

Confidential Computing

Table of Contents

01. Introduction

02. Applications in Financial Services

03. Enhancing Data Security & Privacy

04. Addressing Compliance & Regulatory Challenges

05. Challenges & Considerations

06. Confidential Computing for Zero Trust Architectures in Financial Services

07. Conclusion



TORI
Experience. The difference.

01. Introduction

In today's interconnected financial ecosystem, data serves as the lifeblood of innovation, decision-making, and customer engagement. The financial services sector—spanning banking, wealth management, and insurance—relies on the secure handling of sensitive information to maintain trust, comply with stringent regulatory standards, and foster competitive growth. Despite advancements in encryption and secure storage technologies, a critical vulnerability persists: data in use, or data actively processed in memory, often remains exposed to sophisticated cyber threats.

Confidential computing emerges as a transformative technology addressing this gap, providing hardware-based security solutions that protect data during processing. By leveraging Trusted Execution Environments (TEEs), confidential computing ensures data integrity and confidentiality, even in the presence of malicious actors or compromised systems. This paradigm shift not only enhances cybersecurity but also empowers financial institutions to adopt advanced technologies like Artificial Intelligence (AI) and secure multi-party computations without compromising data privacy.

As regulators impose increasingly complex requirements for data protection, and as cyber threats grow in sophistication, confidential computing offers a robust framework for safeguarding sensitive information. This white paper explores the implications of confidential computing for financial services, detailing its applications, challenges, and potential to revolutionise the industry's approach to data security.



Figure 1.1: Illustration of confidential computing. Confidential computing refers to cloud computing technology that can isolate data within a protected central processing unit (CPU) while it is being processed. Within the CPU's environment is the data that the CPU processes and the methods used to process this data. Source: Fortinet (n.d.), 'Confidential computing'

1.1 Understanding Confidential Computing

Confidential computing is an emerging paradigm that focuses on protecting data during its processing phase, addressing a critical vulnerability in traditional security models. While data at rest (stored data) and data in transit (data being transmitted over networks) are commonly encrypted to prevent unauthorised access, data in use (data being actively processed) has historically been more susceptible to breaches. Confidential computing aims to fill this security gap by ensuring that data remains protected even while being processed.

At the core of confidential computing are Trusted Execution Environments (TEEs). TEEs are secure, isolated areas within a processor that safeguard data and code from unauthorised access or modification. They provide a hardware-based root of trust, ensuring that sensitive computations can be performed securely, even in potentially compromised environments. This hardware-based approach offers stronger security guarantees compared to software-only solutions, as it reduces the attack surface and mitigates risks associated with software vulnerabilities.

The Confidential Computing Consortium (CCC), a collaborative industry organisation, defines confidential computing as the protection of data in use by performing computation in a hardware-based, attested TEE. This definition underscores the importance of hardware-based security measures in achieving the objectives of confidential computing.

In the context of financial services, the adoption of confidential computing is particularly pertinent. Financial institutions handle vast amounts of sensitive information, including personally identifiable information (PII), financial transactions, and proprietary algorithms. The protection of this data is not only a matter of maintaining customer trust but also a regulatory requirement. Confidential computing offers a robust solution to these challenges by ensuring that sensitive data remains protected throughout its lifecycle, including during processing.

"The protection of data is not only a matter of maintaining customer trust but also a regulatory requirement. Confidential computing offers a robust solution to these challenges by ensuring that sensitive data remains protected throughout its lifecycle, including during processing."

The implementation of confidential computing in financial services can lead to several benefits:

- **Enhanced Data Security:** By protecting data during processing, confidential computing reduces the risk of data breaches and unauthorised access.
- **Regulatory Compliance:** Confidential computing can assist financial institutions in meeting stringent data protection regulations by providing verifiable security measures.
- **Trust and Transparency:** By ensuring the integrity and confidentiality of data, financial institutions can build greater trust with customers and stakeholders.

