Antonio Perfetti[3] and Franco Rosatelli[3]

[1] *Department of Mathematics and Physics, Università degli Studi della Campania, Caserta, Italy*

[2] *Department of Engineering, Università degli Studi della Campania, Via Roma 29, Aversa (CE), Italy*

[3] *Fondazione Ricerca e Imprenditorialità, Napoli, Italy*

Keywords: Patent Evaluation, Patent Classification, Machine Learning, LLM.

Abstract: The rapid expansion of the Internet of Things has led to a surge in patent filings, creating challenges in evaluating their relevance and potential impact. Traditional patent assessment methods, relying on manual review and keyword-based searches, are increasingly inadequate for analyzing the complexity of emerging IoT technologies. In this paper, we propose an AI-driven methodology for patent evaluation that leverages Large Language Models and machine learning techniques to assess patent relevance and estimate future impact. Our framework integrates advanced Natural Language Processing techniques with structured patent metadata to establish a systematic approach to patent analysis. The methodology consists of three key components: (1) feature extraction from patent text using LLM embeddings and conventional NLP methods, (2) relevance classification and clustering to identify emerging technological trends, and (3) an initial formulation of impact estimation based on semantic similarity and citation patterns. While this study focuses primarily on defining the methodology, we include a minimal validation on a sample dataset to illustrate its feasibility and potential. The proposed approach lays the groundwork for a scalable, automated patent evaluation system, with future research directions aimed at refining impact prediction models and expanding empirical validation.

Complete Paper #6

Enhancing Accuracy and Efficiency in Physical Count Processes: Leveraging AI, IoT, and Automation for Real-Time Inventory Management in Supply Chain

Prabhakaran Rajendran[1], Nirmal Balaraman[2] and Hareesh Viswanathan[3]

[1] *CSCS LLC, Alpharetta, Georgia, U.S.A.*

[2] *Inframark LLC, Norcross, Georgia, U.SA.*

[3] *Boston Scientific, Greater Boston, Massachusetts, U.S.A.*

Keywords: AI, IoT, Automation, Inventory Management, Real-Time Tracking.

Abstract: This paper aims at studying how much AI, IoT, and automation play a crucial role in improving the calibration and effectiveness of physical inventory count exercises. As supply chain networks become enhanced, companies are using these technologies to counter issues that come with the use of enhanced inventory control including but not limited to errors, slowness among others. About this, the present paper examines two different case studies one, based on a well-known logistics company in Finland, and the other, Amazon's fulfillment centers exploring how the application of AI, IoT and automation enhance real-time inventory management. The study informs that the adoption of these technologies greatly improves both the integrity and efficiency of inventory data, accurate real-time monitoring, and less reliance on manual adjustments, and streamlines warehouse logistics. This paper fills the existing literature gap in understanding technological advancements in inventory management and provides valuable recommendations to companies that wish to transform in the context of the Fourth Industrial Revolution.

Complete Paper #11

Quantum Convolutional Neural Networks for Image Classification: Perspectives and Challenges

Fabio Napoli[1], Lelio Campanile[1], Giovanni De Gregorio[1,2] and Stefano Marrone[1]

[1] *Dipartimento di Matematica e Fisica, Università degli Studi della Campania "Luigi Vanvitelli", viale Lincoln 5, Caserta, Italy*

[2] *Istituto Nazionale di Fisica Nucleare, Complesso Universitario di Monte S. Angelo, Via Cintia, Napoli, I-80126, Italy*

