2nd European Symposium on Information Systems Engineering

Editors: Rawan AKKOUCH, Ayah THARWAT, Dr. Muriel FRANK, Prof. Dr. Gilbert FRIDGEN & Prof. Dr. Robert Keller

09-09-2025 - 11-09-2025

Clervaux, Luxembourg

Contents

Introduction

Due to their inherent socio-technical nature, the engineering of information systems creates quite distinctive challenges. Addressing them requires not only a deep understanding of technical capabilities, but also of the respective application area, and the behavior of the intended users. Being interdisciplinary by design, the Information Systems field provides a broad tool-set to address these challenges. We are thus delighted to present the proceedings of the 2nd European Symposium on Information Systems Engineering (ESISE), held from September 09 to 11, 2025, in Clervaux, Luxembourg. This symposium brought together researchers and thought leaders to explore the latest advancements and challenges in the field of information systems engineering.

With the ESISE we would like to create a platform for interdisciplinary collaboration among academics in information systems engineering from multiple universities in Europe. In our workshops and presentations, researchers were able to disseminate cutting-edge research findings and practical experiences to advance the field. In subsequent discussions, we identified emerging challenges and opportunities in information systems engineering, particularly in the context of rapidly evolving technologies.

Key Themes

The papers presented at this symposium covered a diverse range of topics, reflecting the multifaceted nature of information systems engineering. The key themes included:

- **Artificial Intelligence:** Exploration of the future of artificial intelligence (AI), as well as the applications of large language models (LLMs) in various domains such as tourism.
- **Financial Technologies:** Analyses of digital infrastructures, security risks associated with blockchain technologies, and the privacy considerations for digital identity wallets.
- **Energy Systems and Sustainability:** Studies highlight how factors like energy literacy, electricity tariffs, and other costs associated with the systems influence on the energy transition.
- **Security, Privacy, and Verifiability:** Investigations into employee security behaviors, privacy concerns in central bank digital currencies (CBDCs), crisis management training efficacy, and governance of digital identities.
- **Tourism and Visitor Management:** Research on visitor behavior analysis, crowding perceptions, and the use of LLMs to enhance tourism experiences.

We believe that the insights and innovations shared during the symposium will significantly contribute to the advancement of information systems engineering. We extend our sincere gratitude to all authors, reviewers, and participants who made this event a success.

We hope that these proceedings will serve as a valuable resource for researchers and practitioners, inspiring future work and collaboration in this dynamic field.

Acknowledgments

The success of the 2nd European Symposium on Information Systems Engineering (ESISE) is the result of the collective efforts of many individuals and organizations. We would like to express our heartfelt appreciation to:

• **The Authors:** For their high-quality submissions and contributions, which form the backbone of this symposium.

• **The Organizing Committee:** For their dedication and hard work in planning and executing the symposium.

• **SnT - University of Luxembourg and University of Applied Sciences Kempten and**: For their support and collaboration in hosting this event. Additionally, we gratefully acknowledge the financial support provided by Luxembourg National Research Fund (FNR), grant reference NCER22/IS/16570468/NCER-FT, and PayPal-FNR, PEARL grant reference 13342933/Gilbert Fridgen, which made this conference possible.

• **Participants:** For their active engagement, stimulating discussions, and contributions to the success of the symposium.

We also acknowledge the invaluable assistance of the administrative staff and volunteers who worked tirelessly behind the scenes to ensure a seamless experience for all attendees.

Thank you all for your commitment and support.

Cite This Work

Please cite this work as:
Author(s), ”Title of paper,” in Proceedings of 2nd European Symposium on Information Systems Engineering (ESISE), Clervaux, Luxembourg, 2025, pp. [page numbers].

Academic Chairs and Organization

- **Prof. Dr. Gilbert FRIDGEN**
  SnT – University of Luxembourg
- **Prof. Dr. Robert KELLER**
  Kempten University of Applied Sciences
- **Dr. Muriel FRANK**
  SnT – University of Luxembourg
- **Rawan AKKOUCH**
  SnT – University of Luxembourg
- **Ayah THARWAT**
  SnT – University of Luxembourg
- **Magali MARTIN**
  University of Luxembourg
- **Saveria EYER**
  University of Luxembourg

