White Paper

Financial services
Cyber security

Federated Learning through Revolutionary Technology

A 21st Century Solution for Combating Money Laundering and the Financing of Terrorism.

Authors

Gary Shiffman and Juan Zarate
Consilient

Nikhil Deshpande, Raghuram Yeluri and Parviz Peiravi
Intel

Table of Contents

The Challenge: Threats, Inadequate AML/CFT Systems and Regulatory Risk

Threats. Financial institutions are under stress. The enduring responsibility of detecting and preventing illicit financing activities has grown increasingly complex in today's 21st century environment as financial institutions process trillions of dollars in transactions every day. In these financial flows, money launderers, terrorist financiers, fraudsters, sanctions evaders, and a range of illicit actors attempt to hide their criminal activities and leverage sophisticated corporate and financial vehicles and new technologies to avoid detection. Illicit financing fuels dangerous international security threats, empowers and profits criminal networks and rogue regimes, and deepens the corruption of societies and governments.

The United Nations Office on Drugs and Crimes estimates the amount of money laundered globally in one year ranges between two and five percent of global GDP—trillions of dollars each year. In today's digital world, such money moves across the globe in milliseconds, speeding the flow and potential volume of illicit funds.

The current anti-money laundering and countering the financing of terrorism **(AML/CFT)** system is neither keeping pace with the corrosive threats from illicit finance nor preventing the abuse of the international financial system.

A Sub-Optimal AML/CFT Framework. Frustratingly, financial institutions today are relying on an outdated AML/CFT system that has proved inadequate and inefficient in combating illicit financing. It is a reactive system that relies on individual institutions to detect suspicious activity on their own. The sub-optimal nature of the current implementation of the AML/CFT system is rooted in two primary problems:

- **Existing Transaction Monitoring Systems that Fail to Detect Illicit Activity.** Financial institutions today are using 20th century tools to fight 21st century threats. They have spent billions of dollars on rules-based compliance solutions that produce an unacceptably high false-positive rate – often more than 95 percent. Costly manual reviews are then required to sift through the mountains of alerts in order to flag questionable customers and transactions that merit the submission of suspicious activity reports (SARs) to authorities. As a result, not enough significant illicit financing is discovered proactively and prevented in the financial system.

- **Information-Sharing Constraints Among Siloed Financial Institutions.** Financial institutions working within the existing AML/CFT system are islands — they work in isolation to identify and report a suspicious customer or transaction to a financial intelligence unit. The system does not encourage information sharing, dynamic feedback, or collective learning between and among enterprises. Moreover, data privacy and localization concerns globally have further constrained the sharing of sensitive customer data across borders, and technologies and mechanisms established to facilitate inter-bank information sharing have not overcome these barriers systematically.

As a result, financial institutions cannot effectively and efficiently identify the illicit activity within their systems – and the most significant illicit financing happening within the financial system. Suffering from institutional blind spots, they are not able to track sophisticated criminals who take advantage of information limitations to leap selectively among a series of institutions — sometimes within different locations of the same bank — to obscure their activities. For example, similarly, situated banks in the Midwest may not identify the patterns of a money launderer using comparable methods to open front accounts and layer and move money between institutions and into the economy. Ultimately, sophisticated criminals are exploiting these gaps.

Regulatory Risks. Compounding this stress is growing regulatory pressure and heightened expectations for financial institutions to ensure transparency, detect illicit activities, and prevent illicit financing in the financial system. Ever-expanding regulations and standards, technical requirements, and targeted measures to combat illicit finance — at national and global levels — create significant compliance challenges. Stringent and detailed regulatory requirements in the United States arising from the Currency and Foreign Transactions Reporting Act of 1970 (commonly referred to as the Bank Secrecy Act, or BSA) and expanded in Title III of the USA PATRIOT Act, demand that regulated institutions understand and manage their financial crime risk. Globally, the Financial Action Task Force continues to evaluate jurisdictions rigorously on the effectiveness of their AML/CFT systems. Banks need to know and monitor their customers and transactions, the risks and behaviors of their customers' clients and counterparties, and the products and services they offer. Failure to comply fully with AML/CFT expectations results in regulatory risk, with regulators having imposed billions of dollars of fines, particularly where inadequate monitoring systems fail to detect illicit activity.

