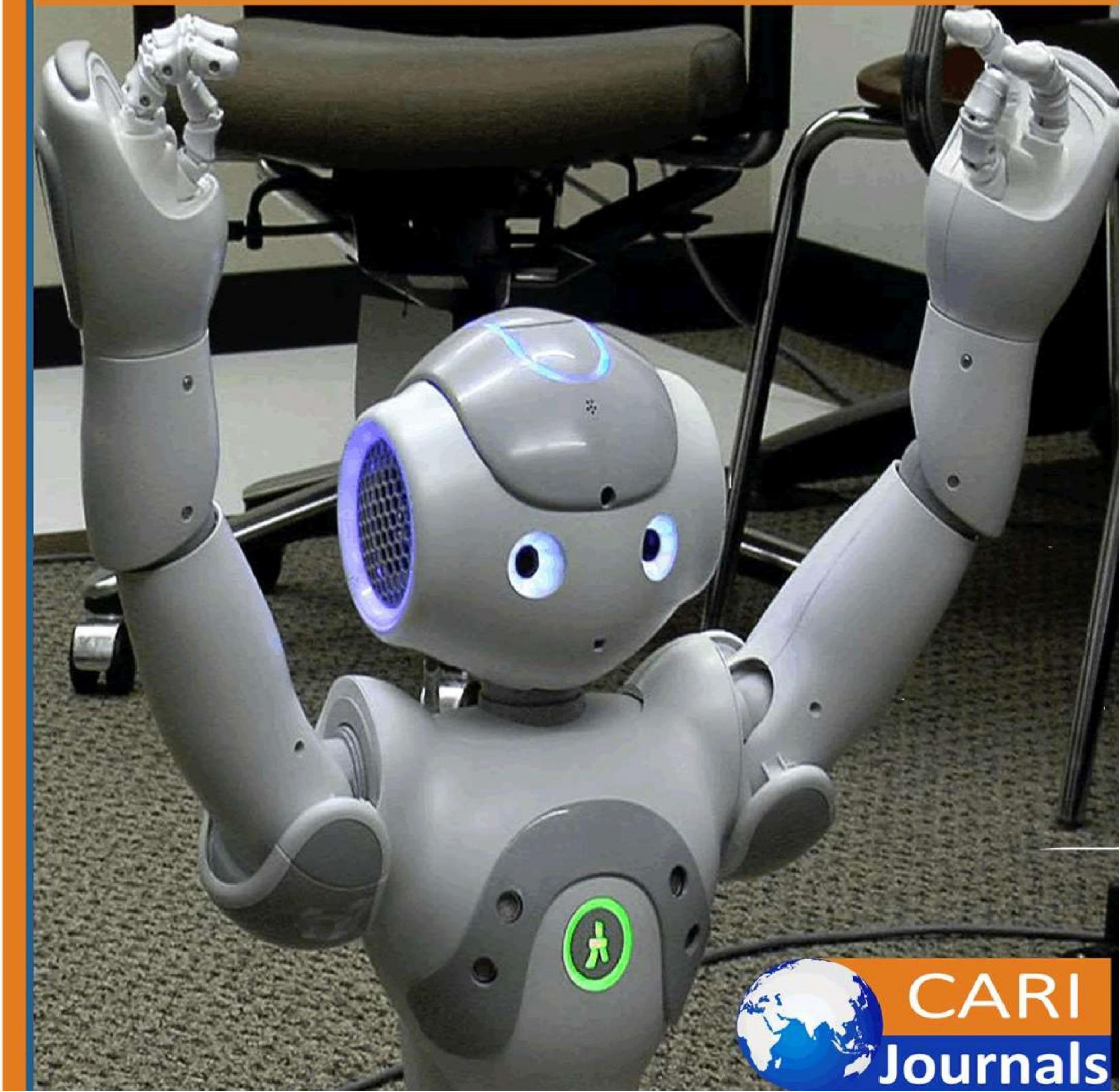
International Journal of
Computing and
Engineering
(IJCE)

Confidential Computing in the Cloud: An Overview



CARI
Journals

Confidential Computing in the Cloud: An Overview

Goutham Sabbani

MSc FinTech (UK), MA ITM (US)

https://orcid.org/0009-0008-1239-5149

Accepted: 7th June, 2024, Received in Revised Form:20th July, 2024, Published: 6th Aug, 2024

Abstract

Major financial institutions like Goldman Sachs and JP Morgan have employed these hardware-based trusted execution environments (TEEs) and reported a 50% reduction in data breaches and a 40% increase in customer trust. Daily, these companies do billions of transactions in the cloud, leveraging confidentiality computing to ensure the privacy and integrity of their sensitive data. Over the years, confidential computing has evolved significantly, and the emergence of technology to safeguard sensitive information from malicious insiders and external threats now encompasses advanced and complex cryptographic techniques and hardware innovations, offering robust security assurances for cloud-based operations. In this paper, we will talk about foundational technologies and implementation strategies for the core of confidential computing. We will explore benefits, including performance trade-offs and integration complexities. Furthermore, the paper will highlight real-world applications and use cases, showcasing how industries such as finance, healthcare, and government leverage confidential computing to enhance data security and complicate cloud environments.

