European Journal of Computer Science and Information Technology,13(24),115-128, 2025
Print ISSN: 2054-0957 (Print)
Online ISSN: 2054-0965 (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Confidential Computing for Privacy-Preserving Fraud Analytics

Ramchander Malkoochi
HCL Tech, USA

doi: https://doi.org/10.37745/ejcsit.2013/vol13n24115128 Published May 20, 2025

Citation: Malkoochi, R. (2025) Confidential Computing for Privacy-Preserving Fraud Analytics, *European Journal of Computer Science and Information Technology*,13(24),115-128

Abstract: *Confidential computing represents a transformative paradigm in fraud analytics, providing robust protection for sensitive financial data throughout the processing lifecycle. By leveraging Trusted Execution Environments (TEEs) such as Intel SGX and AMD SEV, financial institutions can analyze transaction patterns, detect anomalies, and collaborate across organizational boundaries while maintaining data confidentiality. The technology addresses the fundamental tension between effective fraud detection and privacy protection through hardware-based isolation mechanisms that secure data even during computation. This comprehensive overview explores how confidential computing enhances fraud analytics through privacy-preserving machine learning, secure multi-party computation, and cryptographic integrity guarantees. The implementation pathways through cloud platforms enable financial organizations to deploy these solutions within existing infrastructure while acknowledging the challenges related to performance, scalability, and hardware constraints as these technologies mature alongside complementary approaches like homomorphic encryption and blockchain integration, confidential computing positions itself as the cornerstone of privacy-preserving fraud analytics in an increasingly data-sensitive financial ecosystem.*

Keywords: trusted execution environments, privacy-preserving analytics, secure multi-party computation, financial fraud detection, data confidentiality

INTRODUCTION

Confidential computing represents a revolutionary approach to data security, focusing on protecting data during processing rather than merely during storage or transmission. This protection is achieved through hardware-based Trusted Execution Environments (TEEs), such as Intel SGX (Software Guard Extensions) and AMD SEV (Secure Encrypted Virtualization). These TEEs create secure enclaves where sensitive data can be processed without exposure to unauthorized access—even from the operating system, hypervisor, or cloud service providers themselves. A recent study reveals that 60% of organizations rank data security

as their primary concern when moving workloads to the cloud, with 45% specifically worried about protecting data-in-use, highlighting the crucial gap that confidential computing addresses [1].

The conceptual foundation of confidential computing centers on maintaining cryptographic protection throughout the data lifecycle, including during computation. As the research indicates, traditional security models that focus solely on encrypting data at rest and in transit leave a significant vulnerability during processing stages—a gap that has become increasingly critical as cloud adoption accelerates. The study further notes that 95% of enterprises already utilize multiple clouds, making the need for consistent security across diverse environments paramount [1].

In the domain of fraud analytics, where processing sensitive financial data, personal information, and transaction histories is essential, confidential computing offers a robust solution for protecting this data during analysis. Recent research in expert systems demonstrates that fraudsters continuously adapt their techniques, with modern fraud detection systems processing up to 16.4 trillion data points annually across financial networks [2]. By implementing privacy-preserving techniques within secure enclaves, financial institutions can analyze this vast volume of sensitive data while maintaining confidentiality. This approach has shown a 28.7% improvement in model accuracy for fraud detection while simultaneously reducing false positives by 19.3% compared to traditional methods [2].

This technology enables truly privacy-preserving fraud detection while maintaining compliance with stringent privacy regulations like GDPR and CCPA. The advancement comes at a critical time, as regulatory penalties for data protection violations reached $1.3 billion globally in 2022 according to the analysis [1]. The integration of confidential computing with enhanced fraud detection algorithms represents a convergence of security and analytical capabilities that promises to reshape how financial institutions approach the perpetual challenge of balancing effective fraud prevention with robust privacy protection.

The Challenge of Privacy in Fraud Analytics

Effective fraud detection in financial systems necessitates access to substantial amounts of sensitive data across multiple dimensions. Modern financial fraud detection requires processing transaction histories that reveal spending patterns, merchant relationships, and temporal behaviors; personal identifying information (PII) containing names, addresses, and government-issued identification details; comprehensive financial account data including balance histories and credit arrangements; and increasingly critical device and location metadata that creates digital fingerprints of user behavior. Recent research on financial transaction fraud indicates that detection systems must analyze between 50-200 variables per transaction to achieve acceptable accuracy rates, with transaction volumes reaching millions daily in large financial institutions [3]. This vast data requirement creates an inherent tension between detection effectiveness and privacy protection.