KEYNOTES

Household-level electricity forecasting

Speaker: Dimitrios PAPADOPOULOS
Institution: University of Freiburg

SUMMARY

Household-level electricity forecasting plays a crucial role in optimizing residential energy consumption and enabling grid flexibility. However, many households are reluctant to share their energy data, making local and privacy-preserving model deployment increasingly important. The rising adoption of IoT (Internet of Things) devices in modern homes offers a unique opportunity to leverage their computational potential for advanced, data-driven energy optimization. To fully realize this, forecasting pipelines must be both effective and computationally efficient, given the hardware constraints of Home Energy Management Systems (HEMS), which typically operate with limited CPU and RAM resources, without access to GPUs or modern multi-core processors. This study addresses these challenges by evaluating efficient machine learning algorithms under computationally constrained environments for three key household-level time series forecasting tasks: heat pump (HP) demand, overall household electricity consumption, and photovoltaic (PV) power generation. The algorithms tested include XGBoost, CatBoost, LightGBM, Random Forest, Stochastic Gradient Descent (SGD) Regressor, and Kolmogorov-Arnold Networks (KAN), all applied to day-ahead forecasting. Models were assessed on accuracy, computational efficiency, and their ability to capture peak periods, forming a Pareto front of algorithms excelling in both precision and runtime. The findings highlight distinct strengths: the SGD Regressor consistently delivers superior speed, KAN achieves lower RMSE scores, and tree-based methods excel at predicting peak demand. By benchmarking models across these criteria, this study provides practical insights for deploying machine learning forecasting methods in resource-limited residential systems, ultimately supporting efficient household-level forecasting and contributing to enhanced grid flexibility.

Is it real? Can humans recognize AI-generated images?

Speaker: Robert KELLER
Institution: Kempten University of Applied Sciences

SUMMARY

In recent years, generative AI systems have made significant strides, enabling the creation of highly realistic images from textual inputs. Applications like Midjourney and DALL·E have democratized access to these technologies, allowing even non-technical users to generate high-quality visual content. This advancement poses new challenges for advertising, particularly in terms of authenticity, transparency, and audience perception. As the boundary between real and AI-generated images blurs, the credibility of visual advertising content is increasingly scrutinized. This paper explores the impact of generative image AI on advertising by focusing on the ability of digital natives to distinguish between AI-generated images and real photographs. While previous research has primarily addressed technical advancements and media ethics, this study uniquely examines the visual assessment capabilities of young, media-savvy individuals. By investigating this specific demographic, the research aims to provide insights into the interplay between artificial image production and media-related self-perception.

Creative Forecast on the Future of Energy Research

Speaker: Phillip STAUDT
Institution: Carl von Ossietzky Universität Oldenburg

SUMMARY

This presentation investigates plausible futures of the European and global energy transition through the methodological lens of speculative design, as conceptualized by Dunne and Raby. It emphasizes how socio-technical imaginaries shape the direction of energy research and policy, often embedding implicit assumptions about technological progress, human behavior, and sustainability pathways. By applying speculative design as a reflexive framework, the discussion highlights the importance of questioning these underlying narratives and identifying overlooked dimensions in energy system transitions. The contribution aims to broaden the discourse on future-oriented energy research by integrating critical design thinking into the analysis of systemic change and innovation.

FINANCIAL TECHNOLOGIES WORKSHOP

The New Financial Machine: AI, DeFi, and the Emergence of Systemic Risk

Authors: Yunxiu ZHOU, Orestis PAPAGEORGIOU
Institution: University of Luxembourg

ABSTRACT

The convergence of Artificial Intelligence (AI) and Decentralized Finance (DeFi) is creating a new architecture of financial systemic risk that existing models fail to capture. Traditional frameworks, which assume linear causality and stationary actors, are ill-equipped for this complex adaptive system (CAS) where adaptive AI agents, nonlinearity, and co-evolution dominate. Through a CAS lens, we identify three novel risk transmission mechanisms: (1) Algorithmic Homogeneity, where agents converge on similar models, synchronizing failures; (2) Dynamic Network Rewiring, where AI-driven preferential attachment creates 'too-central-to-fail' hubs; and (3) Emergent Multi-Agent Behavior, where strategic interaction leads to tacit collusion and endogenous instability without explicit communication. We illustrate these mechanisms with a case study of the July 2025 Ethereum validator queue crisis, a preview of systemic fragility in AI-DeFi CAS. Our framework reveals a governance trilemma and establishes a foundation for empirical research and anticipatory governance in AI-mediated financial systems.

