


AICLOUDSEC: AI – Curse or Blessing for the Security of Cloud Services?

Special Track running alongside CLOUD COMPUTING 2024, The Fifteenth International Conference on Cloud Computing, GRIDs, and Virtualization, April 14, 2024 to April 18, 2024 - Venice, Italy

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

*Department of Electrical Engineering, Media, and Computer Science
Ostbayerische Technische Hochschule Amberg-Weiden, Amberg, Germany
e-mail: {a.assmuth|c.neumann}@oth-aw.de

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

Abstract—The convergence of cloud computing, security, and artificial intelligence presents new challenges and opportunities. This special track explores how artificial intelligence can enhance the security of cloud services and addresses novel attack techniques leveraging artificial intelligence. Topics include defending against attacks on cloud-based artificial intelligence services, vulnerabilities in artificial intelligence models, and threats to Internet of Things devices impacting cloud services. In summary, the special track aims to advance understanding and solutions for securing cloud environments and connected Internet of Things domains by applying artificial intelligence methods and techniques but also if such methods are used by the adversaries in new and advanced attacks.

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

I. INTRODUCTION

Artificial Intelligence (AI) is currently a hype topic that has long been discussed beyond a circle of experts to the general public. More and more AI services are being made available via the Internet, enabling users to translate their texts or generate computer graphics based on simple text-based descriptions. Additionally, methods of machine learning have already been used in industry to optimize processes and process parameters or to optimally plan the maintenance of the machines used through predictive maintenance. So, Cloud-based AI services are already available, which is reason enough to think about their security.

This special track wanted to address all topics related to the intersection of cloud computing, security, and AI. Contributions describing how AI methods could be used to better detect or prevent attacks against cloud services or cloud-based AI services were as relevant as novel attack techniques against cloud services in which AI methods are used to prepare or conduct the attacks. Another topic was attacks against AI models themselves, i.e., questions such as how can AI models be manipulated so that their output corresponds to what an attacker wants, or how can such attacks be detected and prevented.

As in previous years, devices and services connected to cloud services were also considered, which could also be affected by

the attacks described, i.e., attacks against Internet of Things (IoT) devices of any kind that can have an impact on cloud services were also of interest to the special track.

II. SUBMISSIONS

A total of eight contributions were submitted for the special track, ranging from academic research to industrial and military applications.

Whether in peace-keeping, emergency-relief or even police operations, participants need situational awareness to provide their best service. Often, in these situations, organisations with a different background and mission need to cooperate, however for privacy, confidentiality and in military and police operations, for tactical reasons, information exchange needs to be regulated. In their paper, Tobias Eggendorfer and Gerhard Schwarz propose a multi-tenant multi-domain situational awareness system to support such operations [1].

In the field of military operations, effective and efficient collaboration following the NATO Network-enabled Capability concept for Multi Domain Operations has to be conquered against adversaries as well as other handicaps. Best practices force the segmentation of the user’s “virtual” information space into different security domains. In order to achieve information flow across these separated enclaves, the concept of a dynamic shared information space based information exchange controlled via a security gateway using REST and JSON is outlined and discussed [2].

Pitpimon Choorod has developed a method for distinguishing Tor traffic from other encrypted network traffic, which she presented in her PhD thesis. It is not yet entirely clear why character analysis using machine learning methods has such high success rates. Since the Tor network encrypts data traffic multiple times due to its operating principle, other security protocols usually only encrypt the data once. In this paper, the results of recent experiments investigating the impact of the number of encryptions on the ability to distinguish Tor from non-Tor encrypted traffic are discussed [3].

The paper “Automated Vulnerability Scanner for the Cyber Resilience Act” introduce two prototypes for tools, to help

device manufacturers to implement the necessary security for the Cyber Resilience Act of the EU. The first tool provides a digital checklist for product classification and a prototype to streamline the analysis and monitoring of the security state of software along the software development life cycle. The second tool provides an automated vulnerability scanner with Static Application Software Testing and Software Component Analysis. These testing steps that can be automated and documented for the purpose of the Cyber Resilience Act [4].

The paper entitled “Vocabulary Attack to Hijack Large Language Model Applications” by Patrick Levi and Christoph P. Neumann is about hijacking Large Language Models (LLMs) decorating a user prompt with normal words from the vocabulary. A method is presented to find an optimal set of words to be inserted into a user prompt to manipulate the LLM output. The attacker can trick the model into offensive language or reproducing desired content. Knowledge of the attacked model is not required for the attack to work [5].