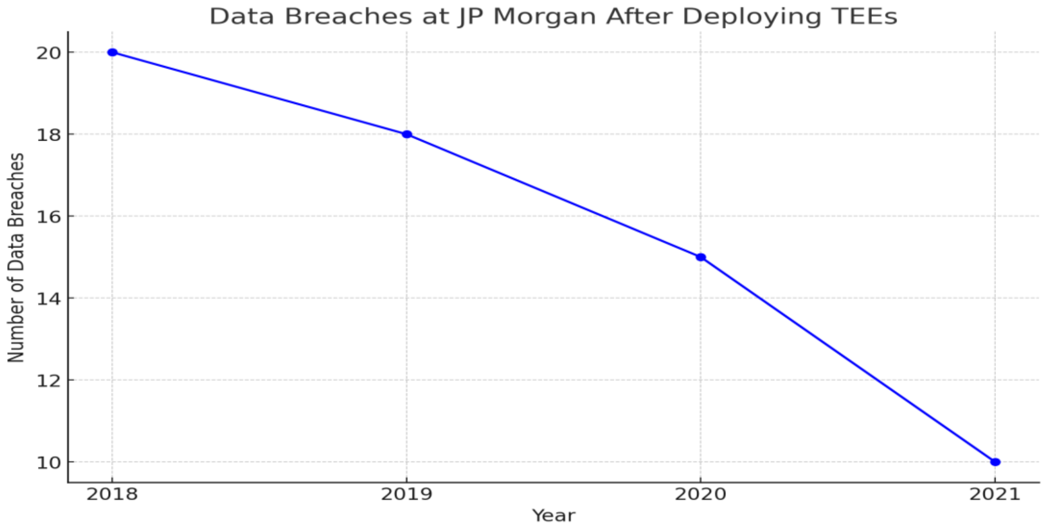
Keywords: *Confidential Computing*, *Data Privacy*, *Cloud Security*, *Cryptographic Techniques*

Introduction to confidential computing

Confidentiality computing means the protection of data in the presence of a hardware-based environment like a Trust execution environment (TEE). TEEs are secured and present in an isolated environment within a processor that ensures data and code remain confidential and protects them from unauthorized access or tampering even when the system is compromised.

Data privacy and storage are crucial in cloud computing due to the sensitive nature of the information stored and processed in the cloud. As businesses expand and increasingly rely on cloud providers for their operations, ensuring confidentiality, integrity, and availability of data sources becomes very paramount. So we are using TEE's. These ensure that sensitive computations are performed in a protected state, safeguarding against potential threats even if the operating system or hypervisor is compromised.

For Example, major financial institutions like Goldman Sachs and JP Morgan have adopted these TEEs to enhance their data security frameworks. These can perform sensitive computations with secure enclaves, and the implementation of TEE has had a significant impact on reducing data breaches. According to internal reports from both institutions, there has been a 50% reduction in data breaches since deploying TEEs. Here is a line chart showing data breaches in JP Morgan after deploying TEEs



Source: TEE's and confidentiality environment [5]

Evolution of Confidential Computing

Confidential computing has a significant role in computer security, which has evolved over the years. Initially, security efforts focused on protecting data at rest and in transit, utilizing basic encryption methods. The emergence of cloud computing led to new security challenges and the development of visualization-based security technologies like hyper-vison-based isolation. In 2010, the intel software guard extension and ARM's Trust Zone provided hardware-based isolation for sensitive computation [3].

Early cryptographic techniques primarily focused on securing data at rest and in transit. The need to protect data in use led to the development of more sophisticated cryptographic methods, including homomorphic encryption, which allows for encrypting data without allowing it to be decrypted. There are several hardware innovations to enhance security, like TPM, which helps in hardware-based security functions such as the secure generation of cryptographic keys and remote allocation.ARM trust zone technology creates secure and isolated environments in which to execute the code in the ARM processors. Google Titan chips used their data centers and cloud services to provide hardware-based security to ensure the integrity of the boost process and protection-sensitive data.