Socio-Technical Perspectives on Privacy in CBDCs

Authors: Martin BRENNECKE, Nadia POCHER, Muriel FRANK, Gilbert FRIDGEN
Institution: University of Luxembourg

ABSTRACT

Central banks worldwide are exploring retail Central Bank Digital Currencies (CBDCs) to replicate cash-like experiences for citizens while ensuring regulatory compliance. Privacy ranks as a top priority for public acceptance, yet full anonymity conflicts with anti-money laundering and counter-terrorist financing requirements, creating trade-offs often addressed through tiered designs. While technical and social aspects of CBDCs have been studied separately, their socio-technical interplay—critical for privacy—remains underexplored. This paper adopts a socio-technical lens to analyze retail CBDC ecosystems and their impact on end-user privacy. Using qualitative coding of G20 and BIS publications, we derive an abstract ecosystem model and examine interdependencies between technical and social dimensions. Findings highlight governance and data-use practices as key determinants of privacy outcomes. Contributions include extending socio-technical systems theory to CBDCs, providing insights into stakeholder roles, and informing privacy-centric design choices. Our work positions IS research to guide CBDC development toward trust and compliance.

EU Member States' Readiness for the European Digital Identity Wallet

Author: Pratyush DIKSHIT
Institution: University of Luxembourg

ABSTRACT

The European Digital Identity Wallet (EUDIW) marks a substantial milestone in the European Union's digital transformation strategy, promising seamless cross-border services and secure digital identity management. Despite unified policy ambitions, the readiness of EU member states to adopt EUDIW remains uneven and under-examined. This study presents a comparative evaluation of all 27 EU countries based on three critical indices: Digital Sovereignty, Data Privacy, and Internet Resilience. Drawing exclusively on publicly available datasets and recent peer-reviewed studies, we construct a multidimensional readiness map of the EU landscape. Our results demonstrate significant regional disparities and the centrality of digital sovereignty, privacy culture, and infrastructure resilience for successful EUDIW integration. The findings provide actionable recommendations for policymakers and suggest a robust methodology for benchmarking digital identity initiatives in Europe. The study will deliver a comparative benchmarking map highlighting significant disparities in these dimensions across member states, revealing clusters of countries leading in sovereign infrastructure, privacy protection, and network robustness versus those lagging.

Is Proof-of-Useful-Work Really Useful?

Author: Ashkan EMAMI
Institution: University of Luxembourg

ABSTRACT

Proof-of-Work (PoW) has long served as the backbone of permissionless blockchains such as Bitcoin, ensuring security and decentralization by requiring miners to solve computationally expensive (mostly cryptographic) puzzles. These puzzles, typically hash-based, serve no purpose other than to regulate block creation and defend against manipulation. Although effective, this mechanism is increasingly criticized for its excessive energy consumption, with Bitcoin alone using more electricity annually than some mid-sized countries. However, despite several proposed PoUW systems (e.g., CoinAI, Proof-of-Solution, Ofelimos), our ongoing research finds that the paradigm is far from mature. We adopt the Toulmin model of argumentation to analyze claims surrounding PoUW—breaking down each mechanism's rationale into claims, data, warrants, backings, and rebuttals. This provides a structured way to test the logical consistency and evidential support behind energy-efficiency and security assertions. While our current findings suggest that PoUW mechanisms do not yet provide a viable substitute for PoW in high-security decentralized systems, we recognize the potential. Our work contributes a critical lens and a technical foundation for researchers, developers, and policymakers considering alternative consensus protocols. The next phase of our study involves formal modeling of PoUW's energy behavior, analysis of reward dynamics, and testing selected prototypes under controlled environments.

Z-Commerce for Digital Identity Wallets

Author: Egor ERMOLAEV
Institution: University of Luxembourg

ABSTRACT

E-commerce drives global markets but faces a persistent tension between privacy and accountability. Platforms seek efficiency through data collection, while users and regulators demand stronger protections. This study introduces z-Commerce, a model integrating Digital Identity Wallets (DIWs) and Zero-Knowledge Proofs (ZKPs) to reconcile data minimization with compliance. Using a Design Science Research approach, we define three objectives: Data Minimization, Convenience, and Accountability, translating them into design requirements and implementing a prototype with modular architecture. The prototype enables selective disclosure and privacy-preserving transactions, validated through expert interviews. Findings highlight DIWs' role in user-centric control and ZKPs' potential for verifiable compliance. From this, we derive three design principles: accountable roots of trust, DIWs as access control, and unlinkable exchanges. Contributions include prescriptive design knowledge, an architectural blueprint, and insights for platform governance. z-Commerce offers a pathway for privacy-enhancing, compliant e-commerce aligned with societal expectations.

