FAST-CAMS: Finding a Solution to Cloud Application Maturity Security

Special Track running alongside CLOUD COMPUTING 2023, The Fourteenth International Conference on Cloud Computing, GRIDs, and Virtualization, June 26, 2023 to June 30, 2023 - Nice, Saint-Laurent-du-Var, France

Andreas Aßmuth*, Bob Duncan†, Rudolf Hackenberg‡ and Magnus Westerlund§

*Ostbayerische Technische Hochschule Amberg-Weiden, Amberg, Germany,
Email: a.assmuth@oth-aw.de
†University of Aberdeen, UK, Email: robert.duncan@abdn.ac.uk
‡Ostbayerische Technische Hochschule Regensburg, Regensburg, Germany,
Email: rudolf.hackenberg@oth-regensburg.de
§Arcada University of Applied Sciences, Helsinki, Finland, Email: magnus.westerlund@arcada.fi

***Abstract*—Cloud Computing has significantly transformed the IT landscape, offering secure and cost-effective services. The initial concerns about information security and privacy have given way to greater acceptance, as Cloud infrastructures provide quick access to new systems and scalability. The COVID-19 pandemic has underscored the robustness and reliability of Cloud services, enabling remote work and online education. In this special track, the importance of information security and privacy in Cloud, Fog, and Edge Computing, including their interfaces with the Internet of Things are discussed. It explores the challenges and opportunities associated with non-traditional scenarios and highlights the need to address data processing and security measures along the cloud journey.**

Keywords*—*Internet of Things; security; privacy.

I. Introduction

During the course of the past decade, Cloud Computing has led to an almost complete transformation of the IT landscape. The initial reluctance of many potential users to use Cloud infrastructures due to scepticism about information security and privacy has given way to greater acceptance now that moving required services to the Cloud can be achieved securely and, above all, cost-effectively compared to using self-hosted dedicated hardware. What has proven particularly attractive is the ability to access new systems quickly without having to worry about planning ahead or accessing corporate budgets, and most importantly, the ability to scale up (or down) systems as needed. The pandemic has also been a remarkable reminder of how robust and reliable Cloud services of all kinds have become. Without such robust Cloud services, working from home or home schooling would not have been possible; additionally, probably not without serious negative effects on society and economy alike.

More and more companies are now using Cloud services, even governments and non-profit organisations. For example, the Cloud opens up opportunities for small and medium-sized enterprises to conduct business on an equal footing with their larger competitors. While there we have achieved a certain robustness both in terms of information security and privacy of by now traditional Cloud services aimed at use by a very large number of users with largely domain or industry-independent usage scenarios, e. g. office services or video conference systems, there are still enormous challenges, especially for services in connection with hardware access through the Internet of Things. In a modern, digitised production plant, for instance, sensor data can be aggregated and transferred to the Cloud and back to optimise actuator operating parameters. Security issues can arise both on-site at the sensors and industrial control systems, which can then pose a threat to the Cloud services, and vice versa. Of particular interest to potential attackers and security personnel as well are these interfaces to or from Cloud services, as great damage can be done via these – both in the Cloud and possibly in several production facilities. These statements also apply comparably, for example, to medical devices that are connected to Cloud services. Basically, for all such non-traditional scenarios, it is necessary to decide at which point on the way to the Cloud or back which processing of data or security/privacy measures can take place.

This special track therefore focuses on topics related to

information security and privacy in Cloud, Fog and Edge computing as well as their interfaces in the Internet of Things.

II. Submissions

In their paper "Encrypted Container File: Design and Implementation of a Hybrid-Encrypted Multi-Recipient File Structure" [1] Bauer and Aßmuth present a tool for secure collaboration in Cloud-native software development, where international teams of developers use Cloud-based version management services like GitHub. This new tool allows secure encryption of confidential files for selected developers, while the others are not capable of decrypting it in order to get access to this sensitive information, like certificates or secret keys.

Distributed denial of service (DDoS) attacks are prevalent and challenging to defend against. Machine learning-based intrusion detection systems show promise in countering this threat, but these require datasets with real DDoS attack traffic for training. In their paper "Generation of Distributed Denial of Service Network Data with Python and Scapy" [2], Görtz, Fischer, and Hackenberg introduce a Python program that creates denial of service packets and simulates distributed sending through multithreading, generating real network traffic. Their new approach improves the quality of the dataset, providing a more accurate and error-free basis for training machine learning algorithms efficiently.

The authors of the contribution entitled "Side Channel Monitoring for Fuzz Testing of Future Mobility Systems" [3] address the challenges in cybersecurity posed by the increasing software content and connectivity in the automotive industry. In their paper, they propose fuzz testing as a security measure and explore the use of side-channel information, such as power consumption and temperature, to monitor and analyze abnormal behavior in hardware-related Electronic Control Unit testing. Their experiments involve generating fuzz data, monitoring the device under test, and analyzing the behavior of side channels during abnormal scenarios.