However, the adoption of confidential computing also presents challenges. Integrating TEEs into existing IT infrastructures may require significant changes and expertise. Additionally, the performance overhead introduced by TEEs can affect transaction speeds, which are critical in financial operations. Despite these challenges, the potential benefits of confidential computing make it a compelling consideration for financial institutions aiming to enhance their data security and compliance posture.

2. Applications in Financial Services

The financial services sector is characterised by its reliance on data-driven decision-making and the necessity to handle sensitive information securely. Confidential computing offers a transformative approach to data security, enabling financial institutions to perform sensitive computations in a secure environment, thereby mitigating risks associated with data breaches and unauthorised access.

2.1 Secure Multi-Party Computation

One of the most compelling applications of confidential computing in financial services is secure multi-party computation (MPC). MPC allows multiple parties to collaboratively compute a function over their inputs while keeping those inputs private. In the context of financial institutions, this capability is invaluable for collaborative efforts such as fraud detection and anti-money laundering initiatives.

For instance, multiple banks can use confidential computing to analyse combined transaction datasets to identify fraudulent patterns without exposing individual customer information. This collaborative approach enhances the detection of complex fraud schemes that may span across different institutions, thereby strengthening the overall security of the financial ecosystem.

2.2 Confidential AI and Machine Learning

Artificial Intelligence (AI) and Machine Learning (ML) are increasingly integral to financial services, powering applications from credit scoring to investment strategies. However, training AI models often requires access to sensitive data, raising concerns about data privacy and security.

Confidential computing enables financial institutions to train and deploy AI models within TEEs, ensuring that sensitive data remains protected during processing. This approach allows institutions to leverage the power of AI while maintaining compliance with data protection regulations and preserving customer trust.

2.3 Secure Data Sharing and Collaboration

Financial institutions often need to share data with partners, regulators, or other third parties. Traditional data-sharing methods can expose sensitive information to potential breaches. Confidential computing facilitates secure data sharing by allowing computations to be performed on encrypted data within TEEs. This ensures that sensitive information is not exposed during the sharing process, enabling secure collaboration between parties.



Figure 2.1: Illustration of data security practices, highlighting protection for data at rest, in transit, and in use, with confidential computing ensuring secure processing environments. Source: NVIDIA, 'What Is Confidential Computing?' Retrieved November 18, 2024, from Nvidia.com.

2.4 Protecting Proprietary Algorithms

Financial institutions develop proprietary algorithms for trading, risk assessment, and other critical functions. Protecting these algorithms from theft or tampering is essential to maintain competitive advantage. Confidential computing ensures that these algorithms can be executed within a secure environment, protecting them from unauthorised access or modification.

2.5 Enhancing Cloud Security

The adoption of cloud services in financial services offers scalability and flexibility but also introduces security concerns, particularly regarding data in use. Confidential computing addresses these concerns by providing hardware-based security measures that protect data during processing in cloud environments. This enables financial institutions to leverage cloud technologies while maintaining robust security postures.

3. Enhancing Data Security and Privacy

Data security and privacy are foundational to the trust that customers place in financial institutions. Confidential computing enhances these aspects by providing robust protections for data during processing, which has traditionally been the most vulnerable phase. With the integration of confidential computing, financial institutions can ensure the integrity and confidentiality of their data, not just in storage or transit but in real-time processing.