SECURITY, PRIVACY, AND VERIFIABILITY WORKSHOP

The Application of Large Language Models for User-Centric Cybersecurity

Authors: Pol HÖLZMER, Muriel FRANK
Institution: University of Luxembourg

ABSTRACT

Large language models (LLMs) increasingly shape both offensive and defensive cyber operations, yet most defenses remain technology centric and shift residual risk to end users. We explore the application of LLMs to user-centric cybersecurity and presents two complementary, human-in-the-loop interventions that aim to reduce social engineering success while preserving user autonomy. First, we describe a client-side, privacy-preserving visual assistant that runs on edge devices to analyze on-screen content, surface real-time risk signals, and deliver just-in-time coaching with transparent, explanation oriented prompts. The assistant leverages multimodal LLMs for screen understanding, integrates contextual and temporal cues, and emphasizes explainability to foster secure decision making. Second, we introduce an LLM-driven scambaiting framework that combines dynamic honeypots and adaptive personas to engage attackers, waste adversarial resources, and extract actionable threat intelligence, while operating within explicit legal and ethical guardrails. Furthermore, we evaluate proof-of-concepts of a hybrid intelligence architecture based on LLaVA that pairs features of visual assistants for on-device risk detection with dialogue models for coaching and controlled adversarial conversations, guided by privacy-by-design and open-source principles. Together, these contributions position LLMs not only as back-end agents, but as front-line, user-facing support that can improve cyber resilience at the point of interaction.

Enhancing Cyber-Crisis Management Exercises

Authors: Ayşe Nur ASYALI, Muriel FRANK, Hicham RIHALI

Institution: University of Luxembourg

ABSTRACT

Cyber crises today are complex, high-impact events that cascade across sectors, exposing technical vulnerabilities and human decision-making challenges. Traditional training methods—tabletop exercises and cyber ranges—often lack realism, adaptability, and rigorous evaluation, making them educational rather than transformative. This project aims to develop an evidence-based framework for cyber-crisis exercises that integrates human-centered design with emerging technologies. Leveraging AI-driven scenario engines, conversational agents, and digital twins, we seek to create adaptive, data-rich simulations that respond dynamically to participant decisions. Three objectives guide the work: (1) assess how technologies enhance realism and evaluation; (2) build and test a prototype with documented scenarios, role cards, and monitoring tools; and (3) synthesize findings into a reusable methodology. Outcomes include behavioral datasets, analysis pipelines, peer-reviewed research, and practitioner toolkits. By bridging research and practice, this project delivers next-generation training—immersive, adaptive, evidence-based, and human-centered—to strengthen organizational resilience

Proactive Identities and Extra-Role Security Behaviors

Authors: Ayah THARWAT, Ayşe Nur ASYALI, Muriel FRANK, Nadia POCHER
Institution: University of Luxembourg

ABSTRACT

As organizations are increasingly challenged by evolving information security threats that demand more than employee compliance to address, interest has grown in understanding extra-role security behaviors (ERSBs). ERSBs are voluntary actions employees take beyond formal security policies that benefit organizations' security, which include helping colleagues, raising concerns, modeling best practices, or proactively seeking information. Notably, ERSBs do not only compensate for policy gaps, but can also reinforce and legitimize formal compliance efforts. ERSBs play a critical role in supporting organizational security, especially in contexts where threats evolve faster than policies can adapt. Understanding how and why these behaviors emerge requires a shift in perspective, from asking whether employees are compliant, to exploring how they interpret their security role to engage in proactive behaviors. Using role identity theory, we examine how employees' security identities are formed through contextual variables that later inform their security-related actions. This study provides contributions for practitioners and organizations to improve security attitudes and environments, as well as for future research to examine the interplay between security identity and ERSBs.

Revocation of Certificates at Scale

Author: Ivan ABELLAN
Institution: University of Luxembourg

ABSTRACT

Certificate-based systems are vital for identity and authentication in modern IT. With the rise of digital identity under eID regulations and wallet-based credentials for blockchain, managing certificate lifecycles—especially revocation—is critical. Revocation ensures validity against non-expiration, legal requirements, or misuse, as these could pose security risks. Traditional methods like CRLs and OCSP are insufficient for today's diverse, privacy-focused systems operating across devices in online and/or offline settings. Effective revocation management relies on certificate status encoding and privacy-preserving status checks. Protocols such as Zero-Knowledge Proofs (ZKP) could support privacy and compliance but demand high computational resources. Specialized data structures like Merkle trees mitigate this by encoding revocation status efficiently, authenticating data in logarithmic time. Combining Merkle trees with ZKP allows privacy-preserving revocation checks: Merkle trees store revocation status, while ZKPs verify validity without revealing sensitive information. This approach supports regulatory compliance and scalability for emerging credential systems.

