Call for Participation

We invite you to join us in **3rd International Conference on Security & Applications (SECURA 2025)**

This conference focuses on all technical and practical aspects of Security and its Applications. The goal of this conference is to bring together researchers and practitioners from academia and industry to focus on understanding modern security research trends and applications to establishing new collaborations in these areas.

Highlights of SECURA 2025 include:

- 8th International Conference on Electrical Engineering (ELEN 2025)
- 3rd International Conference on Artificial Intelligence and IoT (AIIoT 2025)
- 3rd International Conference on Embedded Systems and VLSI (EMVL 2025)
- 3rd International Conference on Education & Technology (EDUT 2025)
- 3rd International Conference on NLP & Signal Processing (NLPSIG 2025)
- 8th International Conference of Advances in Materials Science and Engineering (MATE 2025)
- 8th International Conference on Bioscience & Engineering (BIOSE 2025)
- 8th International Conference on Mechanical Engineering (MEN 2025)
- 3rd International Conference on Computer Science and Software Engineering (CSSE 2025)
- 3rd International Conference on Managing Value, Supply Chains and Public Sector Information Technology (MVSCIT 2025)

Registration Participants

Non-Author / Co-Author/ Simple Participants (no paper)

100 USD (With proceedings)

Here's where you can reach us: secura@secura2025.org (or) securaconf@gmail.com

Accepted Papers

Ai-driven Peripheral Device Management and Assistive Multi-modal Input for Wireless Human-computer Interaction

Minzhou Wang1 and Peijin Du2, 1Independent Researcher, Charlotte, USA, 2Independent Researcher, Los Angeles, USA

ABSTRACT

This paper explores AI-assisted peripheral management techniques that improve traditional input methods through modular and linear layouts combined with voice-based support. Modular and linear approaches let users construct macros with temporal logic, enabling faster setup and more intuitive execution. Voice models extend accessibility by allowing disabled users to configure and later trigger complex key combinations through simplified inputs. Two experiments evaluated these methods: one compared modular/linear layouts with free-design in terms of setup time, consistency, accuracy, and satisfaction; the other tested AI-optimized layouts with gaze heatmaps. Results show faster setup, fewer errors, and improved accessibility.

Keywords

Human-Computer Interaction, Machine Learning, Voice-Based AI, Accessibility, Game and Software Engineering, Natural Language Processing, Software Engineering, Automation.

Advancements in Machine Learning Algorithms with Self-update Parameter Calibration for DDOS Intrusion Detection: A Literature Review

Ainebyoona Patrick and Adeleke Raheem Ajiboye, Department of Computer Science, Kampala International University, Uganda

ABSTRACT

Distributed Denial of Service (DDoS) attacks have become some of the most common and damaging cyberthreats in our increasingly connected world. This literature review explores recent developments in using machine learning algorithms to detect DDoS intrusions, with a special emphasis on approaches that fine-tune self-updating parameters. By bringing together insights from multiple recent studies. This review examines a variety of machine learning methods such as Random Forest (RF), Support Vector Machine (SVM), and K-Nearest Neighbours (KNN). It looks at the strengths and weaknesses of each technique and discusses how best to integrate them with the existing security infrastructure. Particular attention is given to self-updating models that can quickly adapt to new and evolving attack patterns. The paper also reviews performance metrics, important considerations around datasets, and outlines future research directions in this fast-moving area. Overall, the findings indicate that adaptive, self-updating machine learning models outperform static ones in detecting complex DDoS attacks, with Random Forest approaches consistently delivering strong results across various studies.

Keywords

DDoS detection, self-updating algorithms, Adaptive Parameter Calibration, Intrusion Detection Systems. Machine learning.

APost-Quantum OTP Authentication in a Trusted Execution Environment: Implementation with ML-DSA and OP-TEE

Mamadou Cherif Kasse1 and El Hadj Modou Mboup2, 1Cheikh Anta Diop University of Dakar, FST, DMI, LACGAA, Senegal, 2Iba Der Thiam University of Thiès, Senegal

ABSTRACT

In light of emerging quantum threats, traditional authentication mechanisms, particularly those based on One-Time Passwords (OTP), are becoming increasingly inadequate. This paper introduces a post-quantum authentication model that combines an OTP scheme derived from the ML-DSA signature (from the PQClean project) with a Trusted Execution Environment (TEE). The TEE ensures secure generation, storage, and usage of critical cryptographic components, thereby strengthening resistance to both software and hardware attacks. This approach offers a robust solution to modern security challenges. A comprehensive security analysis and discussion position this model as a credible and scalable alternative for authentication in a post-quantum world.

Keywords

Trusted Execution Environment (TEE), Post-Quantum Cryptography, Digital Signature, PQClean, Authentication, OTP, Secure Key Storage.