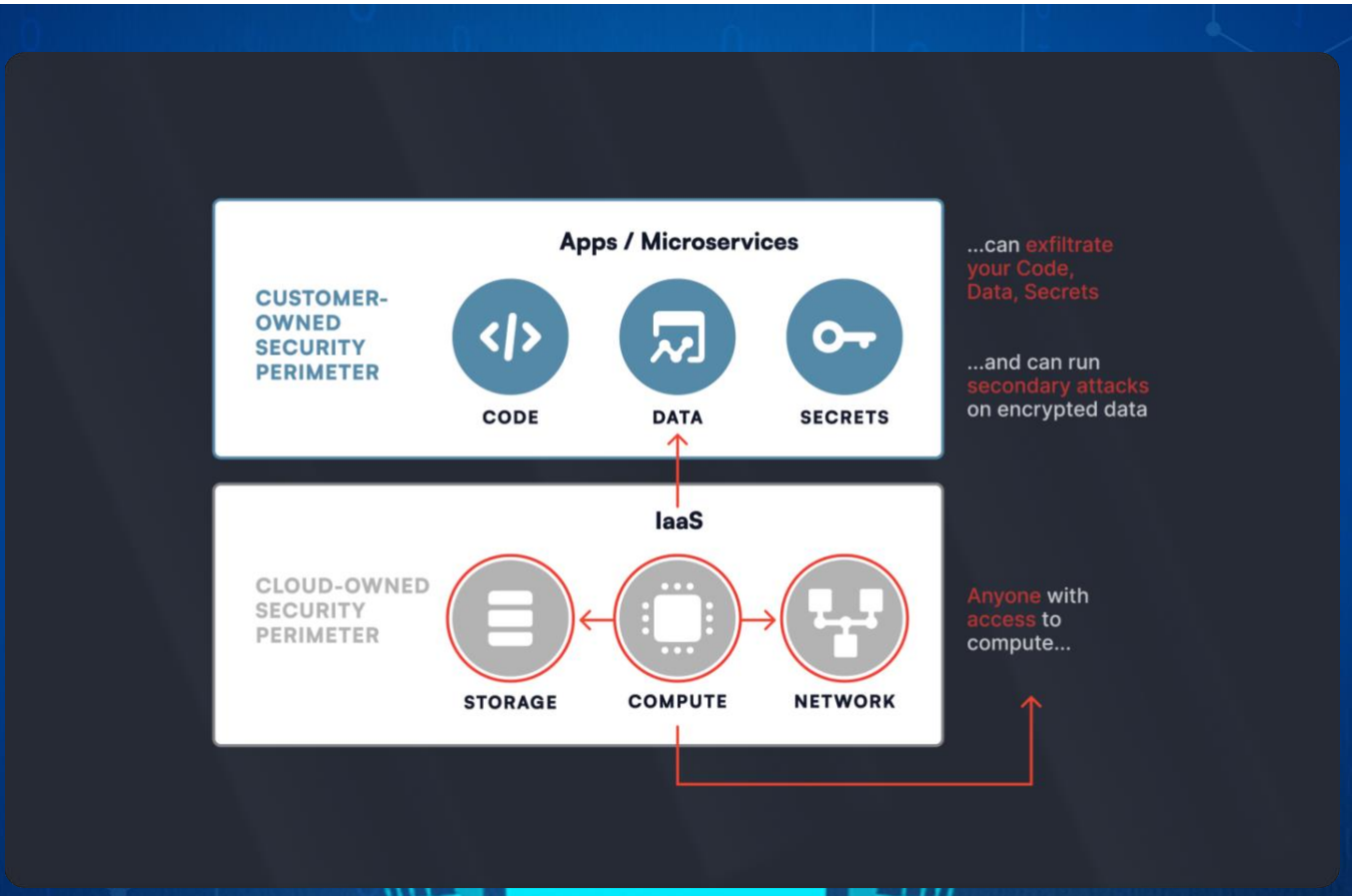


Figure 2.2: Illustration of security perimeters in confidential computing, emphasising the separation between customer-owned and cloud-owned environments, and highlighting potential risks such as data exfiltration, secondary attacks, and vulnerabilities in compute access. Source: Anjuna, 'What is Confidential Computing,' retrieved November 18, 2024, from Anjuna.io

3.1 Strengthening Data Confidentiality

Confidential computing ensures that sensitive information remains confidential even when actively processed. By leveraging TEEs, confidential computing keeps data encrypted and secure within a dedicated hardware environment, accessible only to authorised applications and users. This is especially relevant for financial institutions that handle highly sensitive customer information, such as credit card numbers, social security details, and private transaction records. With confidential computing, this information can remain protected at all times, reducing exposure to cyber threats and mitigating risks from potential insider attacks.