ENERGY WORKSHOP

Towards understanding Energy Consumption of EV Busses

Author: Boris ORTEGA MORENO
Institution: University of Luxembourg

ABSTRACT

The transition to electric buses represents a central strategy for improving air quality, reducing urban noise pollution, and decreasing greenhouse gas and particulate emissions from public transportation. This study explores the multifaceted factors influencing energy consumption in electric vehicle (EV) buses, a critical consideration for sustainable urban transportation. By synthesizing existing literature, we present a preliminary framework that categorizes these influencing factors into several key dimensions: vehicle, operational practices, and environmental conditions. This framework aims to provide a comprehensive understanding of the interplay between these factors, offering insights for stakeholders in the transportation sector to optimize energy use in EV buses. The findings underscore the necessity of an integrated approach to improve the sustainability and efficiency of electric public transportation systems.

PANEL DISCUSSION*: Cost of the Energy Transition – Reality vs Myths and Promises

Speakers: Rawan AKKOUCH, Laura ANDOLFI, Lorenzo Matthias BURCHERI, Joachim GESKE, Timothée Jules HORNEK, Estibalitz Ruiz IRUSTA, Quoc Viet NGUYEN, Sergio POTENCIANO MENCI, Christine Van STIPHOUDT
Institution: University of Luxembourg

SUMMARY

The panel discussion explored different dimensions of the controversial topic of energy transition costs, structured into three thematic rounds: technology costs, system costs, and economic costs. Each round began with individual statements from the panelists, followed by an interactive discussion with the audience. The guiding questions addressed 1) whether the energy transition is prohibitively expensive or increasingly affordable due to falling technology costs; 2) whether hidden system costs (such as for system services) pose a significant risk or are outweighed by the benefits of avoided climate damages; and 3) whether the transition threatens Europe's competitiveness or offers a new engine for growth. Two opposing perspectives were represented in each round: one perspective framed the transition as a cost burden, the other one as a smart investment. Audience perceptions were assessed through interactive polls conducted before and after the discussion.

**Disclaimer: The statements and positions expressed by the debaters are provided for informational purposes only and are not a reflection of their stance, thus shall not be deemed binding upon them in any form.*

GENERATIVE ARTIFICIAL INTELLIGENCE WORKSHOP

DEBATE*: Should the development of AI technologies be accelerated or slowed down?

Speakers: Pratyush DIKSHIT, Pol HÖLZMER, Amir SARTIPI, Igor TCHAPPI, Evgenia Yvonni TSELONI, Ayah THARWAT, Quoc Viet NGUYEN, Qianbo ZANG
Institution: University of Luxembourg

SUMMARY

The debate sought out to discuss an important question: should the development of artificial intelligence be accelerated or slowed down. Both perspectives were represented in each round: one perspective highlighted the advantages of acceleration and the other highlighted the advantages of slowing down. To gauge audience perceptions interactive polls were conducted before and after the each round.

As Artificial Intelligence (AI) quickly permeates into critical domains such as national security, socioeconomic systems, and environmental sustainability it presents both opportunities and challenges. On one hand, rapid development and deployment of AI-driven technologies enhance cyber resilience, strengthen strategic deterrence, and improve operational efficiency across sectors, from defense applications like anomaly detection and counter-drone systems to agricultural innovations that optimize resource use and boost productivity. Speed enables competitive advantage, fosters innovation, and supports crisis response capabilities. On the other hand, unchecked acceleration risks undermining fundamental rights, legal coherence, and institutional preparedness. High-risk AI systems, if deployed prematurely, may compromise privacy, equality, and democratic values, while exacerbating hardware and software dependencies on non-EU actors, threatening Europe's technological sovereignty. Furthermore, rapid adoption can strain environmental resources and deepen socioeconomic disparities, challenging the EU's climate and social stability commitments. A balanced approach, combining strategic pacing with robust governance, is essential. This equilibrium ensures that progress remains efficient, resilient, and sustainable, while safeguarding trust, security, and autonomy as Europe navigates the global AI race. Achieving this balance is far from straightforward, as it demands careful consideration of every dimension, of innovation, governance, trust, and autonomy because overlooking any element risks undermining the entire effort.

**Disclaimer: The statements and positions expressed by the debaters are provided for informational purposes only and are not a reflection of their stance, thus shall not be deemed binding upon them in any form.*