While analyzing these comprehensive datasets is crucial for detecting fraudulent activities and unusual transaction patterns, exposing this sensitive data creates significant privacy and security concerns.

According to Krishna Dama et al., findings, traditional machine learning approaches for fraud detection, while achieving detection rates of 92.7% with Random Forest algorithms and 94.2% with XGBoost models, typically require data to be processed in plaintext during the analysis phase [3]. This exposure creates substantial vulnerabilities throughout the analytical pipeline. Traditional fraud detection systems predominantly process data unencrypted to enable real-time analysis, potentially leading to data breaches with unauthorized access to sensitive information.

The implications extend beyond immediate security concerns to regulatory compliance issues. Research from the Bank for International Settlements demonstrates that privacy-preserving techniques are increasingly necessary as financial data protection regulations have expanded globally, with 51 countries now implementing comprehensive financial data protection frameworks compared to just 17 in 2000 [4]. These regulations place significant constraints on how financial institutions can process personal data, with penalties for non-compliance reaching up to 4% of global annual revenue. The BIS study further notes that financial institutions must balance "sometimes conflicting policy objectives related to data access, data privacy, and legal certainty," creating complex operational challenges for fraud analytics teams [4].

Trust erosion represents another critical concern, as customers become increasingly reluctant to share personal data. BIS research confirms that customer awareness regarding data privacy has increased significantly, with 82% of banking customers in advanced economies expressing concerns about financial data processing [4]. This heightened awareness directly impacts customer behavior, with observable reductions in digital service adoption among privacy-sensitive demographic segments.

Confidential computing addresses these multifaceted challenges by allowing financial institutions, payment processors, and fraud detection service providers to securely analyze sensitive data without exposure. By implementing memory encryption and hardware-based isolation techniques, organizations can maintain data confidentiality throughout processing while still applying sophisticated detection algorithms. As Krishna Dama et al., observe, "privacy-preserving fraud detection represents the frontier of financial security research," with emerging approaches demonstrating the viability of maintaining both privacy and detection efficacy [3]. This technological approach fundamentally alters the traditional trade-off between security effectiveness and privacy protection, enabling financial institutions to satisfy both the regulatory requirements detailed in the BIS research and the growing customer expectations for data protection.

European Journal of Computer Science and Information Technology,13(24),115-128, 2025
Print ISSN: 2054-0957 (Print)
Online ISSN: 2054-0965 (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Table 1: Privacy Challenges and Fraud Detection Metrics in Financial Systems [3, 4]

Metric	Value	Context
Variables required for fraud detection per transaction	50-200	Modern detection systems
Random Forest algorithm detection rate	92.7%	Traditional ML approaches
XGBoost model detection rate	94.2%	Traditional ML approaches
Countries with comprehensive financial data protection (2000)	17	Regulatory landscape
Countries with comprehensive financial data protection (Present)	51	Regulatory landscape evolution
Maximum non-compliance penalty (% of global annual revenue)	4%	Regulatory consequences
Banking customers concerned about financial data processing	82%	Customer trust metrics
Required variables per transaction (minimum)	50	Detection effectiveness threshold
Required variables per transaction (maximum)	200	Detection effectiveness threshold
Daily transaction volume in large financial institutions	Millions	Scale of data processing

How Confidential Computing Enhances Fraud Analytics

Data Protection During Analysis

Confidential computing ensures data remains encrypted and secure even during processing. TEEs isolate and protect the data from both cloud providers and any unauthorized entities, including system

administrators. Recent comprehensive analysis of Trusted Execution Environments reveals that Intel SGX enclaves can maintain cryptographic isolation while processing financial data with only a 7-15% performance overhead compared to non-secure environments [5]. By utilizing secure enclaves, fraud detection algorithms can analyze transaction data without exposing it, even to the systems performing the computations themselves. This protected environment maintains confidentiality while still enabling complex analytical operations, providing a security foundation that traditional systems cannot match.

Privacy-Preserving Machine Learning

Machine learning models for fraud detection typically require access to large datasets for training and prediction. In traditional systems, this would involve processing sensitive data in unprotected environments—a significant risk. With confidential computing, these models can be trained and executed within secure enclaves, ensuring that data used for model development and prediction remains confidential throughout. Research demonstrates that TEE implementations can support neural networks with up to 90 million parameters while maintaining hardware-level security guarantees [5].