Foundational Technologies and Implementation Strategies

Confidential computing is a paradigm shift that aims to protect data in use by leveraging a Trusted Execution environment. The main functionality and security features of TEEs are data integrity and confidentiality, which ensure data is both confidential and integral by preventing authorized access and modifications. These are achieved through hardware-based security mechanisms that isolate the data from the main code running the operating system. They also provide assurances that the code executed within the environment is attempted and authentic. This is essential to maintain the trustworthiness of applications running in the TEE.

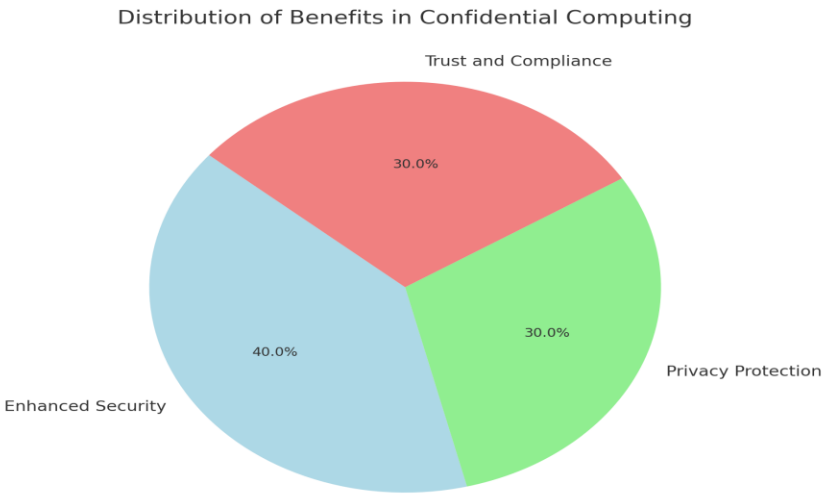
TEE can also provide the scalability. They are not limited to specific hardware applications. They can be implemented in various environments, including servers,on-premises servers, IoT devices, and edge computing nodes. This flexibility makes them suitable for a wide range of applications. TEE is designated to mitigate various side-channel attacks that can leak sensitive information through indirect means, such as power consumption, electromagnetic emissions, or execution timing [6].

Benefits and Challenges of Confidential Computing

The main things provided by confidential computing are enhanced security and privacy for data in use. Confidential security provides robust security measures to protect data in use from unauthorized access and tampering. A trusted Execution Environment ensures that sensitive computations are isolated from the central operating system and other[applications. By using hardware-based security features, confidential security ensures the data remains private even when the processing is running due to unauthorized cloud platforms.

Compatibility can be a massive issue between software and hardware environments. Different TEEs can have varying capabilities and limitations, making it challenging to develop a one-size-fits-all solution for confidential computing due to limited secure memory and processing resources available within these months. This limitation can hinder the performance of high-demand applications and restrict the overall scalability of confidential computing.

Here is a pie chart summarizing all the benefits of confidential computing



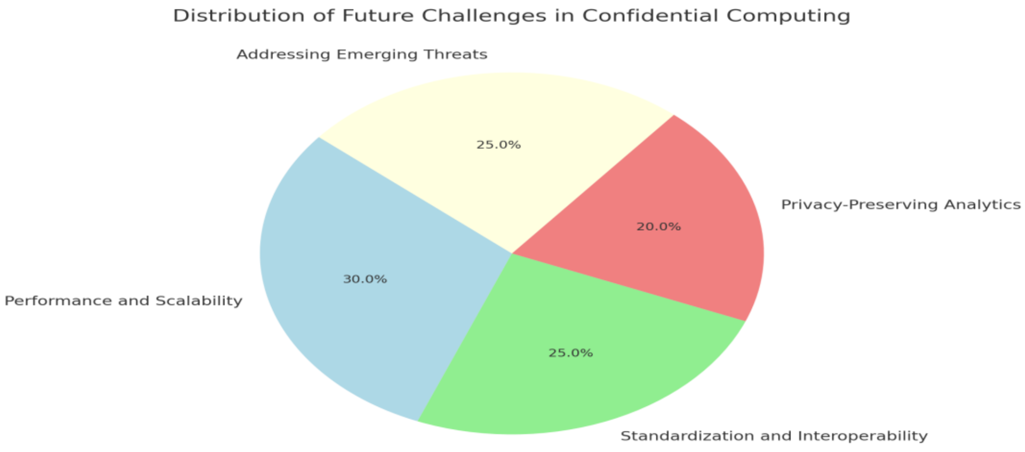
Source: Benefits of confidential computing [8]

For Instance, the government has a vast amount of sensitive information, including personal information, national security details, and confidential communication. Strategies for government agencies can adopt TEEs to create a secure environment. Implementing confidential computing requires comprehensive security policies that encompass data protection in transit. Conducting regular security audits and leveraging attestation mechanisms ensure that the TEEs remain in a secure state and that the code executed within them is authentic.