Sub-Optimal Results. Altogether, the current AML/CFT system has undelivered in its mission while simultaneously burdening financial institutions with unacceptable and unintended costs. There have been many attempts to quantify the gaps in the current system, with most studies pointing to the failure to seize or freeze sufficient criminal assets to justify the related expenditures. According to one 2018 study:

- Anti-money laundering policy intervention has less than a 0.1 percent impact on criminal finances.
- Compliance costs are more than a hundred times greater than recovered criminal funds.
- Banks, taxpayers, and ordinary citizens are penalized more than criminal enterprises.

Though it is difficult to judge the overall effectiveness of preventing or deterring money laundering and the related costs imposed on criminal organizations with these types of metrics, there is no dispute that the system is not designed to achieve the policy goals of preventing illicit funds from entering the financial system. By not enabling banks or authorities to identify and manage systemic risk proactively and dynamically across institutions or borders, the current AML/CFT system simply is not fit for purpose.

The Consilient Solution: Powered with Secured Federated Learning

There is a new model for the AML/CFT system that provides a more effective and efficient means to prevent illicit finance and manage compliance risk. This model moves beyond traditional rules-based monitoring and toward one that facilitates information sharing among various authorities and institutions across the globe; enables collective learning on complex threats; distributes and shares risk; and simultaneously safeguards customer privacy and data.

It is called Federated Learning, and it is brought to you by Consilient.

Consilient is the next-generation AML/CFT model. It is the result of the commitment between K2 Intelligence and the Financial Integrity Network **(K2-FIN)** — the world's premier strategic advisory firm dedicated to financial integrity and security -- and Giant Oak — a leading technology company built upon the premise of leveraging big data, cutting-edge behavioral analytics and machine learning (ML) to uncover and counter criminal activities.

Federated Learning: How Does Work? Federated Learning is the principle behind Consilient's technology. Consilient has created a behavioral-based, ML-driven governance model that allows its algorithm to access and interrogate data sets in different institutions, databases, and even jurisdictions without ever moving the data. The technology does this through a machine learning algorithm — **not the data** — that is exchanged between servers at different institutions, allowing it to detect illicit activity more accurately within their networks. The more data the algorithm encounters and analyzes as it travels, the more effective the algorithm becomes.

Consilient utilizes artificial intelligence and access to massive data sets to provide AML/CFT and anti-fraud analytics — without moving the data or any sensitive information (see Figure 1). This model leverages federated data analytics and Consilient's proprietary DOZER technology, enabling participating financial institutions, authorities, and regulators to uncover and manage systemic risks more effectively, efficiently, and sustainably while also preserving privacy and ensuring security. Relying on behavioral analysis, DOZER's