Federated learning represents a particularly valuable application in this context, where multiple institutions can collaborate to train shared fraud detection models without revealing their individual datasets. This approach preserves data confidentiality while still benefiting from collective intelligence across organizations. Similarly, differential privacy techniques can be implemented within TEEs, ensuring that machine learning algorithms applied to financial data do not reveal sensitive information about individual transactions or users. The combination of these privacy-enhancing technologies within the confidential computing framework creates multiple layers of protection for sensitive financial information.

Secure Multi-Party Computation (SMPC)

SMPC enables multiple parties such as financial institutions, payment processors, or law enforcement agencies to collaboratively analyze data without revealing their individual datasets. According to research, financial institutions implementing such collaborative frameworks have successfully detected 89% of sophisticated fraud attempts compared to 72% using isolated systems [6]. Confidential computing enhances SMPC by enabling secure computations in trusted execution environments, where each party can contribute to analysis without disclosing private data. This capability is particularly valuable for cross-border fraud detection, where different jurisdictions enforce varying data privacy requirements. The technology allows for compliance with multiple regulatory frameworks simultaneously while maintaining operational effectiveness.

Data Integrity and Auditability

Confidential computing provides cryptographic proofs of computation, ensuring data integrity throughout analytical processes. When analyzing transaction patterns for fraud, the system generates cryptographic evidence proving that data was processed correctly and securely, without alteration or exposure of sensitive information. According to industry research, AI-powered fraud detection systems now process over 6,000 transactions per second in banking environments, making integrity guarantees essential at scale [6]. This audit capability helps meet compliance requirements and provides verifiable trails for regulatory purposes.

As banking fraud costs have reached approximately $30 billion globally, these integrity measures become increasingly critical for both operational and regulatory requirements [6]. The attestation capabilities of modern TEEs ensure that all parties can verify that computations were performed correctly without compromising the underlying data, providing trust in environments where it would otherwise be impossible.

Benefits of Confidential Computing in Fraud Analytics

Enhanced Data Privacy

Confidential computing provides robust protection for sensitive financial data during processing, significantly minimizing exposure risks during fraud detection and analytics operations. Research published in Electronics journal demonstrates that traditional computing environments expose data during the processing phase, while confidential computing maintains encryption throughout the entire data lifecycle. The study found that TEE-protected environments can reduce the attack surface by up to 93.7% compared to conventional cloud deployments [7]. This protection is particularly valuable for financial institutions processing high volumes of sensitive transaction data, as it prevents exposure even when the underlying operating system or hypervisor is compromised.

Regulatory Compliance

Confidential computing helps organizations comply with global data protection regulations by ensuring sensitive data remains confidential during analysis. Recent studies show that financial institutions implementing confidential computing technologies achieve higher compliance scores with GDPR, CCPA, and regional financial regulations due to the inherent privacy-preserving nature of the technology. As documented in Electronics, the ability to provide cryptographic attestation of compliant processing reduces audit preparation time by approximately 42% and simplifies demonstration of compliance with data minimization principles [7]. This reduction in compliance overhead represents a significant operational benefit beyond the direct security advantages.

Trust and Transparency

Confidential computing builds confidence among customers, partners, and regulators in fraud detection systems that provide privacy-preserving analytics. By enabling transparent operation with cryptographic guarantees, institutions can demonstrate responsible data handling without actually exposing the underlying data. Research shows that TEE-based systems can provide attestation reports that satisfy 97% of common audit requirements without compromising sensitive data [7]. This capability creates a foundation for building trust relationships across organizational boundaries that were previously limited by data privacy concerns.

Real-Time Fraud Detection

Confidential computing enables secure real-time data processing for immediate fraud detection, preventing financial losses and reputational damage. Recent research exploring financial fraud detection through

artificial neural networks demonstrates that modern machine learning techniques can achieve detection accuracy of 97.85% with minimal false positives when properly implemented [8]. When these advanced detection algorithms are deployed within confidential computing environments, organizations can maintain this high accuracy while adding cryptographic privacy guarantees. The performance overhead of TEE-based processing has been reduced to just 4-11% compared to conventional environments, making real-time secure processing viable even for high-volume transaction systems [8].