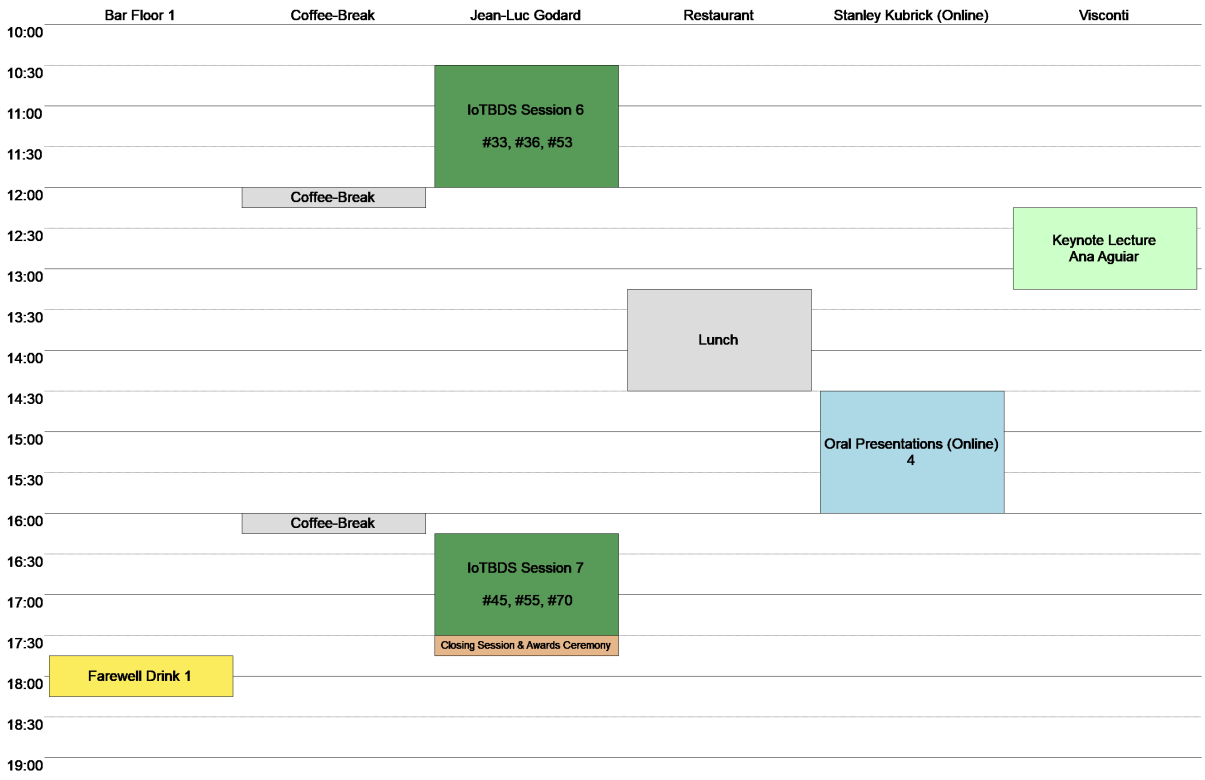
Keywords: Quantum Convolutional Neural Networks, Labelled Faces in the Wild, Face Recognition.

Abstract: Quantum Computing is becoming a central point of discussion in both academic and industrial communities. Quantum Machine Learning is one of the most promising subfields of this technology, in particular for image classification. In this paper, the model of Quantum Convolutional Neural Networks and some related implementations are explored in their potential for a non-trivial task of image classification. The paper presents some experimentations and discusses the limitations and the strengths of these approaches when compared with classical Convolutional Neural Networks. Furthermore, an analysis of the impact of the noise level on the quality of the classification task has been performed. This paper reports a substantial equivalence of the

perfomance of the model with respect the level of noise.

Tuesday Sessions: April 8

Tuesday Sessions: April 8 Program Layout



Session 6A **IoTBDS**
10:30 - 12:00 **Room Jean-Luc Godard**
Big Data Research

Complete Paper #33

Data Network Game: Enabling Collaboration via Data Mesh

Lucaleonardo Bove[1,2], Nicolò Totaro[1,2] and Massimiliano Gervasi[1,2]

[1] *Department of Engineering for Innovation, University of Salento, Lecce, Italy*

[2] *Centre for Applied Mathematics and Physics for Industry (CAMPI), University of Salento, Lecce, Italy*

Keywords: Data Sharing, Big Data Analytics, Data Value, Data Network, Cooperative Game Theory, Data Mesh.