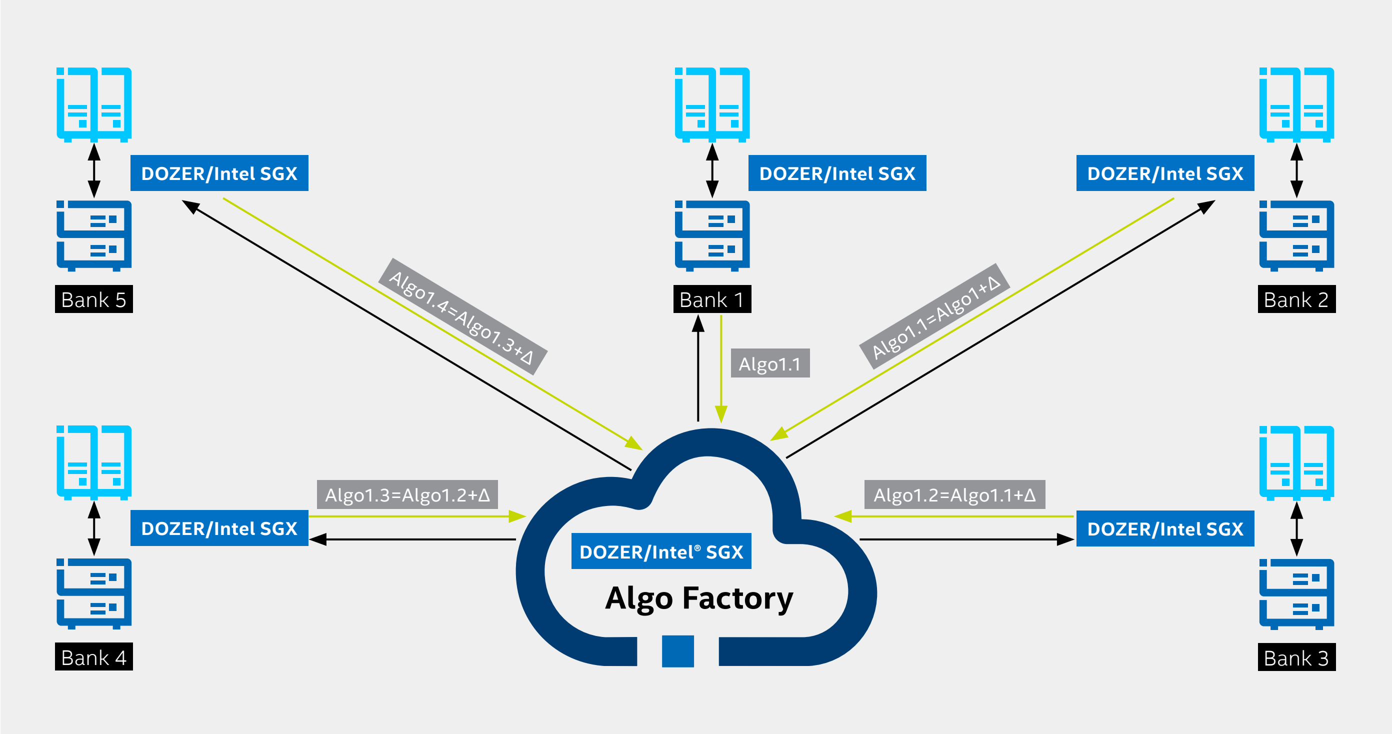

Figure 1. Consilient's Federated Learning Framework

traveling algorithms helps overcome analytic challenges, organizational siloes, and information-sharing constraints in traditional AML/CFT monitoring systems. It does this by building models of what "normal" or "legal" behavior looks like in different scenarios in order to identify when an individual's or business's financial behavior strays from the norm.

Effective Results with Federated Learning

Federated Learning leads to the following results:

- **A Reduction in Errors:** While traditional rule-based screening and AML/CFT systems have a false-positive rate typically in excess of 95 percent, Consilient's self-learning DOZER technology has proven to reduce the false-positive rate to 12 percent. This capability will allow organizations to save costs, redeploy personnel, and prioritize their counter illicit finance efforts more effectively.
- **Protection of Privacy:** The governance model is built around the anonymization and encryption of data, safeguarding the privacy of customers, users, and citizens. In doing so, jurisdictions and financial institutions will be able to maintain their commitment to removing criminal activity from their financial system while also preserving the rights of those they serve.
- **A More Effective System:** By transforming the traditionally siloed environment of financial crimes compliance into a federated network, financial institutions and jurisdictions can prevent criminal actors from exploiting the virtual financial safe havens created by the industry's inability to timely share information, risks, and insights.

Infusing Federated Learning with Security and Privacy: Intel

While Federated Learning enables dynamic collaboration across AML/CFT systems, the incorporation of end-to-end security and privacy safeguards are essential to running this innovative model within the marketplace. Data not only must remain private and confidential, but the model inside DOZER's Algorithm Factory must also remain secure from theft that could lead to data leaks or from tampering that would undermine the integrity or accuracy of the model. The communication links between federated nodes and the aggregator must also be protected from interference, potentially resulting in denial-of-serve **(DoS)** attacks.

To provide these assurances, hardware-rooted security technologies are central to the Federated Learning process. Institutions utilizing Federal Learning can be protected through security layers down to the silicon inside the compute node, or server, through hardware-based Trusted Execution Environments **(TEEs)** such as Intel® SGX at the institutions' compute nodes, as well as the aggregation engine (i.e., DOZER Algorithm Factory), where the aggregated model resides. This ensures the model at the institutions, as well as the model inside the aggregation engine, are computed inside a trusted environment that protects the confidentiality and integrity of code and data. Simultaneously, the communications between edge and aggregation engine are also protected from tampering, providing confidence in the privacy and security of both the dataset and the machine learning model.