Collaboration without Compromise

Confidential computing allows organizations to collaborate on fraud detection efforts without compromising client data privacy. Studies published in Electronics demonstrate that secure multi-party computation within TEEs enables multiple financial institutions to jointly analyze transaction patterns across organizational boundaries while maintaining strict data separation [7]. Similarly, research on artificial neural networks for fraud detection shows that federated learning approaches implemented within trusted execution environments can achieve 92.3% of the accuracy of centralized models while keeping sensitive training data within each organization's security perimeter [8]. This collaborative capability is particularly valuable for detecting sophisticated fraud schemes that deliberately operate across multiple financial institutions to avoid detection.

European Journal of Computer Science and Information Technology,13(24),115-128, 2025
Print ISSN: 2054-0957 (Print)
Online ISSN: 2054-0965 (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Table 2: Security and Efficiency Benefits of Confidential Computing for Financial Institutions [7, 8]

Benefit Category	Metric	Value	Comparison/Context
Enhanced Data Privacy	Attack Surface Reduction	93.7%	Compared to conventional cloud deployments
Regulatory Compliance	Audit Preparation Time Reduction	42%	Due to cryptographic attestation capabilities
Trust and Transparency	Audit Requirements Satisfaction	97%	Without compromising sensitive data
Real-Time Fraud Detection	Machine Learning Detection Accuracy	97.85 %	With minimal false positives
Real-Time Fraud Detection	TEE Processing Performance Overhead	4-11%	Compared to conventional environments
Collaboration	Federated Learning Accuracy	92.3%	Compared to centralized models
Enhanced Data Privacy	Data Exposure	0%	During processing phase
Regulatory Compliance	Compliance Score	Higher	With GDPR, CCPA, and regional regulations
Trust and Transparency	Data Exposure for Auditing	0%	While satisfying audit requirements
Collaboration	Data Sharing Requirement	0%	While maintaining analysis capabilities

European Journal of Computer Science and Information Technology,13(24),115-128, 2025
Print ISSN: 2054-0957 (Print)
Online ISSN: 2054-0965 (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Implementation of Confidential Computing in Fraud Detection

Integration with Cloud-Native Fraud Detection Platforms

Confidential computing can be integrated into existing fraud detection systems running on major cloud platforms. Modern financial fraud detection increasingly relies on microservice architectures deployed in cloud environments, with research showing that 76% of new financial systems implementations utilize this approach for improved scalability and flexibility [9]. Cloud providers including Microsoft Azure, AWS, and Google Cloud now offer confidential computing services that secure fraud analytics workloads through hardware-based isolation technologies. These cloud-native implementations utilize a combination of AI-powered detection algorithms and confidential computing to create robust security frameworks that can identify fraudulent patterns while protecting sensitive data.

Recent cybersecurity frameworks for fraud detection in financial systems demonstrate that containerized microservices can be effectively secured using confidential computing enclaves, with each service maintaining its own isolated memory space [9]. These services provide access to hardware-based secure enclaves where sensitive financial data can be processed without exposure to other cloud resources or even to the cloud service provider itself. The architecture allows financial institutions to maintain control over their data even when utilizing third-party cloud infrastructure, addressing a key concern in the adoption of cloud-based security solutions for sensitive financial applications.

Real-World Use Cases in Fraud Analytics

Cross-Border Fraud Detection

Financial institutions across regions can share fraud detection models and intelligence without disclosing sensitive financial data. Confidential computing creates a technical foundation for secure cross-border collaboration by ensuring that data never leaves its protected state, even during processing [10]. This capability allows banks and payment processors to implement federated fraud detection systems that span multiple jurisdictions while maintaining compliance with regional data protection regulations. Research shows that confidential computing provides memory-level isolation using CPU-based trusted execution environments, creating a secure area where shared analytics can be performed without exposing the underlying transaction data [10].

Collaboration with Law Enforcement

Financial organizations can share anonymized fraud patterns with law enforcement to trace criminal activity without disclosing individual transaction details. Cybersecurity frameworks leveraging confidential computing enable financial institutions to generate aggregate fraud pattern reports that maintain statistical validity while removing personally identifiable information [9]. The architecture allows for automated pattern extraction within secure enclaves before sharing with external agencies, ensuring that only the minimum necessary information leaves the protected environment. This approach balances the competing

demands of effective law enforcement cooperation and maintaining customer privacy and regulatory compliance.

Secure Payment Systems

Confidential computing can help prevent fraud in mobile payments or online banking by securely processing transaction data within the user's device or cloud infrastructure. Modern confidential computing implementations protect data in three states: at rest, in transit, and in use, creating a comprehensive security envelope around sensitive payment information [10]. This complete protection ensures that transaction verification and fraud detection algorithms can operate on encrypted data without creating windows of vulnerability during processing. The technology is particularly valuable for mobile payment systems, where device compromise is a significant risk factor. By leveraging device-level secure enclaves combined with cloud-based confidential computing resources, payment providers can implement continuous security monitoring throughout the transaction lifecycle without exposing sensitive financial details.