Abstract: Organizations aim to transform raw data into valuable insights using advanced analytical methods. Since data can be replicated and shared, multiple actors can simultaneously utilize the same information. This study presents the Data Network, a theoretical framework representing potential collaborations among organizations sharing data in large-scale big data projects, using Data Mesh as a supporting architecture. The Data Network Game (DNG) extends this model by applying game theory to analyze inter-organizational collaborations, incorporating market-imposed constraints that limit compatibility. Various scenarios, defined by distinct benefit and cost functions, are explored to understand their impact on coalition formation and market dynamics. A simplified theoretical example shows how coalitions can achieve greater value through collaboration than by acting independently. This model serves as a practical tool for assessing the trade-offs of cooperation and offers insights into managing emerging data-driven markets.

Complete Paper #36

Approach to Deploying Batch File Data Products in a Big Data Environment

Richard Felix, Patricia Plentz and Jean Hauck

Federal University of Santa Catarina, Florianópolis, Brazil

Keywords: Batch Processing, Big Data, Data Science, Agility.

Abstract: Data science has become essential across industries such as government, healthcare, and finance, driving decision-making through large-scale data analysis. Deploying batch data products, like the periodic calculation of credit scores for millions, presents significant challenges, including integration with existing big data architectures and ensuring scalability and efficiency. This study proposes an optimized approach that leverages software engineering and agile methodologies to streamline the deployment of such products. Validated through action research conducted at a Brazilian credit bureau, the approach demonstrated a substantial reduction in deployment time by improving documentation, development, and testing processes, offering a scalable solution to modern batch data processing challenges.

Complete Paper #53

Graph-Based Learning for Multimodal Route Recommendation

Zakariya Ghalmane and Brahim Daoud

CESI LINEACT UR 7527, Strasbourg, France

Keywords: Graph Convolutional Network, Complex Networks, Centrality Measures, Multi-Task Learning, Multimodal Transportation, Route Recommendation.

Abstract: Transportation recommendations are a vital feature of map services in navigation applications. Earlier transportation recommendation systems have struggled to deliver a satisfactory user experience because they focus exclusively on single-mode routes, such as cycling, taxis, or buses. In this paper, we represent the transportation network as a complex network (or graph). Modeling transportation as a network of nodes and edges has gained attention in the literature, generating numerous studies over the years. This approach requires a clear definition of what constitutes a node or an edge: nodes represent stops, while edges represent road segments connecting these stops. Based on this representation, we propose a framework that generates embeddings for each node and edge in the transportation network. These embeddings are created using GRU (Gated Recurrent Units) and GCN (Graph Convolutional Network) models to capture spatial and temporal patterns within the network, while incorporating centrality measures reflecting the influence of each stop. This vector representation facilitates multi-task learning for effective multi-modal transportation recommendations. The proposed framework is applied to the transportation network of Strasbourg, France. Experimental results demonstrate the framework's efficiency in recommending suitable multimodal transportation routes, considering criteria such as meteorological conditions, safety, and passenger comfort.

Keynote Lecture **IoTBDS**
12:15 - 13:15 **Room Visconti**

It's All About the Data

Ana Aguiar

Faculty of Engineering University of Porto/ Instituto de Telecomunicações, Portugal

Abstract: Not Available

Oral Presentations (Online) 4 **IoTBDS**
14:30 - 16:00 **Room Stanley Kubrick (Online)**
Security, Privacy and Trust

Complete Paper #22

Sockpuppet Detection in Wikipedia Using Machine Learning and Voting Classifiers

Rafeef Baamer and Mihai Boicu

Department of Information Sciences and Technology, George Mason University, University Dr, Fairfax, VA, U.S.A.