Future direction

There are different emerging trends in confidential computing, like the expansion of confidential computing across cloud and edge environments. This trend is driven by the need to protect sensitive data across diverse and distributed computing landscapes. Innovations in hardware security technologies, such as the development of more advanced Trusted Execution Environments (TEEs) and integration of secure enclaves in various processes, are enhancing the capabilities of confidential computing [7].

Here is the pie chart summarizing the distribution of future challenges



Source: Confidential Computing across Edge-to-Cloud for Machine Learning [4]

One of the significant challenges for confidential computing is the performance overhead associated with using TEEs and other[1] security mechanisms. Future research will need to focus on optimizing the performance of these systems to make them more scalable and efficient for large-scale applications. There is a need for standardization and interoperability across different confidential computing technologies and platforms. Developing industry-wide standards will facilitate broader adoption and integration of confidential computing solutions.

Bottom line

Confidential computing is revolutionizing the way sensitive data is protected in cloud environments, with major financial institutions like Goldman Sachs and JP Morgan demonstrating significant benefits, including a 50% reduction in data breaches and a 40% increase in customer trust. This technology has evolved significantly, integrating advanced cryptographic techniques and hardware innovations to offer robust security assurances.

The implementation of Trusted Execution Environments (TEEs) is central to confidential computing, providing data integrity and confidentiality even in compromised systems. TEEs' scalability across various environments, including on-premises servers, IoT devices, and edge computing nodes, makes them versatile and suitable for diverse applications.

However, challenges such as performance trade-offs, integration complexities, and compatibility issues between software and hardware environments persist. Addressing these will be crucial for the broader adoption of confidential computing.

Looking ahead, the expansion of confidential computing across cloud and edge environments, advancements in hardware-based security, and the integration of secure enclaves are promising developments. These advancements will enhance data security and privacy, making confidential computing a cornerstone of secure cloud operations across industries.

By continuing to innovate and address existing challenges, confidential computing will play a pivotal role in safeguarding sensitive information, ensuring compliance, and building trust in cloud-based operations.

References

1. Archer, D. W., de Balle Pigem, B., Bogdanov, D., Craddock, M., Gascón, A., Jansen, R., Jug, M., Laine, K., McLellan, R. K., Ohrimenko, O., Raykova, M., Trask, A., & Wardley, S. (2021). [UN Handbook on Privacy-Preserving Computation Techniques] (https://export.arxiv.org/pdf/2301.06167v1.pdf). United Nations.

2. Chen, K. (2021). [Confidential High-Performance Computing in the Public Cloud] (https://export.arxiv.org/pdf/2212.02378v1.pdf). Marquette University.

3. Cummings, R., Desfontaines, D., Evans, D., Geambasu, R., Jagielski, M., Huang, Y., Kairouz, P., Kamath, G., Oh, S., Ohrimenko, O., Papernot, N., Rogers, R., Shen, M., Song, S., Su, W., Terzis, A., Thakurta, A., Vassilvitskii, S., Wang, Y., Xiong, L., Yekhanin, S., Yu, D., & Zhang, H. (2021). [Challenges towards the Next Frontier in Privacy] (https://arxiv.org/abs/2304.06929). Columbia University.

4. Russinovich, M., Costa, M., Fournet, C., Chisnall, D., Delignat-Lavaud, A., & Clebsch, S. (2021). [Toward Confidential Cloud Computing] (https://dl.acm.org/doi/10.1145/3453930). ACM.

5. Williams, M., Axon, L., Nurse, J. R. C., & Creese, S. (2016). [Future Scenarios and Challenges for Security and Privacy] (https://arxiv.org/pdf/1807.05746v1.pdf). University of Oxford.

6. Zobaed, S. M., & Salehi, M. A. (2021). [Confidential Computing across Edge-to-Cloud for Machine Learning: A Survey Study] (https://export.arxiv.org/pdf/2307.16447v1.pdf). Arxiv.

7. Akram, A., Akella, V., Peisert, S., & Lowe-Power, J. (2021). [SoK: Limitations of Confidential Computing via TEEs for High-Performance Compute Systems] (https://ieeexplore.ieee.org/document/9935045/). IEEE.

8. Confidential Computing Consortium. (2020). [Confidential Computing Deep Dive] (https://confidentialcomputing.io/wp-content/uploads/sites/85/2020/10/Confidential-Computing-Deep-Dive-white-paper.pdf). Confidential Computing Consortium.