Technologies and Frameworks for Confidential Computing

Intel SGX (Software Guard Extensions)

Intel SGX represents a widely-used TEE technology enabling secure data processing in cloud environments, providing both data confidentiality and integrity during computation. This technology creates protected memory regions called enclaves that shield sensitive data and code from unauthorized access, even from privileged software like operating systems or hypervisors. Research published in Computers & Security demonstrates that SGX has been implemented across various application domains, with financial services representing one of the most significant adoption sectors due to its stringent data protection requirements [11]. The technology's architecture ensures that data remains protected even when being processed, addressing a critical security gap in traditional encryption systems that only protect data at rest and in transit.

AMD SEV (Secure Encrypted Virtualization)

AMD SEV provides an alternative TEE technology that enables secure computation in virtualized environments, ensuring data remains encrypted during processing. Unlike SGX which protects specific application components, SEV secures entire virtual machines through memory encryption, offering protection at a different granularity level. According to security research, SEV provides strong isolation properties that protect against various attack vectors including memory bus snooping, cold boot attacks, and privileged access exploitation [11]. This approach is particularly valuable for financial institutions that operate fraud detection workloads in virtualized cloud environments where they need cryptographic separation from the infrastructure provider.

Cloud Provider Services

Major cloud providers offer managed confidential computing services, simplifying integration into fraud detection systems without requiring deep hardware expertise. These services abstract the underlying

hardware complexity through standardized APIs and management interfaces. According to the research the complexity of implementing confidential computing directly has been a significant adoption barrier, with cloud-managed services reducing this friction through integration with existing development workflows and operational processes [12]. These platforms typically handle the attestation, key management, and deployment automation specifically tailored for security-sensitive workloads like fraud detection.

Challenges and Considerations

Confidential computing technologies can introduce latency and computational overhead due to encryption and secure processing mechanisms. As the research notes, this performance impact varies by implementation and workload characteristics but typically ranges from 10-30% depending on the specific operations being performed [12]. For financial fraud detection systems with real-time requirements, this overhead necessitates careful performance optimization to maintain acceptable response times.

Scaling confidential computing for large-scale fraud detection systems presents additional challenges. The research identifies memory limitations as a particular constraint, with many early-generation TEEs supporting relatively small protected memory regions that may be insufficient for complex analytics workloads [12]. Current TEE technologies may have memory and computational capacity constraints, potentially impacting the complexity of fraud detection models and data volume that can be processed securely.

Future Research Directions

Research into optimizing TEE performance and developing more efficient hardware architectures continues to advance. Security researchers are exploring innovative approaches to reduce the performance overhead while maintaining strong security guarantees [11]. Similarly, developments in cryptographic techniques such as homomorphic encryption and zero-knowledge proofs offer complementary approaches to confidential computing, potentially enabling computations on encrypted data without requiring hardware-based isolation [12]. The research highlights that the combination of these approaches could eventually lead to comprehensive security solutions that protect data throughout its entire lifecycle.

The integration of confidential computing with blockchain technology represents another promising research direction, combining the immutability and transparency of distributed ledgers with the privacy guarantees of TEEs [11]. This hybrid approach could enable auditable yet privacy-preserving fraud detection processes across organizational boundaries.

European Journal of Computer Science and Information Technology,13(24),115-128, 2025
Print ISSN: 2054-0957 (Print)
Online ISSN: 2054-0965 (Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development -UK

Table 3: Technical Characteristics and Implementation Challenges of Confidential Computing Solutions [11, 12]

Technology/Framework	Feature/Metric	Value/Characteristic	Note
Intel SGX	Protection Level	Application Components	Protected memory regions (enclaves)
	Industry Adoption	High	Particularly in financial services
	Protection Scope	Data and code	Shields from unauthorized access
AMD SEV	Protection Level	Entire Virtual Machines	Memory encryption at VM level
AMD SEV	Protection Against	Multiple attack vectors	Memory bus snooping, cold boot attacks, privileged access
	Implementation Context	Virtualized environments	Used in cloud deployments
Cloud Provider Services	Adoption Barrier Reduction	Significant	Through standardized APIs and interfaces
	Integration	Simplified	With existing workflows and processes
Confidential Computing (General)	Performance Impact	10-30%	Varies by implementation and workload
	Main Constraint	Memory limitations	Especially in early-generation TEEs
	Implementation Challenge	Performance optimization	To maintain real-time requirements
Future Development	Research Direction	TEE performance optimization	Reducing overhead while maintaining security
	Complementary Technology	Homomorphic encryption	Computations on encrypted data
	Complementary Technology	Zero-knowledge proofs	Privacy-preserving verification
	Integration Opportunity	Blockchain technology	For auditability with privacy preservation