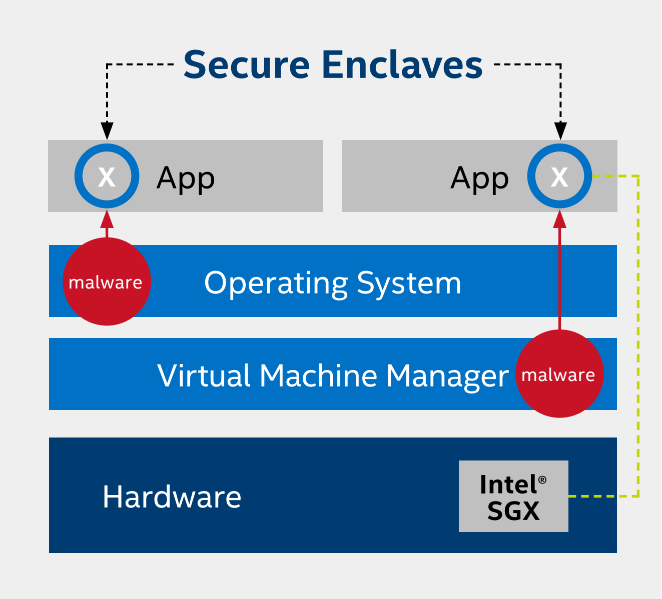

Figure 2. Intel® SGX Stack

Secure Federated Learning Architecture with TEE Intel® SGX

Intel® Software Guard Extensions is a hardware-based TEE that helps protect against code/data snooping, as well as code and data modifications by malware on the system. The technology has the root of trust limited to a small portion of the CPU hardware and the machine learning application itself. The fundamental principle behind Intel® SGX is to minimize the trusted computing base in order to significantly reduce the surface from where an attack can be launched. Figure 2 shows how Intel® SGX helps protect against malware inside the OS or VMM from snooping on the application code and data.

Effective Results with TEE Intel® SGX

Incorporation of Intel® SGX into Federated Learning leads to the following results:

- **Protection Against Software Attacks.** Intel® SGX helps protect against software attacks, even if OS/drivers/BIOS/VMM/SMM are compromised - and helps increase protections for secrets (data/keys) even if an attacker has full control of the platform. This helps protect against insider attacks at financial institutions where the attacker might try to modify or exploit the model, resulting in sensitive data leaks and model inefficacy.
- **Prevention of Attacks Against Memory Content.** Intel® SGX helps prevent attacks—including memory bus snooping, memory tampering, and “cold boot” attacks—against memory contents in RAM. Such protection helps ensure the data in memory (e.g., model hyperparameters, weights) are not tampered with or stolen, which could help the attacker identify sensitive data about the model and the data.
- **Option for Hardware-Based Attestation.** Intel® SGX provides an opportunity for hardware-based attestation capabilities to measure and verify valid code and data signatures. The attestation mechanisms increase the confidence level across the participants in the AML/CFT system regarding the integrity of the model and data.

