2nd AICLOUDSEC: Securing the Future – Navigating the Intersections of AI, Cloud, and IoT

Special Track running alongside CLOUD COMPUTING 2025, The Sixteenth International Conference on Cloud Computing, GRIDs, and Virtualization, April 6, 2025 to April 10, 2025 – Valencia, Spain

Andreas Aßmuth[*], Sebastian Fischer[†], and Christoph P. Neumann[‡]

[*]Faculty of Computer Science and Electrical Engineering
Kiel University of Applied Sciences, Kiel, Germany
e-mail: andreas.assmuth@fh-kiel.de

[†]Department of Computer Science and Mathematics
Ostbayerische Technische Hochschule Regensburg, Regensburg, Germany
e-mail: sebastian.fischer@oth-regensburg.de

[‡]Department of Electrical Engineering, Media, and Computer Science
Ostbayerische Technische Hochschule Amberg-Weiden, Amberg, Germany
e-mail: c.neumann@oth-aw.de

***Abstract*—Companies have been using machine learning for several years now, for example to search for patterns in large amounts of data. However, it is only in recent years that artificial intelligence has left the niche of specialised applications. Since the public availability of large language models and generative artificial intelligence, new and innovative ideas and applications for their use are constantly emerging. Many of these new services are offered as cloud services. In this global gold-rush atmosphere, however, some downsides are now also coming to light. Not only the good guys are using AI, but also the bad guys. Known attacks against services in the cloud can be greatly improved or simplified by artificial intelligence. Attackers can also use machine learning to search large amounts of data in order to find vulnerabilities. And last but not least, despite all the euphoria, some users forget that these new cloud-based AI services can also be interesting targets for cyberattacks.**

At last year's conference, a special track was dedicated to the intersection of cloud, Internet of Things, security and AI. Due to the interest, the unbroken global AI hype and also new attacks with and against AI services, this complex of topics is discussed in another special track.

***Keywords*-artificial intelligence; cloud computing; internet of things; security; privacy.**

I. Introduction

In the digital age, where Artificial Intelligence (AI) has evolved from a distant vision to a ubiquitous force shaping our daily lives and work, the challenges and dangers accompanying this technological revolution have also intensified. The proliferation of AI services across the Internet has ushered in a new era of convenience for users, ranging from text translation to the generation of computer graphics based on simple text descriptions. However, with this widespread use, these systems and the computing systems in the cloud that are used to provide them have become interesting targets for cyber criminals.

We are now witnessing an increasingly sophisticated landscape of targeted attacks against AI systems. These attacks range from manipulating artificial intelligence to achieve desired, often malicious outcomes, to model stealing attacks, to misusing generative AI technology for creating phishing emails, forging voices, or producing convincingly real images and videos (deepfakes) boosting social engineering attacks. In February 2024, for example, a company in Hong Kong was tricked into sending a multimillion-dollar transfer after an employee participated in a video call. What the employee didn't realize was that the other 'people' in the call, including someone who looked and sounded like the CFO, were actually fake, created using generative AI.

IoT devices are often interconnected with cloud services, and successful attacks against these cloud services can have significant repercussions for the IoT devices themselves. Similarly, attacks on or manipulations of (numerous) IoT devices can also have consequences for the associated cloud services – even if it's only in terms of receiving incorrect sensor data. This, in turn, could invalidate calculations in the cloud aimed at optimizing the operating parameters of the IoT devices, essentially rendering them useless, for instance. Thus, it is essential to also focus on attacks targeting IoT devices or cloud services connected to these devices. These attacks can be AI-powered or traditional, underscoring the importance of comprehensive security strategies that consider both, the cloud and the IoT ecosystem. This special track continues the reflections and discussions from CLOUD COMPUTING 2024. It aims to explore the intersections between cloud computing, security, and artificial intelligence. We invite researchers, practitioners, and experts to submit contributions on all topics related to this convergence.

II. Submissions

A total of nine contributions were accepted for the special track, ranging from academic research to industrial applications.

Stangl and Neumann [1] introduce Kosmosis, for rug pull detection and prevention in blockchains. It implements an incremental knowledge graph construction that integrates semantically-enriched blockchain data with social media insights into a unified knowledge graph. Kosmosis extracts semantic information from blockchain transactions using the application binary interface to decode smart contract interactions and tag addresses based on their extracted relationships. Currently, the prototype is limited to blockchains utilizing the account-based accounting model, like Ethereum. By extending the graph with social media data, it allows for extended analysis, where knowledge about on-chain behaviors and social media interactions can be correlated, to detect anomalous patterns and assign blockchain addresses with risk scores. Thus, Kosmosis aims to provide the basis for a more comprehensive understanding of blockchain ecosystems and to contribute to the development of robust anti-fraud measures.