3.2 Ensuring Data Integrity

Data integrity is critical in financial services, as data manipulation can have far-reaching consequences, from financial fraud to reputation damage. By performing computations within a secure TEE, confidential computing minimises the risk of unauthorised alterations to data in use. This level of integrity can support financial applications such as automated trading platforms and loan approval systems by maintaining accurate and trustworthy data inputs and outputs. It also prevents tampering with algorithms, which are often proprietary and give financial firms a competitive advantage.

3.3 Guaranteeing Code Integrity

Financial institutions rely on complex algorithms and software to make decisions that impact their customers and business operations. By running this code within a TEE, confidential computing ensures that code remains secure and unaltered by external forces. This guarantees that proprietary algorithms are protected from unauthorised access or manipulation, which is particularly important in high-stakes financial applications where any change in the algorithm can result in significant financial implications.

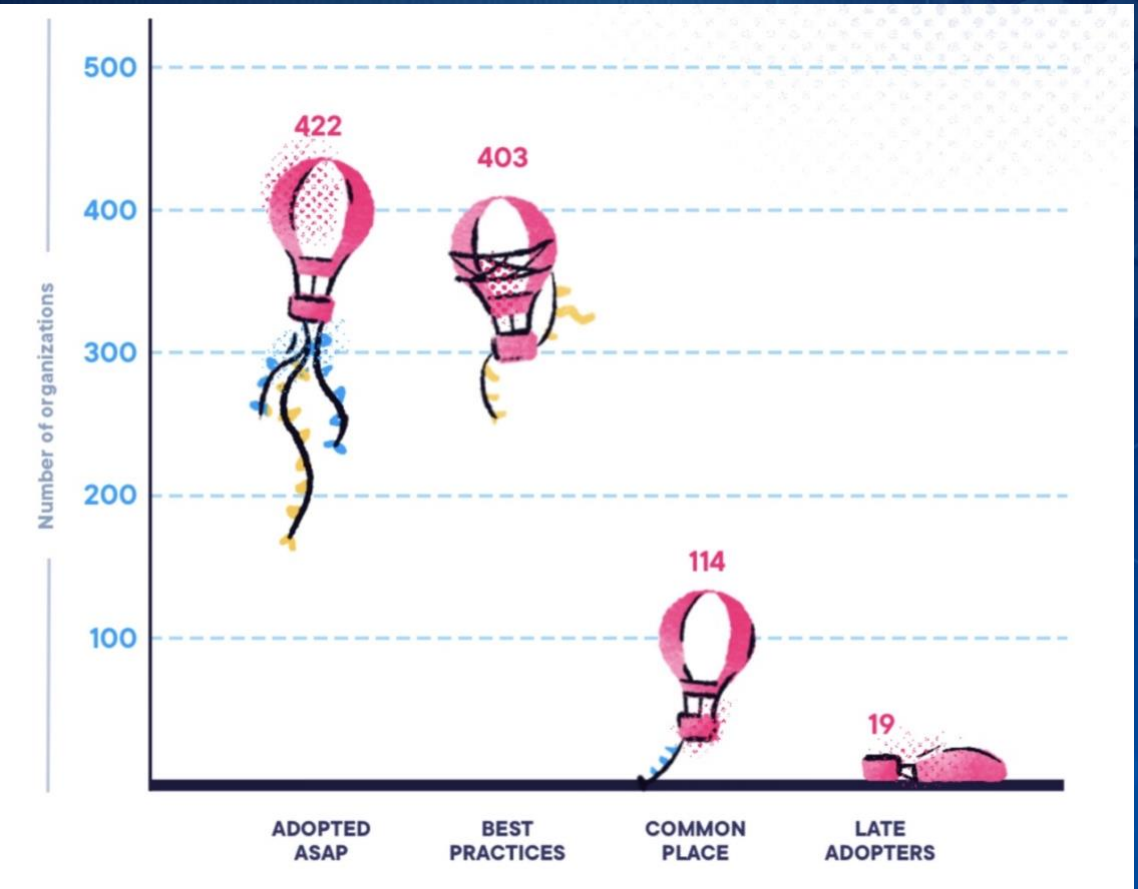


Figure 3.1: Adoption of cloud technologies by organisations, as highlighted in the State of Cloud 2023 report by Plural Insight. The chart emphasises how the rapid adoption of cloud services drives the need for advanced security measures like confidential computing, ensuring data remains protected during processing in increasingly cloud-dependent infrastructures. Published June 2023.