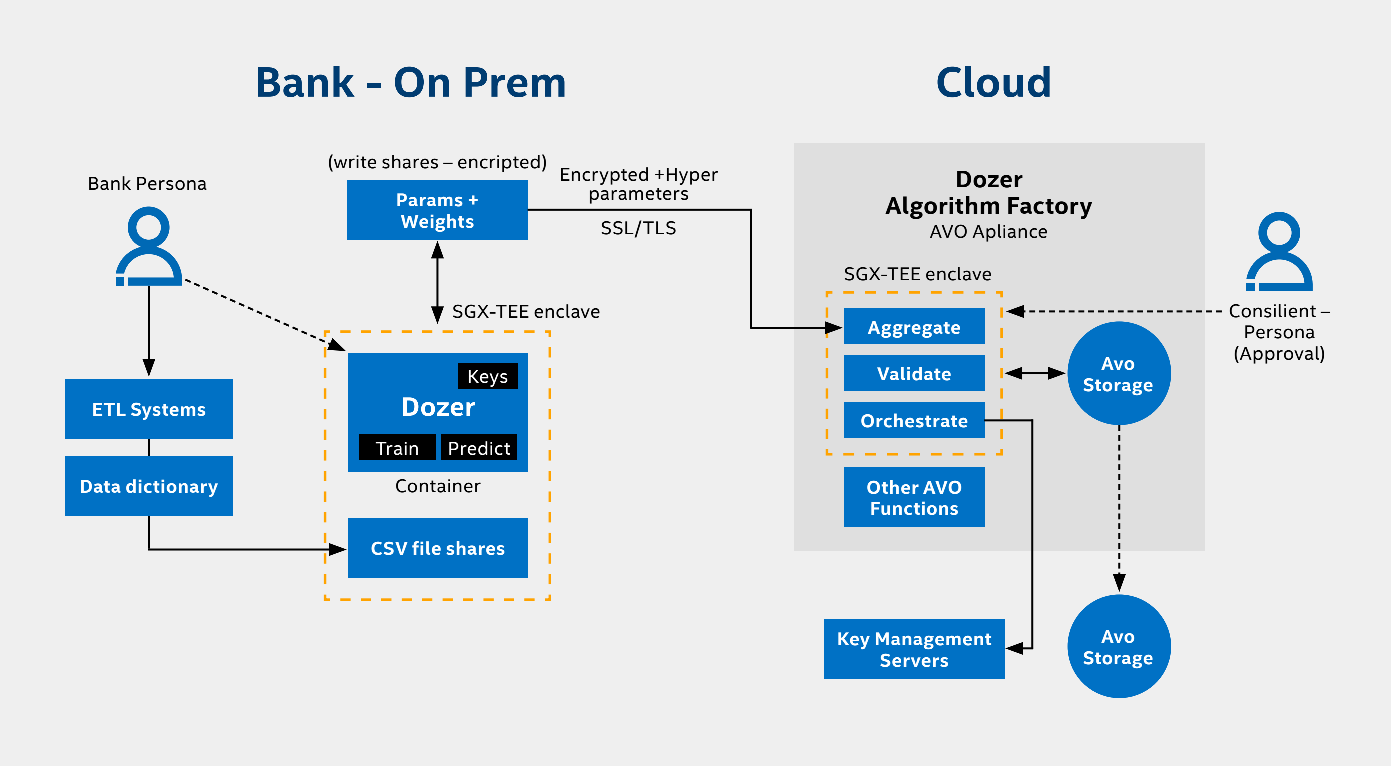

Figure 3. Secure Privacy-Preserving Federated Learning AML Solution Architecture

The Comprehensive Security Architecture: An AML/CFT system with fully enabled Intel® SGX protections requires a comprehensive system security architecture to better protect itself against insider and external attacks on the system.

Within the architecture outlined in Figure 3, compute nodes at the bank premises run DOZER models inside a trusted container protected by Intel® SGX. The container is encrypted outside of the CPU via Intel® SGX, which helps prevent anyone accessing the compute node from seeing or modifying model hyperparameters and weights. After training the DOZER algorithm on one node, the modified weights will be transmitted over an encrypted link (SSL/TLS) to the DOZER Algorithm Factory for Validation and further Orchestration.

In order to help ensure confidentiality and integrity protection for the aggregation engine compute and data, Intel® SGX is deployed on the cloud-side of the system. The code and data for the Dozer Algo Factory executes inside an Intel® SGX protected Docker container, as displayed in Figure 3.

Conclusion

As it exists today, the current AML/CFT system compels the financial industry to spend billions of dollars on compliance, while illicit financing continues to flow to the tune of trillions of dollars. There is a fundamental need for a new design for the AML/CFT system, and this technology and model provide an elegant new framework and capability.

Until now, the financial industry has never had a Federated Learning technology that allows the access and interrogation of data sets in different institutions, databases, and even jurisdictions without ever moving the data or any sensitive customer information.

Consilient's DOZER technology can analyze, identify, and find "normal" and "abnormal" patterns in datasets that human eyes and most current technologies cannot. In turn, Intel® SGX can help protect AML/CFT systems against malware and data snooping while helping to comply with required privacy and confidentiality laws. Using both the DOZER and Intel® SGX technologies, government and financial institutions can securely detect enormous amounts of illicit activity quickly, which will have significant implications in combating financial crime, thwarting terrorist efforts, and enabling legitimate individuals and businesses to thrive.

The combination of this new architecture, analytics, and governance makes this the **preferred** model in today's quest for a more effective and efficient AML/CFT system.

Intel technologies may require enabled hardware, software or service activation.
No product or component can be absolutely secure.
Your costs and results may vary.