Securing Agentic AI: A Comprehensive Threat Model and Mitigation Framework for Generative AI Agents

Vineeth Sai Narajala1 and Om Narayan2, 1Washington State University, Washington, USA, 2New York University, New York City, New City, USA

ABSTRACT

As generative AI (GenAI) agents become more common in enterprise settings, they introduce security challenges that dif er significantly from those posed by traditional systems. These agents aren't just LLMs—they reason, remember, and act, often with minimal human oversight. This paper introduces a comprehensive threat model tailored specifically for GenAI agents, focusing on how their autonomy, persistent memory access, complex reasoning, and tool integration create novel risks. Our research identifies 9 primary threats and organizes them across five key domains: cognitive architecture vulnerabilities,temporal persistence threats, operational execution vulnerabilities, trust boundary violations, and governance circumvention. These threats aren't just theoretical—they bring practical challenges such as delayed exploitability, cross-system propagation, cross system lateral movement, and subtle goal misalignments that are hard to detect with existing frameworks and standard approaches. To help address this, we present two complementary frameworks: ATFAA (Advanced Threat Framework for Autonomous AI Agents), which organizes agent-specific risks, and SHIELD, a framework proposing practical mitigation strategies designed to reduce enterprise exposure. While this work builds on existing work in LLM and AI security, our focus is squarely on what makes agents dif erent—and why those dif erences matter. Ultimately, this research argues that GenAI agents require a new lens for security. If we fail to adapt our threat models and defenses to account for their unique architecture and behavior, we risk turning a powerful new tool into a serious enterprise liability.

Keywords

Terms—generative AI, threat model, AI agents, cybersecurity, attack vectors, security framework.

Anomaly Detection in Network Traffic using Selected Statistical and Entropy-based Features

Rakhmatov Furkat1 and Karimov Norbek2, 1Faculty of Computer Engineering, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, Uzbekistan, 2Department of Methodology of Exact and Natural Sciences, Tashkent Region Pedagogical Skills Center, Bo'stonliq District, Ghazalkent City, Tashkent Region, Uzbekistan

ABSTRACT

The rapid evolution of cyber threats, particularly Distributed Denial of Service (DDoS) and other advanced attack vectors, has significantly challenged the resilience of modern network infrastructures. This study proposes an anomaly detection framework that leverages a compact yet highly informative feature set — request rate (Rt), traffic volume (Vt), source IP entropy (St), flow duration (Tt), and unique protocols (Qt) — to identify a broad spectrum of attack types, including DDoS, Slow Attacks, Volumetric Attacks, Service Outage, Application Layer Attacks, and Stealth Attacks. Using the CIC-IDS2017 dataset, we evaluated three machine learning models: Random Forest (RF), Support Vector Machine (SVM), and Extreme Gradient Boosting (XGBoost). Experimental results demonstrate that XGBoost achieves the highest detection accuracy of 99.1%, outperforming RF and SVM while maintaining an optimal trade-off between precision and recall. The findings highlight that ensemble-based models, when combined with carefully selected statistical and entropy-based features, provide robust and efficient solutions for real-time intrusion detection in diverse attack scenarios.

Keywords

TNetwork Anomaly Detection, Request Rate, Traffic Volume, Source IP Entropy, Flow Duration, Unique Protocols, Machine Learning, Intrusion Detection System

Call to Action: Reimagining Odl Instructional Approaches in Preparing Open Secondary School Students in Malawi for Evolving Global Market

Victor Pangani Phiri1, Wezi Kancheche Banda2, Modester Simwaka Malisita3, Martin Elifala4, 1Centre for Research and Consultancy, Nalikule College of Education, Lilongwe, Malawi, 2Centre for Continuing Education, Nalikule College of Education, Lilongwe, Malawi, 3Centre for Research and Consultancy, Nalikule Colle of Education, Lilongwe, Malawi, 4Faculty of Education Foundations, Nalikule College of Education, Lilongwe, Malawi

ABSTRACT

This paper investigated the effectiveness of Open distance and e-learning (ODeL) instruction in Malawi's Open Secondary School (OSS). Employing TPACK framework and concurrent mixed methods, the study sampled six OSS, involving 6 head teachers, 6 ODeL coordinators and 24 teachers. Differentiated instruction is credited for enhancing student's motivation, performance, and self-efficacy. However, findings indicated over-reliance of teacher-centered methods. Eighty-six percent of coordinators and 72% of teachers attached this to overcrowded classes and limited contact time. The study underscored the necessity to integrate technology into differentiated instructions to address these constraints. In response to the challenges, COMADI framework was developed to advance use of technology in differentiated instruction. It is

envisaged that the developed instructional framework would revolutionize the existing OSS instructional practices in open schools. This initiative aligns with Regional ODL Strategic Plan 2022–2030 and Malawi Vision 2063, promoting inclusive, self-reliant national development through effective education reform.