Amir Pakmehr investigates the integration of Deep Reinforcement Learning (DRL) in fog computing to optimize task offloading for enhanced operational efficiency and security. By examining current methodologies and proposing future research directions, the paper suggests the potential of DRL to improve resource allocation, reduce response times, and bolster security against vulnerabilities. Additionally, the paper explores the synergy of DRL with blockchain technology to ensure robust, efficient, and secure fog computing environments, highlighting the need for advancing DRL and blockchain applications to address evolving challenges in fog computing task offloading [6].

The paper “MANTRA: Elevating Cybersecurity Applications Through a Privacy-Preserving CTI Sharing Platform” introduces MANTRA, a conceptual framework aimed at enhancing Cyber Threat Intelligence (CTI) sharing across organizations through a privacy-preserving model. It addresses the challenges of effective CTI dissemination, such as reputational risks, technical barriers, and data silos, by leveraging federated learning, secure protocols, and peer-to-peer communication to ensure data confidentiality, integrity, and availability. MANTRA’s architecture, encompassing a protocol layer for secure data exchange, an application layer for CTI model processing, and a federated learning layer for model aggregation, promotes a collaborative ecosystem for sharing cybersecurity intelligence. Through the integration of internal and external data sources, MANTRA aims to improve threat detection and organizational cybersecurity, presenting an advancement towards a collective defense against evolving cyber threats [7].

The paper entitled “A Forensic Approach to Handle Autonomous Transportation Incidents within Gaia-X” outlines

a forensic approach to investigating incidents related to autonomous transportation within Gaia-X. It analyses possible forensic scenarios such as vehicle control unit manipulation and Distributed Denial of Service (DDoS) attacks and proposes an investigation procedure based on the guidelines defined by the German Federal Office for Information Security [8].

III. CONCLUSIONS

The 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 and GOs introducing interesting ideas for future work in this thriving research domain.

ACKNOWLEDGMENT

We would like to thank the organizers of Cloud Computing 2024 for their tireless efforts and for accepting AICLOUDSEC as a special track. Last, but not least, we are very thankful to the authors for their very interesting contributions.

REFERENCES

- [1] T. Eggendorfer and G. A. Schwarz. “Towards Multi-Domain Multi-Tenant Situational Awareness Systems,” in Special Track: AI – Curse or Blessing for the Security of Cloud Services (AICLOUDSEC), along with Cloud Computing 2024. IARIA XPS Press, 2024.
- [2] G. A. Schwarz. “Security Enforcement Within Multiple Shared Information Space Environments,” in Special Track: AI – Curse or Blessing for the Security of Cloud Services (AICLOUDSEC), along with Cloud Computing 2024. IARIA XPS Press, 2024.
- [3] P. Choorod, T. J. Bauer, and A. AlMuth. “Distinguishing Tor From Other Encrypted Network Traffic Through Character Analysis,” in Special Track: AI – Curse or Blessing for the Security of Cloud Services (AICLOUDSEC), along with Cloud Computing 2024. IARIA XPS Press, 2024.
- [4] S. Falter, G. Brukh, M. Wess, and S. Fischer. “Automated Vulnerability Scanner for the Cyber Resilience Act,” in Special Track: AI – Curse or Blessing for the Security of Cloud Services (AICLOUDSEC), along with Cloud Computing 2024. IARIA XPS Press, 2024.
- [5] P. Levi and C. P. Neumann. “Vocabulary Attack to Hijack Large Language Model Applications,” in Special Track: AI – Curse or Blessing for the Security of Cloud Services (AICLOUDSEC), along with Cloud Computing 2024. IARIA XPS Press, 2024.
- [6] A. Pakmehr. “Task Offloading in Fog Computing with Deep Reinforcement Learning: Future Research Directions Based on Security and Efficiency Enhancements,” in Special Track: AI – Curse or Blessing for the Security of Cloud Services (AICLOUDSEC), along with Cloud Computing 2024. IARIA XPS Press, 2024.
- [7] P. Fuxen, M. Hachani, R. Hackenberg, and M. Ross. “MANTRA: Elevating Cybersecurity Applications Through a Privacy-Preserving CTI Sharing Platform,” in Special Track: AI – Curse or Blessing for the Security of Cloud Services (AICLOUDSEC), along with Cloud Computing 2024. IARIA XPS Press, 2024.
- [8] L. Ahmeti, K. Dolos, C. Meyer, A. Attenberger, and R. Hackenberg. “A Forensic Approach to Handle Autonomous Transportation Incidents within Gaia-X,” in Special Track: AI – Curse or Blessing for the Security of Cloud Services (AICLOUDSEC), along with Cloud Computing 2024. IARIA XPS Press, 2024.