Fürst and Aßmuth explore in their paper [2] the feasibility of acoustic side-channel attacks to infer typed passphrases using unsupervised learning. The authors demonstrate that keyboard acoustic emanations can be exploited without prior training data, enabling attackers to recover passphrases more efficiently than brute-force methods. Experimental results show that mechanical keyboards are particularly vulnerable, and combining partial passphrase recovery with a dictionary attack significantly reduces attack complexity. The findings highlight the risks of relying solely on passwords and emphasize the need for stronger authentication mechanisms.

Mehra, Aßmuth, and Prieß [3] introduce the Graph of Effort (GOE) as a method to quantify the risk of offensive AI in vulnerability assessments. As AI becomes more powerful, attackers can leverage it to automate exploits, making certain vulnerabilities more dangerous. The GOE model assesses the effort required for AI-based attacks across different stages of an intrusion kill chain, factoring in automation tools, trainable models, and data availability. By integrating GOE with established frameworks like CVSS, security analysts can better prioritize AI-driven threats. Examples on real vulnerabilities demonstrate how GOE provides a structured, intuitive approach to evaluating AI-assisted cyberattacks.

Eggendorfer and Andresen [4] highlight in their paper the urgent need for security metrics to evaluate and improve IoT and embedded system security. Due to their widespread adoption and inherent vulnerabilities, IoT devices are often exploited in cyberattacks, yet patching them remains challenging due to operational constraints. The authors propose a measurable security metric to assess IoT security levels, aiding procurement decisions and regulatory enforcement. They argue for legislative support, suggesting mandatory testing and certification similar to other critical industries. By implementing standardized security assessments, organizations can enhance cyber resilience and mitigate risks associated with insecure IoT ecosystems.

Reichel et al. [5] investigate GNSS spoofing attacks on autonomous vehicles, focusing on detection methods both during and after an attack. They analyze data storage strategies essential for forensic analysis, emphasizing the importance of preserving position, signal, and camera data. The study also proposes a simulation setup to evaluate relevant forensic data and assesses existing data frameworks for their suitability in detecting spoofing attacks.

Stey et al. [6] introduce the Genetic Fuzz Data Generator (GFDG), a fuzzing method that leverages Genetic Algorithms and side-channel analysis to enhance Controller Area Network (CAN) security testing. GFDG dynamically refines its fuzzing strategy by analyzing side-channel data, such as processing unit temperatures and power supply variations, to evaluate system responses. By structuring CAN messages as genetic individuals and applying evolutionary principles—selection, crossover, and mutation—GFDG systematically identifies active CAN IDs and generates targeted fuzz messages. Experimental validation on a real automotive Electronic Control Unit in a controlled lab environment demonstrated its effectiveness, uncovering system anomalies, including a Denial of Service vulnerability that disrupted ECU functions. The results highlight the potential of feedback-driven fuzzing for improving black-box security testing in CAN-based systems, with future research focusing on optimizing fitness functions and exploring additional side-channel metrics.

Graf et al. [7] present a decentralized approach to securing charging infrastructure in private and semi-public sectors by enhancing resilience through context-based security mechanisms. They propose an architecture that integrates data acquisition, information exchange, and analysis methods to efficiently monitor Electric Vehicle Supply Equipment systems. As part of the "Resiliente und Sichere Ladeinfrastruktur" research project, the architecture connects charging hardware with a scalable Peer-to-Peer cybersecurity mesh network and AI-supported analysis processes. Key security tasks—including detection, reaction, attribution, and prevention—are addressed through a shared information space that aggregates data from different domains. Context data, such as charging procedures, network communication parameters, system loads, and Open Charge Point Protocol parameters, are collected and analyzed for attack monitoring and classification.

Folger et al. [8] introduce a Transformer-based architecture for anomaly detection in multivariate time series, leveraging self-attention to efficiently process high-dimensional sensor data with minimal feature engineering. This approach enables early detection of unusual patterns to prevent critical system failures. In a laboratory setup, the framework will be applied to an Electronic Control Unit using fuzzing techniques to induce anomalies while monitoring side channels, such as temperature, voltage, and Controller Area Network (CAN) messages. The paper details the model's structure, preprocessing steps—including temporal aggregation and classification—and hyperparameter optimization. The evaluation demonstrates that the model robustly handles anomaly scenarios, though further research is needed to assess its applicability in cloud environments and the Industrial Internet of Things. Overall, the findings highlight the potential of Transformer models for automated and reliable monitoring of complex time series data.