Keywords

effectiveness, OSS, TPACK model, differentiated instruction, COMADI framework

Learning, Education, and Technology in Deep Historical Perspective

Cornelius N. Grove, Ed.D, Independent Ethnologist of Education, New York, USA

ABSTRACT

In this meditation on children's learning from prehistoric times until today, Grove contrasts traditional child-rearing with child-rearing in our modern world. In the former, parents are not responsible for the rearing and learning of their children, who are cared for by an older sibling. Youngsters learn everything they need to know by observation and imitation of adults. How did humans get from that to modern education and technology? Grove imagines a prehistoric scene in which a child queries an aunt who had devised a way of record-keeping. She had begun to think using abstractions. If the child's going to learn that, his aunt must formally instruct him. In microcosm, this is the story of today's highly technological world, the product of abstract and symbolic thought. Too cerebral to be learned by observation and imitation, it must be learned via formal instruction. Without formal instruction, technologically advanced societies would not exist.

Keywords

Children's learning, Applied anthropology of education, Child-rearing practices, Ethnology, Cultural history

About Ontology,absoluteness-relativity of Scientific Cognition and the Unified Method Substantiation Ofscientific Theories.

Alexander Voin, International Solomon University, Ukraine

ABSTRACT

The problem of ontology is inextricably linked with the problem of absoluteness-relativity of scientific knowledge. The article shows the erroneousness of the solution of these problems both in the classical rationalism of Descartes, Pascal, Bacon, Newton, which absolutized scientific knowledge, and in the post-positivism of Quine, Kuhn, Feyerabend, Popper, Lakatos that replaced it, which excessively relativized it. The article proposes a solution to these problems based on the unified method of substantiation of scientific theories developed by the author.

When replacing one theory substantiated by a unified method of substantiation with another (Newton - Einstein), although contrary to classical rationalism, the definitions of concepts (that means ontology) and formulas change, but contrary to post-positivists, both theories guarantee the truth of their predictions with a given accuracy and probability in the area of action of each of these theories. Only these areas do not coincide. (The area of action of the theory of relativity is larger than the area of Newton's mechanics and includes it).

Keywords

ontology, concept, theory, truth, cognition

Ozqyrqbert - Towards a Universal Turkic Language ¨part-of-speech Tagger

Yuanhao Zou, Nikhil Lyles, Stanford University, USA

ABSTRACT

Part-of-speech (POS) tagging for low-resource languages presents unique challenges due to limited annotated data and suboptimal tokenization. For this project, we make the first steps towards building a universal Turkic Language Part-of-Speech Tagger by developing OzQyrqBERT, a model that ¨ performs the task on both Uzbek and Kyrgyz, with the latter being a low resource language. We fine-tune an Uzbek POS tagging model on Kyrgyz data, systematically improving performance through enhanced tokenization. We evaluate our model using accuracy and confusion matrices, demonstrating how improved tokenization significantly reduces misclassifications. Our results highlight the effectiveness of adapting models from linguistically related languages for low-resource NLP tasks.

Integrating Predictive Compliance and High-Voltage Safety Monitoring in AI-based Power Systems for Data Centers

Chirag Devendrakumar Parikh, Computer Engineering, California State University, Fullerton, CA, USA

ABSTRACT

The engineering challenge of continuously complying with safety protocols for high-voltage systems in hyperscale data centers, which deploy AI power management systems to handle high-performance compute workloads, becomes even more difficult. This issue is addressed in the paper by proposing an integrated framework that combines real-time high-voltage hazard alert systems with compliance monitoring and is further enhanced by predictive compliance strategies. The described methods and solutions permit the embedded intelligent control systems to tackle

adaptive diagnostics and highly advanced sensor networks and extend their functionality to the power systems to detect early non-conformant conditions and electrical threats to safety. AI-based engines applied to real-time compliance data evaluation enhance the decision processes regarding maintenance, alterations, and updates of the structure in question, and even to the regulations that govern it. Compliance with UL 61010, UL 62368-1, IEC 61010, IEC 62477, and other critical safety standards is also fully observed in the paper, making sure that equipment and processes used will not pose unnecessary hazards. The paper addresses simulations in high-density rack-level power distribution, uninterruptible power supplies, and busway systems, focusing on the application of predictive compliance and high-voltage safety monitoring, reporting reduced operational downtime and enhanced reliability. The intention is to redesign the next generation of data centers by eliminating the traditional approach to risk management and replacing it with an intelligent compliance approach.

Keywords

Compliance, Product Safety, Data Centers, AI, Global Market Access, Safety