4. Addressing Compliance and Regulatory Challenges

The financial sector is governed by stringent regulatory requirements designed to protect customer data, prevent fraud, and ensure overall stability in the system. Confidential computing aligns well with these regulatory goals, providing financial institutions with tools to demonstrate compliance while maintaining high data security standards.

4.1 Adherence to Privacy Regulations

Confidential computing aids financial institutions in adhering to data privacy laws such as GDPR, CCPA, and PSD2 by protecting data during processing. This ensures that customer data remains secure at all times, providing peace of mind to both institutions and their clients. For instance, confidential computing can enable institutions to perform analytics on customer data without exposing raw data, thereby achieving compliance with data minimisation principles outlined in many privacy laws.

4.2 Data Residency and Sovereignty Compliance

Global financial institutions often operate across multiple jurisdictions, each with its own set of data residency and sovereignty requirements. Confidential computing allows financial institutions to meet these requirements by keeping data encrypted and processed securely within designated geographic boundaries. This can be crucial for institutions operating in areas with strict regulations on cross-border data transfers.

4.3 Enhanced Audit and Attestation Capabilities

Regulators require financial institutions to provide verifiable evidence of data security measures, which can be challenging with traditional data protection methods. Confidential computing offers enhanced auditability and attestation capabilities, enabling financial institutions to demonstrate compliance through verified proof that data and code remain protected during processing. This can help institutions proactively meet regulatory requirements and respond swiftly to audit requests, reducing the risk of penalties and enhancing transparency with regulatory bodies.

5. Challenges and Considerations

While confidential computing offers significant advantages, its adoption within the financial sector comes with certain challenges that institutions must address to fully realise its benefits.

5.1 Integration Complexity

Adopting confidential computing involves integrating TEEs into existing IT infrastructures, which can be complex and resource-intensive. Financial institutions may need to redesign certain processes or update legacy systems to accommodate the requirements of TEEs. Additionally, institutions may face challenges related to interoperability between different TEEs, especially when using a mix of hardware from various vendors. Careful planning and expertise are necessary to ensure a smooth integration process.

5.2 Performance Overheads

Running computations within TEEs can introduce performance overheads due to the additional security layers. While these overheads are often minimal, they may affect the performance of high-frequency financial transactions or latency-sensitive applications. Financial institutions must assess the performance impact and consider ways to optimise systems to minimise latency, especially in areas where real-time processing is critical.

Confidential computing empowers financial institutions to meet stringent regulatory requirements while ensuring robust data security and transparency. Despite integration challenges, its benefits in compliance, trust-building, and safeguarding sensitive data make it an indispensable tool for modern financial operations.

5.3 Vendor Dependence and Ecosystem Maturity

Confidential computing relies on specific hardware and software ecosystems that are still maturing. Financial institutions may find themselves dependent on certain vendors for TEEs, which can create vendor lock-in and limit flexibility. Additionally, the relatively nascent ecosystem for confidential computing means that tools, support, and standardisation are still evolving. Financial institutions should carefully evaluate the maturity of vendors and the ecosystem to ensure long-term viability and support.

5.4 Cost Implications

Implementing confidential computing involves upfront costs for new hardware and possibly ongoing expenses for maintenance and vendor support. Financial institutions should assess these costs against the expected benefits, particularly in high-risk areas where data protection is critical. For many institutions, the improved security and regulatory compliance offered by confidential computing can justify these expenses, but a thorough cost-benefit analysis is essential.