Ahmeti et al. [9] describe a multilayered architecture concept that integrates Hyperledger Fabric into the Gaia-X ecosystem to address the challenges of securing and managing distributed data. They propose using advanced encryption methods and smart contracts for securely distributing fragmented data and ensuring access only for authorized actors. This approach aims to enhance digital sovereignty and scalability within Gaia-X-compliant data spaces, serving as a conceptual foundation for future technical validation and development.

III. Conclusions

The 2nd AICLOUDSEC special track includes a broad range of topics related to AI, security and the influence on Cloud services and the Internet of Things. It contains both, academic research papers as well as studies from industry introducing interesting ideas for future work in this thriving research domain.

Acknowledgment

We would like to thank the organizers of Cloud Computing 2025 for their tireless efforts and for accepting 2nd AICLOUDSEC as a special track. Last, but not least, we are very thankful to the authors for their very interesting contributions.

References

[1] P. Stangl and C. P. Neumann. “Kosmosis: Crypto Rug Pull Detection and Prevention by Fusing On- and Off-Chain Data in a Knowledge Graph,” in Special Track: Securing the Future – Navigating the Intersections of AI, Cloud, and IoT (2nd AICLOUDSEC), along with Cloud Computing 2025. IARIA XPS Press, 2025.

[2] D. Fürst and A. Aßmuth. “Practical Acoustic Eavesdropping On Typed Passphrases,” in Special Track: Securing the Future – Navigating the Intersections of AI, Cloud, and IoT (2nd AICLOUDSEC), along with Cloud Computing 2025. IARIA XPS Press, 2025.

[3] A. Mehra, A. Aßmuth, and M. Prieß. “Graph Of Effort: Quantifying Risk of AI Usage For Vulnerability Assessment,” in Special Track: Securing the Future – Navigating the Intersections of AI, Cloud, and IoT (2nd AICLOUDSEC), along with Cloud Computing 2025. IARIA XPS Press, 2025.

[4] T. Eggendorfer and K. Andresen. “On The Necessity of Measuring Security in IoT,” in Special Track: Securing the Future – Navigating the Intersections of AI, Cloud, and IoT (2nd AICLOUDSEC), along with Cloud Computing 2025. IARIA XPS Press, 2025.

[5] T. Reichel, M. Gerstner, L. Schuller,A. Attenberger, R. Hackenberg, and K. Dološ. “A Forensic Analysis of GNSS Spoofing Attacks on Autonomous Vehicles,” in Special Track: Securing the Future – Navigating the Intersections of AI, Cloud, and IoT (2nd AICLOUDSEC), along with Cloud Computing 2025. IARIA XPS Press, 2025.

[6] M. Stey, M. Hachani, P. Fuxen, and R. Hackenberg. “GFDG: A Genetic Fuzzing Method For The Controller Area Network Protocol,” in Special Track: Securing the Future – Navigating the Intersections of AI, Cloud, and IoT (2nd AICLOUDSEC), along with Cloud Computing 2025. IARIA XPS Press, 2025.

[7] J. Graf, C. Moser, P. Fuxen, and R. Hackenberg. “Intrusion Detection using Peer-to-Peer Distributed Context-Information for Electric Vehicle Supply Equipment,” in Special Track: Securing the Future – Navigating the Intersections of AI, Cloud, and IoT (2nd AICLOUDSEC), along with Cloud Computing 2025. IARIA XPS Press, 2025.

[8] F. Folger, M. Hachani, P. Fuxen, J. Graf, S. Fischer and R. Hackenberg “A Transformer-Based Framework For Anomaly Detection in Multivariate Time Series,” in Special Track: Securing the Future – Navigating the Intersections of AI, Cloud, and IoT (2nd AICLOUDSEC), along with Cloud Computing 2025. IARIA XPS Press, 2025.

[9] L. Ahmeti, K. Dolos, C. Meyer, A. Attenberger, and R. Hackenberg “Theoretical Integration of Hyperledger Fabric in Gaia-X: Towards an Approach For Federated Data Access,” in Special Track: Securing the Future – Navigating the Intersections of AI, Cloud, and IoT (2nd AICLOUDSEC), along with Cloud Computing 2025. IARIA XPS Press, 2025.