Keywords: Sockpuppet, Machine Learning, Classifier, Random Forest, Naive Bayes, Support Vector Machine, K-Nearest Neighbour, AdaBoost, XGBoost, Logistic Regression, Voting Classifier, Soft Voting, Hard Voting.

Abstract: Sockpuppet accounts, deceptive identities created by individuals on social networks, present significant challenges to online integrity and security. In this study, we analyse various approaches for detecting Sockpuppet accounts through the computation of several distinct features and the application of seven different classifiers. To enhance detection accuracy, we employ simple majority voting to aggregate the predictions from multiple classifiers, involving all seven classifiers, or only best five or three of them. This approach allows us to leverage the strengths of different classifiers while mitigating their individual weaknesses. Our experimental results show a significant improvement over previous studies, achieving an accuracy rate of 88% with 87% precision. Additionally, our experiments highlight the critical importance of feature engineering, demonstrating how carefully selected features directly influence classification performance. The findings also emphasize the value of human-in-the-loop involvement, where iterative feedback refines the models and improves their predictive capabilities. These insights offer meaningful contributions toward strengthening the security and integrity of online social networks by enabling more accurate and robust detection of Sockpuppet accounts.

Complete Paper #19

Enhanced Intrusion Detection in IIoT Networks: A Lightweight Approach with Autoencoder-Based Feature Learning

Tasnimul Hasan, Abrar Hossain, Mufakir Ansari and Talha Syed

Department of Electrical Engineering and Computer Science, The University of Toledo, Toledo, OH, U.S.A.

Keywords: Industrial Internet of Things, Intrusion Detection System, Autoencoder, Edge Computing, Lightweight Machine Learning.

Abstract: The rapid expansion of the Industrial Internet of Things (IIoT) has significantly advanced digital technologies and interconnected industrial sys- tems, creating substantial opportunities for growth. However, this growth has also heightened the risk of cyberattacks, necessitating robust security measures to protect IIoT networks. Intrusion Detection Systems (IDS) are essential for identifying and preventing abnormal network behaviors and malicious activities. Despite the potential of Machine Learning (ML)-based IDS solutions, existing models often face challenges with class imbalance and multiclass IIoT datasets, resulting in reduced detection accuracy. This research directly addresses these challenges by implementing six innovative approaches to enhance IDS perfor- mance, including leveraging an autoencoder for di- mensional reduction, which improves feature learning and overall detection accuracy. Our proposed Decision Tree model achieved an exceptional F1 score and accuracy of 99.94% on the Edge-IIoTset dataset. Furthermore, we prioritized lightweight model design, ensuring deployability on resource-constrained edge devices. Notably, we are the first to deploy our model on a Jetson Nano, achieving inference times of 0.185 ms for binary classification and 0.187 ms for mul-ticlass classification. These results highlight the novelty and robustness of our approach, offering a practical and efficient solution to the challenges posed by imbalanced and multiclass IIoT datasets, thereby enhancing the detection and prevention of network intrusions.

Complete Paper #42

A Comparative Analysis of Anonymous and Non-Anonymous Authorization Architectures for IoT Environments in Cooperative Intelligent Transport Systems

Hannes Salin

Swedish Transport Administration, Department of Information and Communication Technology, Borlänge, Sweden

Keywords: Trust Model, Trust Architecture, Cryptographic Accumulators, Group Signatures, Anonymous Credentials, C-ITS, Authentication, Authorization.

Abstract: In this paper, we present a comparative analysis of two distinct authorization architectures with a focus on their applicability in dynamic and cooperative intelligent transportation networks (C-ITS) suitable for low-powered IoT devices. Both architectures leverage accumulators for authorization and secret key storage, while our modification of the original architecture introduces an enhanced privacy feature enabling anonymous device access via a proxy node. This modification results in increased communication complexity, trading off anonymity against increased interaction overhead. We provide a proof of concept implementation with performance experiments, and conclude that the cryptographic computational performance remains relatively unaffected between the two architectures. Our findings suggest a potential for different deployment strategies of these architectures; in urban settings with a dense presence of proxy nodes, but also in sparser regions where privacy is not paramount due to minimal vehicle presence.