5.5 High-Level Encryption on Hardware: Mechanisms and Insights into RAM Encryption

High-level encryption implemented directly on hardware provides robust security for data during processing, a phase traditionally vulnerable to attacks. Confidential computing achieves this by integrating encryption mechanisms into the physical architecture of devices, particularly within Trusted Execution Environments (TEEs). A prime example is RAM encryption, where data in volatile memory is encrypted in real time to mitigate risks such as physical memory attacks, cold boot exploits, and memory scraping.

The encryption of RAM operates through dedicated hardware units embedded within the CPU. These units encrypt data as it is written to memory and decrypt it only when accessed by authorised processes. The encryption keys are securely generated and stored within the processor, often protected by secure enclaves or cryptographic key management hardware, ensuring that keys are inaccessible even to privileged system processes. RAM encryption not only preserves the confidentiality of data but also verifies its integrity. This dual functionality guards against unauthorised modifications, ensuring that computations and data flows remain reliable and untampered.

The diagram below highlights how confidential computing protects data in use, complementing existing encryption technologies for data at rest and in transit. Mechanisms like Memory Encryption Engines (MEEs) enable this protection by encrypting data as it is processed in memory, ensuring security even against physical or side-channel attacks. Operating within the CPU, MEEs decrypt data only in isolated caches, preventing exposure in untrusted areas. This process, while not visually detailed in the diagram, underscores the critical role of hardware-managed encryption in securing sensitive computations, making RAM encryption a cornerstone of end-to-end data protection.

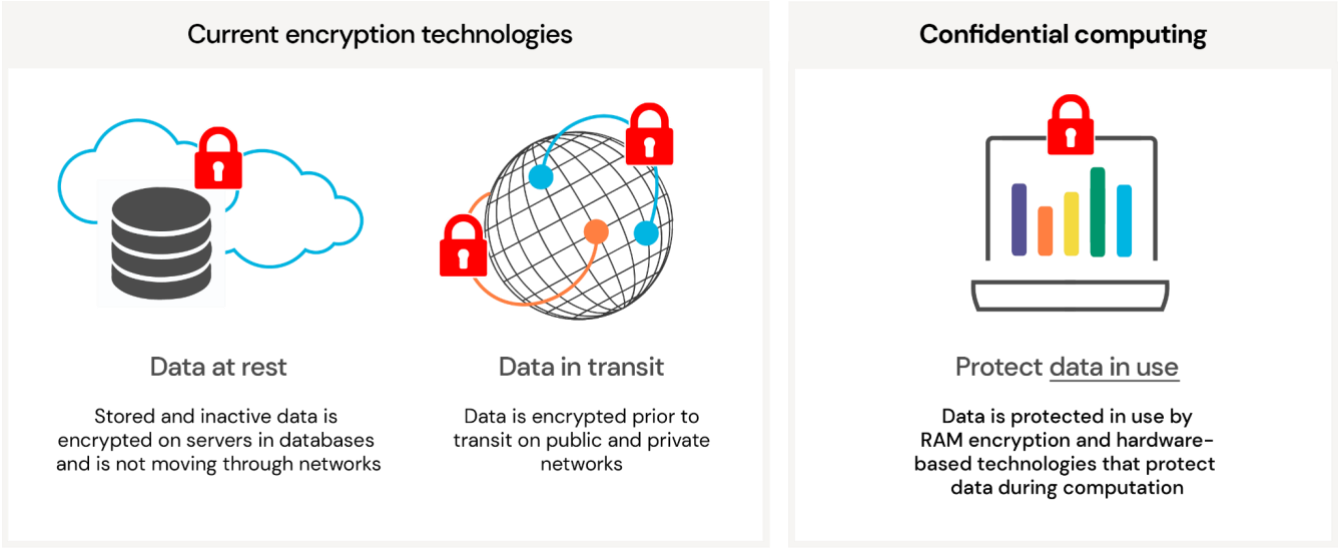


Figure 5.1: Comparison of current encryption technologies, which protect data at rest and in transit, with confidential computing, which extends protection to data in use. Confidential computing provides an essential layer of security for cloud-based data processing. Source: Ledidi, 'Confidential Computing: The Missing Link in Cloud Data Protection,' retrieved November 18, 2024, from Ledidi.