Pakmehr et al. address the security challenges of cloud or fog-based machine learning services in their paper entitled "Security Challenges for Cloud or Fog Computing-Based AI Applications" [4]. They highlight the importance of securing the underlying cloud or fog services to prevent impairments to machine learning applications. The paper distinguishes between AI applications used in the cloud and in fog computing networks, as these have different requirements and face different threats. The responsibilities for security differ between cloud platforms and fog computing networks, with a focus on securing user data and physical access to edge devices.

In their paper "On the creation of a secure key enclave via the use of memory isolation in Systems Management Mode" [5], Sutherland, Coull, and Ferguson describe their research on using Systems Management Mode in order to protect sensitive areas of memory from tampering and intrusion. Their approach involves creating a dedicated memory area for cryptographic operations, ensuring the encryption key's protection even against intruders with full administrator access. Their paper presents a case study of a secure web server that validates the effectiveness of this approach in safeguarding the encryption key.

The paper "FoodFresh: Multi-Chain Design for a Food Supply Chain Network" [6] by Stangl and Neumann discusses the challenge of achieving supply chain data visibility in a blockchain-enabled network. Existing methods are limited in handling varying levels of data visibility, as they record transactions on a single blockchain. To overcome this limitation, the authors propose FoodFresh, a multi-chain consortium where organizations store immutable data on their individual blockchains. A decentralized hub facilitates the exchange of digital assets across different blockchains, ensuring interoperability and enabling data sharing while preserving the benefits of independent blockchains.

The final contribution adds a military perspective to the special track. The contribution entitled "Information Dominance: Multi Level Security enabled Shared Information Space" [7] clarifies that information dominance is crucial for both civilian and military activities, particularly in the context of NATO's network-enabled capability concept for multi domain operations. Achieving dynamic leadership and synchronized command intent requires not only technical proficiency but also social, cognitive, and organizational coherence. The provision of services such as awareness, collaboration, coordination, and teaming is vital, and the implementation of a shared information space that enables information sharing is essential. Emphasizing the importance of fine-grained multi level security, Schwarz argues that the traditional "need to know" principle is superseded by a "must share with need to know" mantra.

III. Conclusions

The FAST-CAMS special track includes a broad range of topics related to the security of 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 2023 for their tireless efforts and for accepting FAST-CAMS as a special track. Last, but not least, we are very thankful to the authors for their very interesting contributions.

References

[1] T. J. Bauer and A. Aßmuth. "Encrypted Container File: Design and Implementation of a Hybrid-Encrypted Multi-Recipient File Structure," in Special Track: Finding a Solution to Cloud Application Maturity Security (FAST-CAMS), along with Cloud Computing 2023. IARIA XPS Press, 2023.

[2] S. Görtz, S. Fischer, and R. Hackenberg. "Generation of Distributed Denial of Service Network Data with Python and Scapy," in Special Track: Finding a Solution to Cloud Application Maturity Security (FAST-CAMS), along with Cloud Computing 2023. IARIA XPS Press, 2023.

[3] P. Fuxen, M. Hachani, J. Schmidt, P. Zaumseil, and R. Hackenberg. “Side Channel Monitoring for Fuzz Testing of Future Mobility Systems,” in Special Track: Finding a Solution to Cloud Application Maturity Security (FAST-CAMS), along with Cloud Computing 2023. IARIA XPS Press, 2023.

[4] A. Pakmehr, A. Aßmuth, C. P. Neumann, and G. Pirkl. “Security Challenges for Cloud or Fog Computing-Based AI Applications,” in Special Track: Finding a Solution to Cloud Application Maturity Security (FAST-CAMS), along with Cloud Computing 2023. IARIA XPS Press, 2023.

[5] J. A. Sutherland, N. Coull, and R. I. Ferguson. “On the creation of a secure key enclave via the use of memory isolation in Systems Management Mode,” in Special Track: Finding a Solution to Cloud Application Maturity Security (FAST-CAMS), along with Cloud Computing 2023. IARIA XPS Press, 2023.

[6] P. Stangl and C. P. Neumann. “FoodFresh: Multi-Chain Design for an Inter-Institutional Food Supply Chain Network,” in Special Track: Finding a Solution to Cloud Application Maturity Security (FAST-CAMS), along with Cloud Computing 2023. IARIA XPS Press, 2023.

[7] G. Schwarz. “Information Dominance: Multi Level Security enabled Shared Information Space,” in Special Track: Finding a Solution to Cloud Application Maturity Security (FAST-CAMS), along with Cloud Computing 2023. IARIA XPS Press, 2023.