Complete Paper #65

Unravelling the Sequential Patterns of Cyber Attacks: A Temporal Analysis of Attack Dependencies

Fares ElSalamony[1], Nahla Barakat[1] and Ahmad Mostafa[2]

[1] *Artificial Intelligence Department, Faculty of Informatics and Computer Science, The British University in Egypt (BUE), El-Sherouk City, Cairo, Egypt*

[2] *Faculty of Computers and Information Technology, Innovation University, Cairo, Egypt*

Keywords: Cyber-Attack Sequence Identification, Deep Learning for Cyber Attacks Detection, Network Intrusion Detection, Time-Series Attack Prediction.

Abstract: Cybersecurity has become increasingly challenging, particularly in understanding and predicting complex attack sequences within network traffic. In this paper, we introduce a new approach for predicting cybersecurity attacks utilizing time series data and transformer architecture, which has achieved the state-of-the-art F1-score for a time series, multiclass problem on the UNSW-NB15 dataset. This is despite earlier studies either considered binary task only (attack/non-attack) or did not deal with the problem as a time series. For the first time, we integrated time series prediction with analysis and visualization methods for detecting possible sequences of cyber-attacks, which were then verified with domain experts. Statistical methods confirmed the significance of the detected sequence, ensuring that these attacks are not random. Our findings revealed the existence of patterns of attack sequences, demonstrating how one attack type often precedes another in predictable patterns. This paper not only fills a critical gap in attack progression modelling but also introduces advanced visualization and analysis that confirm the predictions of the model.

Session 7A **IoTBDS**
16:15 - 17:30 **Room Jean-Luc Godard**
Security, Privacy and Trust

Complete Paper #45

Understanding How to Use Open-Source Libraries for Differentially Private Statistics on Energy Metering Time Series

Ana Paixão[1], Breno R. da Silva[2], Rafael Silva[2], Filipe Cardoso[2] and Alexandre Braga[2]

[1] *Institute of Computing, University of Campinas (UNICAMP), Campinas, São Paulo, Brazil*

[2] *CPQD – Centro de Pesquisa e Desenvolvimento, Campinas, São Paulo, Brazil*

Keywords: Differential Privacy, Time Series, Energy Metering, Statistical Distinguishability, Utility Metric, Smart Grid.

Abstract: Demand forecasting and dynamic pricing for renewable energy open markets may require heavy analytics capabilities on fine-grained consumption data. With differential privacy, data aggregators in the energy sector can compute statistics on metering information without accidentally leaking consumption patterns of specific consumers over time. However, differential privacy is complex and hard to implement correctly. In this paper, we propose a method for evaluating differential privacy libraries by their ability to produce private and useful statistics on time series for energy consumption. The method was validated by applying it to three open source libraries used to compute differentially private averages, counts, and sums on energy metering data. The method was able to clearly distinguish between private (indistinguishable) and disclosed (distinguishable) statistics. Our method and findings can help data scientists and privacy officers within the energy sector better understand how open-source differential privacy libraries behave with time series for energy metering data.

Complete Paper #55

Enhancing IoT Network Intrusion Detection with a New GraphSAGE Embedding Algorithm Using Centrality Measures

Mortada Termos[1,2], Zakariya Ghalmane[1], Mohamed-el-Amine Brahmia[1], Ahmad Fadlallah[2,3], Ali Jaber[2] and Mourad Zghal[1]

[1] *CESI LINEACT UR 7527, Strasbourg, France*

[2] *Computer Science Department, Faculty of Sciences, Lebanese University, Beirut, Lebanon*

[3] *Computer Science Department, University of Sciences and Arts in Lebanon (USAL), Beirut, Lebanon*

Keywords: Intrusion Detection, Complex Networks, Graph Neural Networks, Artificial Intelligence, Cyber Security.