6. Confidential Computing for Zero Trust Architectures in Financial Services

As financial institutions face increasingly sophisticated cyber threats, Zero Trust Architecture (ZTA) has emerged as a security model that assumes no implicit trust within a network. Every access request is verified, authenticated, and authorised before granting access to any resources. Confidential computing enhances the effectiveness of Zero Trust by securing sensitive computations in hardware-isolated environments, ensuring that no unauthorised entities, even those within the network, can access data in use.

6.1 Zero Trust Overview and Its Relevance in Financial Services

The Zero Trust model has gained traction across sectors, especially in financial services, due to its proactive approach to security. In traditional network security models, once users gain access to the network, they have implicit trust within it. However, the rise of advanced persistent threats (APTs), phishing attacks, and insider threats has demonstrated that this trust model is outdated. The Zero Trust model requires continuous verification at every layer, from network access to application and data access, which aligns with the compliance and security requirements of financial institutions.

6.2 Role of Confidential Computing in Enforcing Zero Trust

Confidential computing directly supports the Zero Trust model by securing data and applications during processing, protecting them from unauthorised access, even from privileged users. Here's how:

- **Micro-Segmentation of Workloads:** Confidential computing enables the isolation of sensitive workloads within TEEs, which aligns with the Zero Trust principle of micro-segmentation. Each TEE acts as an isolated environment, reducing the risk of lateral movement by attackers. Only authorised applications and users with the appropriate access credentials can execute computations within these TEEs, adding an additional security layer against unauthorised access.

- **Continuous Verification with Attestation:** Confidential computing includes an attestation process that verifies the integrity of the TEE before executing sensitive workloads. This feature ensures that only trusted and verified environments handle sensitive computations. When incorporated into a Zero Trust framework, attestation provides an additional verification step that aligns with the model's "never trust, always verify" principle. TEEs periodically re-attest to confirm their integrity, preventing unauthorised modifications or tampering.

- **Protecting Identity and Access Management (IAM) Data:** Financial institutions use IAM systems extensively in Zero Trust architectures to enforce stringent access controls. IAM data, such as user credentials, access logs, and session tokens, is highly sensitive and a prime target for cyberattacks. Confidential computing can protect IAM data during processing, ensuring that access decisions are based on accurate, untampered data. By running IAM processes within a TEE, institutions prevent unauthorised manipulation of access policies, enhancing the security of identity management in a Zero Trust environment.

6.3 Enabling Secure Remote Access and Multi-Cloud Zero Trust

In financial services, many applications and services are moving to multi-cloud environments, which adds complexity to Zero Trust implementations. Confidential computing ensures secure processing of data across cloud providers without relying on the inherent trust of each provider. TEEs protect workloads regardless of the cloud provider, which enables secure collaboration and data sharing between different cloud environments.

Additionally, as remote work has become prevalent, secure remote access to financial data and systems is essential. Confidential computing allows remote employees to access sensitive resources within TEEs, maintaining a secure processing environment even outside the traditional corporate perimeter. This minimises the risks associated with remote access and enhances the robustness of Zero Trust policies.

6.4 Integration with Threat Detection and Response

Confidential computing can also complement threat detection and response strategies within a Zero Trust framework. By securing sensitive logs and telemetry data during analysis, TEEs ensure that threat detection algorithms work with accurate data, free from tampering. This integrity is essential in financial services, where timely and accurate threat detection is critical. For example, a TEE could securely process real-time data from transaction monitoring systems, ensuring that threat detection models have access to unaltered data for accurate analysis.

6.5 Limitations and Future Directions for Confidential Computing in Zero Trust Architectures

While confidential computing strengthens Zero Trust architectures, some limitations persist:

- **Latency in Real-Time Applications:** The extra layers of verification and encryption may introduce latency in high-frequency transactions, impacting real-time financial applications.
- **Interoperability Challenges:** Integrating TEEs from different providers can be complex, especially in multi-cloud Zero Trust implementations where consistent policies and controls must span diverse environments.