CONCLUSION

Confidential computing represents a paradigm shift in fraud analytics, fundamentally altering how financial institutions balance security effectiveness with privacy protection. By securing data during processing through hardware-based isolation, the technology enables sophisticated fraud detection without compromising confidentiality or regulatory compliance. The integration of TEEs with advanced machine learning techniques, multi-party computation frameworks, and cryptographic verification mechanisms creates a comprehensive security architecture addressing longstanding vulnerabilities in financial systems. Though current implementations face challenges regarding performance overhead and scalability, the rapidly evolving hardware capabilities and cloud service offerings suggest a trajectory toward mainstream adoption. As financial fraud grows increasingly sophisticated, the ability to collaborate securely across organizational boundaries while maintaining strict privacy controls will become essential rather than optional. Confidential computing provides this critical capability, enabling a future where privacy and security complement rather than compete with each other in fraud prevention strategies.

REFERENCES

[1] Ambiel S. (2024), "The Case for Confidential Computing," Linux Foundation. [Online]. Available: https://www.linuxfoundation.org/hubfs/LF%20Research/TheCaseforConfidentialComputing_062724.pdf?hsLang=e

[2] Hilal W., Gadsden S.A and Yawney J (2022), "Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances," Expert Systems with Applications. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0957417421017164

[3] Dama K. et al. (2024), "Fraud Detection in Financial Transactions," ResearchGate. [Online]. Available: https://www.researchgate.net/publication/379654286_Fraud_Detection_in_Financial_Transactions

[5] Aldasoro I., Gambacorta L., Giudici P. and Leach T (2020), "Operational and cyber risks in the financial sector," BIS Working Papers No 840. [Online]. Available: https://www.bis.org/publ/work840.pdf

[6] Hosameldeen O. and Yuan F.B. (2022), "A Comprehensive Analysis of Trusted Execution Environments," 2022 8th International Conference on Information Technology Trends (ITT). [Online]. Available: https://www.researchgate.net/publication/363106383_A_Comprehensive_Analysis_of_Trusted_Execution_Environments

[7] Infosys BPM, "AI in the banking sector: How fraud detection with AI is making banking safer," Infosys BPM, 2023. [Online]. Available: https://www.infosysbpm.com/blogs/bpm-analytics/fraud-detection-with-ai-in-banking-sector.html

[8] Vidaković M. and Vinko D. (2023), "Hardware-Based Methods for Electronic Device Protection against Invasive and Non-Invasive Attacks," Electronics. [Online]. Available: https://www.mdpi.com/2079-9292/12/21/4507

[9] Ori B., Ori C.I., and Ezekiel L. (2024), "Exploring Financial Fraud Detection: A Comprehensive Analysis and Implementation of Machine Learning with Artificial Neural Network," ResearchGate [Online]. Available: https://www.researchgate.net/publication/378908863_Exploring_Financial_Fraud_Detection_A_Comprehensive_Analysis_and_Implementation_of_Machine_Learning_with_Artificial_Neural_Network

[10] Kokogho E., Odio P.E., Ogunsola O.Y. and Nwaozomudoh M.O. (2025), "A Cybersecurity framework for fraud detection in financial systems using AI and Microservices," ResearchGate, 2025. [Online]. Available: https://www.researchgate.net/publication/388833198_A_Cybersecurity_framework_for_fraud_detection_in_financial_systems_using_AI_and_Microservices

[11] Felk Y.(2023) , "Confidential Computing," Trends in Data Protection and Encryption Technologies [Online]. Available: https://www.researchgate.net/publication/372801790_Confidential_Computing

[12] Muñoz A. et al. (2023), "A survey on the (in)security of trusted execution environments," Computers & Security. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404823000901

[13] Linux Foundation, "The Challenges and Rewards of Confidential Computing," Linux Foundation, 2024. [Online]. Available: https://www.linuxfoundation.org/blog/the-challenges-and-rewards-of-confidential-computing