Abstract: The rapid expansion of the Internet of Things (IoT) has led to many opportunities in addition to introducing complex security challenges, necessitating more powerful Network Intrusion Detection Systems (NIDS). This study addresses this challenge by enhancing Graph Neural Networks (GNNs) with centrality measures to improve intrusion detection performance in IoT environments. We propose the so-called ”Centrality-based E-GraphSAGE”, an extension to the E-GraphSAGE model incorporating the centrality measures: Degree, Betweenness, Closeness, PageRank, and K-truss. These centrality measures, which highlight both the local and global influence of nodes (IoT devices), can uncover hidden patterns and relationships in network traffic data, thereby enhancing the performance of IDS systems. The centrality-informed initialization of node embeddings aids the model in capturing critical structural insights in the graph. The inclusion of residual connections further improves classification accuracy. Our models were evaluated on four datasets: NF-UQ-NIDS, NF-CSE-CIC-IDS2018, CCD-INID, and X-IIoTID. Results showed significant performance gains in accuracy of detection evaluated using F1-score and reduced number of false alarms. This work paves the way for more advanced and robust intrusion detection systems to improve the security of IoT networks.

Complete Paper #70

Cybersecurity Indicators Within a Cybersecurity Testing and Monitoring Framework

Steve Taylor[1], Norbert Goetze[2], Joerg Abendroth[2], Jens Kuhr[3], Rosella Mancilla[4], Bernd Wenning[5], Pasindu Kuruppuarachchi[5], Aida Omerovic[6], Ravishankar Borgaonkar[6], Andrea Skytterholm[6], Antonios Mpantis[7], George Triantafyllou[7], Oscar Garcia[8] and Oleh Zaritskyi[9]

[1] *IT Innovation Centre, University of Southampton, Southampton, U.K.*

[2] *Nokia Bell Labs, Munich Germany*

[3] *Nokia Solutions and Networks, Munich, Germany*

[4] *Ingegneria Informatica Spa, Rome, Italy*

[5] *Munster Technological University, Cork, Ireland*

[6] *SINTEF AS, Trondheim, Norway*

[7] *Athens Technology Center, Athens, Greece*

[8] *Data Analytics for Industries 4 0 SL, Xàtiva, Spain*

[9] *World Research Center of Vortex Energy, Zaporizhzhya, Ukraine*

Keywords: Cybersecurity, Cybersecurity Testing, Intrusion and Anomaly Detection, Cybersecurity Indicators, Device Under Test (DUT), System Under Test (SUT), Decision Support, Risk Assessment.

Abstract: This paper describes the concept and use of Indicators for cybersecurity decision support. We define an Indicator as observable information about a Device Under Test (DUT) or System Under Test (SUT) that potentially can underpin insight on its cybersecurity posture. We describe different types of Indicators, how they are generated by tools and components in a cybersecurity testing and monitoring framework, how they may be transformed to increase their utility and illustrate their use via an exemplary case in smart manufacturing. We summarise key observations and properties of Indicators based on collaborative multidisciplinary work that has brought together developers of tools that generate Indicators, tools that consume and analyse indicators, and representatives of users who have motivating scenarios where Indicators may inform about their cybersecurity posture.

Closing Session & Awards Ceremony **IoTBDS**
17:30 - 17:45 **Room Jean-Luc Godard**

Final Program and Book of Abstracts of IoTBDS 2025

10th International Conference on Internet of Things, Big Data and Security

https://iotbds.scitevents.org

EVENT MANAGEMENT SYSTEM:

LOGISTICS:

PROCEEDINGS WILL BE SUBMITTED FOR EVALUATION FOR INDEXING BY: