UDC 336.717:004.056

FIGHTING MONEY LAUNDERING WITHOUT SHARING SECRETS: PRACTICAL USE OF CONFIDENTIAL COMPUTING

Sosnovskiy T.I.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Goncharova I.V. – Lecturer at the Department of Foreign Languages

Annotation. This paper explores the conflict between anti-money laundering efforts and strict banking privacy laws. It introduces Confidential Computing and Secure Enclaves as a secure solution to this problem. By utilizing secure, isolated environments, financial institutions can collaboratively analyze encrypted transaction data to detect financial crimes without ever exposing sensitive customer details. The article also highlights current real-world applications of this technology.

Keywords: confidential computing, secure enclaves, banking privacy, privacy-enhancing technologies, anti-money laundering, financial crime.

Introduction. Money laundering is the lifeblood of organized crime. It is the process by which illegally obtained funds are made to look legitimate, allowing criminals to use their profits without drawing the attention of law enforcement. In today's digital age, money laundering has become highly sophisticated. Modern criminal enterprises rarely use a single bank to clean their money. Instead, they fragment their transactions across multiple banks and send money across borders to make the trail confusing and borderline untraceable. [1]

Main part. It's usually impossible for a single bank to catch these transactions without seeing the full picture: where the money came from initially, who approved the transfer, their transaction history, etc. Banks need to share this data to connect the dots. However, this creates a massive conflict with data privacy. Strict laws forbid banks from simply handing over their clients' private transaction records to competitors or third parties. This creates a paradox: banks must share information to stop financial crime, but they are legally forbidden from sharing information to protect their customers' privacy. [2]

For years, this barrier seemed impossible to overcome. However, with the advent of Confidential Computing and secure enclaves, it became possible to share secrets between computers of different parties without actually revealing any data to a human. [3]

To understand it, let's first look at how data is typically protected. Historically, cybersecurity focused on protecting data when it is saved on a hard drive with the use of encryption (data at rest), and when it is sent over a network (data in transit). [4] However, there is a third state: data in use (Figure 1). Usually, a processor cannot work on encrypted data directly, so it needs to be decrypted and loaded into memory first. This is the vulnerable point where data is exposed to the operators of the system and hackers.

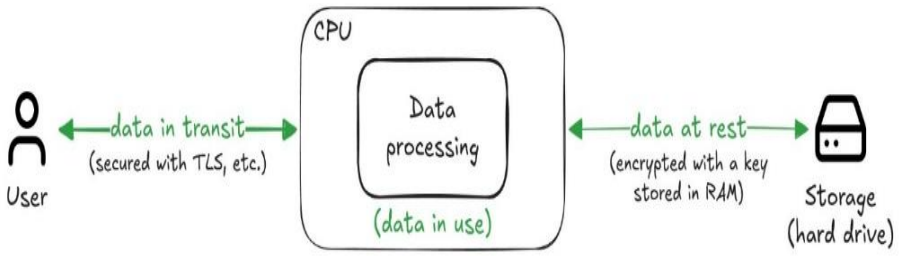

Figure 1 – Overview of the three states of digital data

Confidential Computing closes this gap by protecting data while it is being used. It does this through a hardware technology called a secure enclave. A secure enclave is an imaginary «locked box» stored deep within the computer's processor. Encrypted data comes into it, gets processed inside

it without leaking anything, and then some output becomes available to the outside world.his isolation is built directly into the physical hardware of the CPU, we only need to trust its manufacturer and the code running inside the enclave. Everything else can be cryptographically proven. Furthermore, developers can utilize memory-safe programming languages, such as Rust, to build secure software to be run inside the isolated environment, ensuring that no underlying vulnerabilities can be exploited to leak information from inside.

So, we can solve the privacy problem by allowing banks to share data between each other securely by building upon this hardware-level security. Crucially, the enclave can be programmed to output only the results of an analysis, not the transaction data. The output might simply be an alert: "This account and that account have a 95% probability of being part of the same money laundering network." This analysis can even be performed by an AI model that is running on a connected GPU. [5] Because the algorithm is transparent and verifiable, all participating banks or regulatory bodies know exactly what happens with the data, even if no one knows what data is coming in.

