

SUNRISE 2025: 3rd Workshop on SecUre aNd Resilient digItal tranSformation of healthcarE (SUNRISE) 2025 co-located with the 37th Norwegian ICT Conference for Research and Education (NIKT 2025),

24 November 2025, Halden, Norway

Location: Room: D1-055/56

Program

12:30-13:15

Welcome and Lunch (Rom: Aud 6 / Kantine)

13:15 – 13:45

Invited Keynote 1

Chair: Sandeep Pirbhulal, Norsk Regnesentral (NR), Norway

Invited Keynote Title: Enhancing Trust and Security in Healthcare Robotics: Challenges and Opportunities

Abstract: TBD

Speaker: Sabarathinam Chockalingam, Institute for Energy Technology (IFE), Norway

13:45 – 14:45

SESSION 1: Cybersecurity for IoT-based Healthcare

Chair: Sandeep Pirbhulal

- **Blockchain-Based Data Provenance Architecture for IoMT-based Healthcare Systems Decision**

Presenter: Noah Holmdin, SINTEF, Norway

Abstract: The healthcare sector increasingly relies on personal Internet of Medical Things (IoMT) devices for clinical decision-making and research. However, low-cost consumer devices introduce fundamental trust challenges. IoMT devices such as smartwatches and smart rings are prone to cyberattacks and data manipulation due to trade-offs between security, cost, and performance. This paper addresses the challenge of establishing verifiable data provenance for health information from inherently untrusted personal IoMT devices. Our approach leverages Hyperledger Fabric to maintain immutable and distributed provenance records, enabling transparent data lifecycle tracking across organizational boundaries. The architecture integrates privacy-preserving authentication mechanisms, including national electronic identification systems, and fine-grained access controls through organizational channels and private data collections. A proof-of-concept implementation supports multi-organizational networks with comprehensive operations for dataset registration, modification, deletion, querying, and history retrieval. Our results demonstrate that trustworthy and auditable health data exchange can be achieved across healthcare and research institutions while preserving privacy and ensuring regulatory compliance without requiring inherent trust in the underlying devices

- **A Systematic Review of Experimentally Validated Authentication Schemes for 5G/6G Smart Healthcare Edge Devices**

Presenter: Ali Hassan Sodhro, HKR, Sweden

Abstract: The integration of 5G/6G networks with smart healthcare has accelerated the use of Internet of Medical Things (IoMT) devices at the edge, where authentication is critical for security and patient safety. This paper presents a systematic review of authentication schemes for 5G/6G IoMT edge devices, focusing on works with simulation or prototype-based validation. After a rigorous screening process, 22 studies from 2020-2025 were analyzed. We categorize them into lightweight cryptographic, AI/ML-based, and blockchain-based approaches, consolidating key metrics like latency, energy cost, and accuracy. Our findings reveal a clear trade-off: lightweight crypto offers minimal latency (1.6ms) for constrained devices, AI/ML enables context-aware authentication with high handover success (99%), and blockchain provides decentralization at the cost of higher latency (400ms+). A significant gap was found in the experimental validation of PUF-based schemes. The study identifies challenges such as the lack of standardized benchmarks and real-world deployments, and recommends future work on hybrid models, lightweight post-quantum cryptography, and energy-adaptive authentication to bridge the gap between theoretical design and practical deployment in secure healthcare systems

- **Aurora-Fuzzware: Bridging the Gap to Enable Practical Fuzzing of Microcontroller-Based IoT Devices**

Presenter: Noah Holmdin, SINTEF, Norway

Abstract: Firmware fuzzing has proven to be a useful tool for discovering vulnerabilities in embedded devices, but it requires a significant level of expertise to yield meaningful results. In this paper we have shown how using Fuzzware for embedded medical devices can be simplified using our custom configuration script. We validated our approach through three 24-hour fuzzing experiments using different configurations, as well as through a questionnaire completed by one of our industry partners. The results show that (i) the configuration tool successfully generates working configurations for nRF52 binaries developed with the NSDK 15.3, (ii) workflow-guided optimizations identified through Aurora-Fuzzware significantly improve coverage, and (iii) although the configuration tool is relatively user-friendly, there remains clear room for improvement. To bridge the gap between academic prototypes and practical industrial use, future research should emphasize improving the usability and overall user experience of fuzzing frameworks.

14:45:15:45

SESSION 2: Digital Twins and Cyber Campus for Healthcare Systems

Chair: TBD

- **Navigating Cybersecurity Compliance: The Cyber Compass for Medical Device Manufacturers (Invited Paper)**

Presenter: Bjørn Magnus, SINTEF, Norway

Abstract: Connected Medical Devices (CMDs) show great potential for improving patients' quality of life, and manufacturers work tenaciously to bring such products to market as quickly as possible. However, to protect patients, CMDs must be developed in accordance with applicable regulations. Manufacturers therefore need not only to identify and implement relevant requirements for their CMDs, but also to document their product lifecycle management, risk management approach, and cybersecurity strategy. Inspired by curated cybersecurity management lists in other domains ("Awesome Lists"), the Cyber Compass tool has been developed to provide a similar

overview of relevant cybersecurity resources for the healthcare sector. With its user-friendly interface and crowd-sourced nature, the tool helps manufacturers navigate and filter regulatory resources, easing the compliance burden. Beyond simply identifying relevant documents and requirements, the tool also addresses the greater challenge of fully understanding regulatory expectations and implementing appropriate measures for all stakeholders involved throughout the CMD's lifecycle. Results from the evaluation of the Cyber Compass tool indicate that CMD stakeholders can successfully use the tool for this purpose.

- **Towards Implementing and Analyzing the Adaptive Cognitive Digital Twins Architecture for Achieving Resilient Healthcare Infrastructures and Services**

Presenter: Sandeep Pirbhulal, NR, Norway

Abstract: The healthcare sector has a profound impact on individuals, society, and the global economy, as everyone requires healthcare services at some point in their lives. This demand is growing, particularly with an increasing elderly population driven by advancements in medical science and technology. However, cyber-attacks against healthcare infrastructures and services are also rising, partly because attackers can gain substantial financial benefits from successful breaches. This underscores the need for research on how to achieve a new paradigm of resilient healthcare infrastructures and services. In this context, the Adaptive Cognitive Digital Twins (ACDT) architecture was introduced at SUNRISE 2024 as an innovative approach to enabling resilience in healthcare systems. In this paper, we examine how to model the ACDT architecture, what mechanisms can be incorporated into implementing resilient healthcare infrastructures and services, and which metrics can be used to assess their resilience. This work represents a significant step toward instantiating the abstract ACDT architecture in real-world systems.

- **ACDT-IT: An Architecture of Adaptive Cognitive Digital Twins for Resilient IT Infrastructures and Services**

Presenter: Sandeep Pirbhulal, NR, Norway

Abstract: Assuring the cybersecurity and resilience of IT infrastructures has challenged researchers and practitioners for decades. Despite combined efforts across industry, academia, and government, cyber incidents remain pervasive. This raises a key question: What new cybersecurity architecture could better enhance the security and resilience of IT systems? This paper proposes a novel architecture that integrates Digital Twins—an approach not yet systematically explored for IT cybersecurity maps directly to the NIST Cybersecurity Framework (CSF) 2.0 and introduces a seven-layer design. The architecture builds upon existing mechanisms such as intrusion detection, firewalls, and cryptographic solutions, while incorporating emerging techniques like zero trust.

15:45 –15:50

Closing Session: Conclusion & Planning

Chair: Sandeep Pirbhulal