Despite these challenges, confidential computing is likely to become integral to Zero Trust frameworks as TEEs and Zero Trust technologies continue to mature. As financial services face growing cyber threats, combining Zero Trust with confidential computing presents a robust solution for securing highly sensitive data and critical computations.

7. Conclusion: Confidential Computing as a Pillar of Financial Security

Confidential computing represents a significant advancement in securing sensitive data during processing, addressing a critical vulnerability in traditional data security models for financial services. With the integration of hardware-based Trusted Execution Environments (TEEs), confidential computing provides unprecedented protection for data in use, allowing financial institutions to operate securely in increasingly complex digital landscapes. This approach has the potential to transform the way banks, wealth management firms, and insurance companies handle sensitive information, ensuring that data remains secure across all stages of its lifecycle.

In a sector where trust is paramount, confidential computing enhances data confidentiality, integrity, and availability, making it indispensable for protecting sensitive financial and customer information. Its applications, from secure multi-party computations and confidential AI processing to enhanced cloud security, demonstrate its versatility and critical role in meeting regulatory requirements and building customer trust. Additionally, by supporting frameworks like Zero Trust Architecture, confidential computing empowers financial institutions to implement proactive, multi-layered security strategies that align with modern cybersecurity demands.

The path to widespread adoption of confidential computing is not without challenges. Institutions must navigate complexities in integration, manage performance impacts on latency-sensitive applications, and address issues like vendor dependency. However, as the technology matures and industry standards evolve, these challenges are likely to become more manageable, making confidential computing increasingly accessible to financial institutions of all sizes.

Looking forward, confidential computing is poised to become a core component of the financial sector's cybersecurity strategy. With continued investment and collaboration among technology providers, financial institutions, and regulatory bodies, confidential computing will evolve to offer even greater levels of security, interoperability, and usability. By embracing this technology, financial services can ensure that their operations remain secure, compliant, and resilient against emerging threats, fostering a safer, more trustworthy financial ecosystem for the future.



References

1. Confidential Computing Consortium. "Confidential Computing: Hardware-Based Trusted Execution for Applications and Data."

2. Accenture. "Securing Business Transformation with Confidential Computing."

3. Google Cloud. "Expanding Confidential Computing for AI Workloads."

4. Future of Privacy Forum. "Confidential Computing and Privacy: Policy Implications of Trusted Execution Environments."

5. IBM. "Confidential Computing for Total Privacy Assurance in Cloud Environments."

6. Microsoft Azure. "Azure Confidential Computing – Protect Data In Use."

7. Red Hat. "Confidential Containers for Financial Services on Public Cloud."

8. Dark Reading. "How Confidential Computing Can Change Cybersecurity."

9. Microsoft. "Microsoft's Confidential Computing Improves Security for Banks."

10. Ubuntu. "Confidential Computing and Financial Services Cloud."

11. Microsoft Azure. "Common Azure Confidential Computing Scenarios and Use Cases."

12. Microsoft Azure. "Enabling Data Clean Rooms with Confidential Computing."

13. IBM. "Confidential Computing: What's the Big Deal?"

14. Microsoft Azure. "Azure and AMD Announce Landmark in Confidential Computing Evolution."

15. Microsoft Azure. "Announcing: Microsoft Moves $25 Billion in Credit Card Transactions to Azure Confidential Computing."

16. Investors.com. "Nvidia Led The First AI Stocks Wave. These Data Players Are Targeting The Next One."

17. Financial Times. "Banks Moving into the Cloud Prompt Forecasts of Security Risk."

18. Wall Street Journal. "China's AI Engineers Are Secretly Accessing Banned Nvidia Chips."

19. Deloitte. "NIST's Postquantum Cryptography Standards: 'This Is the Start of the Race'."

20. Deloitte. "Beyond Numbers: Critical Role of Cybersecurity in M&A Deals."


TORİ
Experience. The difference.