Several major institutions have already begun deploying Confidential Computing to tackle financial crime and other data-sensitive problems. One of the most remarkable examples is the collaboration between SWIFT and their partners. They have been developing an AI model with the help of Confidential Computing that allows them to detect fraud more easily. Along with other privacy-enhancing technologies, their initiative allows participants to collectively screen transactions for signs of money laundering and terrorist financing across institutional boundaries, all without any single party ever seeing another's customer data. They claim that this approach made the AI model twice as effective. [6,7]

Beyond the financial sector, confidential computing is also being adopted in healthcare. [8] The major cloud providers have recognized this demand as well. Microsoft Azure, Google Cloud, and Amazon Web Services all now offer confidential computing services built on top of hardware enclaves from Intel, AMD, NVIDIA, and others, making the technology accessible to smaller organizations that previously lacked the resources to implement such solutions on their own. [8–10]

Conclusion. The fight against money laundering has always been an arms race, with criminals constantly finding new ways to exploit the gaps between institutions and jurisdictions. For decades, one of the biggest gaps was legal and ethical: the inability to share private data across organizational borders. Confidential Computing does not eliminate privacy regulations. Instead, it offers an architectural solution that respects the spirit of these laws while still enabling collaborative analysis. By ensuring that sensitive data is also protected while it is actively being processed, secure enclaves remove the need for trust or contracts between parties and replace it with something far more reliable: verifiable, hardware-enforced isolation. This technology proves that privacy and transparency are not opposing forces but can, with the right engineering, work hand in hand.

References

1. Радюк Д. И. Легализация незаконных доходов: анализ моделей «отмывания» денег // Банковский бизнес и финансовая экономика: глобальные тренды и перспективы развития : материалы V Междунар. науч.-практ. конф. молодых ученых, магистрантов и аспирантов. Минск: Белорус. гос. ун-т, 2020. Pp. 170–177.

2. Guidance on private sector information sharing. Paris: FATF, 2017. 50 p.

3. Scapicchio M., Kosinski M. What is confidential computing? [Electronic resource]. IBM. Mode of access: https://www.ibm.com/think/topics/confidential-computing (accessed: 28.02.2026).

4. Fitzgibbons L. States of Digital Data [Electronic resource]. 2019. Mode of access: https://www.techtarget.com/searchdatamanagement/reference/states-of-digital-data (accessed: 28.02.2026).

5. Kumar U., Emily S. Protecting Sensitive Data and AI Models with Confidential Computing [Electronic resource]. NVIDIA, 2023. Mode of access: https://developer.nvidia.com/blog/protecting-sensitive-data-and-ai-models-with-confidential-computing/ (accessed: 28.02.2026).

6. 2023 Swift Annual Review [Electronic resource]. SWIFT, 2023. Mode of access: https://www.swift.com/swift-resource/252305/download (accessed: 02.03.2026).

7. Swift AI innovation creates blueprint for banks to stop fraud faster through cross-border collaboration [Electronic resource]. SWIFT, 2025. Mode of access: https://www.swift.com/news-events/press-releases/swift-ai-innovation-creates-blueprint-banks-stop-fraud-faster-through-cross-border-collaboration (accessed: 02.03.2026).

8. Azure Confidential Clean Rooms Preview [Electronic resource]. Microsoft, 2025. Mode of access: https://learn.microsoft.com/en-us/azure/confidential-computing/confidential-clean-rooms (accessed: 02.03.2026).

9. Confidential Computing [Electronic resource]. Google Cloud. Mode of access: https://cloud.google.com/security/products/confidential-computing (accessed: 02.03.2026).

10. Brown D. Confidential computing: an AWS perspective [Electronic resource]. AWS Security Blog, 2021. Mode of access: https://aws.amazon.com/blogs/security/confidential-computing-an-aws-perspective/ (accessed: 02.03.2026).