**Securing Confidentiality in Distributed Ledger Systems with Secure Multi-Party Computation for Financial Data Protection**

**Abstract**

*This study investigates the effectiveness of Secure Multi-Party Computation (SMPC) in enhancing confidentiality within Distributed Ledger Systems (DLS) for financial applications. Using the Elliptic AML Bitcoin Transactions dataset, anomaly detection (Isolation Forest) identifies financial confidentiality vulnerabilities, revealing that anomalous transactions exhibit a 336.1% increase in volume and a 15.5% rise in frequency, suggesting heightened risks. A comparative analysis of SMPC protocols utilizing the MP-SPDZ benchmark dataset and one-way ANOVA confirms that Yao’s Garbled Circuits is the most computationally efficient (180.50 ms execution time), whereas Shamir’s Secret Sharing offers superior security (0.73 high-probability security). Kaplan-Meier survival analysis of Verizon DBIR 2024 establishes that SMPC extends financial system longevity (36.11 months vs. 21.91 months for traditional encryption). Recommendations include integrating scalable SMPC models, standardizing regulatory frameworks, optimizing algorithmic efficiency, and enhancing anomaly detection in financial DLS.*

**Keywords: Secure Multi-Party Computation, Distributed Ledger Systems, Confidentiality Risks, Anomaly Detection, Financial Cryptography**

**1. Introduction**

The increasing reliance on digital infrastructures in the financial sector has heightened concerns regarding data confidentiality and security. Distributed Ledger Systems (DLS) offer a decentralized and immutable framework that enhances transparency and security in financial transactions. However, the inherent transparency of DLS raises significant confidentiality challenges, particularly in safeguarding sensitive financial data from unauthorized access. This issue is further exacerbated by the rising frequency of cyber breaches, necessitating the implementation of advanced security mechanisms that preserve data privacy while maintaining the benefits of decentralization.

The growing prevalence of cyber incidents underscores the urgency of enhancing security measures within financial institutions. According to Gregorian (2019), approximately 75% of financial services organizations have experienced at least one data breach in the past five years, surpassing the industry average of 66%. The financial consequences are substantial, with the average cost of a data breach in the sector reaching $6.08 million in 2024 (Petrosyan, 2024). Notable breaches, such as those affecting LoanDepot and Evolve Bank & Trust—compromising the data of 16.9 million and 7.6 million individuals, respectively—illustrate the vulnerabilities associated with handling sensitive customer information (Schappert, 2024; Uberoi, 2024). Regulatory bodies have responded by imposing stringent penalties, as evidenced by New York State’s $11.3 million fine on Geico and Travelers for cybersecurity lapses (Kapko, 2024). These developments highlight the critical need for robust security measures that safeguard financial data while ensuring compliance with evolving regulatory frameworks.

Several vulnerabilities contribute to confidentiality challenges in DLS implementations. While encryption secures data during transit and storage, decryption is required for processing, thereby introducing potential exposure points (Agrawal et al., 2024). Additionally, adversaries can exploit inference attacks by correlating seemingly anonymized data across multiple sources, reconstructing sensitive financial information such as transaction details, customer identities, and proprietary trading strategies. Furthermore, the decentralized architecture of DLS complicates secure key management, increasing the risk of unauthorized access. These vulnerabilities expose financial institutions to significant threats, including financial losses, reputational damage, and regulatory penalties, underscoring the need for advanced cryptographic solutions to address confidentiality concerns effectively (Prakash & Garg, 2024).

Secure Multi-Party Computation (SMPC) has emerged as a viable cryptographic approach to mitigating these confidentiality risks. SMPC enables multiple parties to collaboratively compute functions on encrypted data without revealing individual inputs, ensuring that sensitive financial information remains protected throughout the computation process (Nookala, 2023). The financial sector's adoption of SMPC is being driven by regulatory mandates and technological advancements. The global SMPC market, valued at $794.1 million in 2023, is projected to grow at a compound annual growth rate of 11.8%, reaching approximately $1.72 billion by 2030 (SEC, 2023). North America holds a dominant market share due to rapid technological advancements and stringent data protection regulations, further emphasizing the significance of privacy-preserving technologies in financial applications.

The practical applications of SMPC in financial DLS implementations demonstrate its effectiveness in enhancing data security. Inpher’s collaboration with the UK’s Financial Conduct Authority illustrates how SMPC facilitates fraud detection and anti-money laundering (AML) initiatives by enabling financial institutions to analyze transaction patterns while preserving data confidentiality (Inpher, 2023). Similarly, Parfin has leveraged SMPC since 2019 to enhance security in digital asset custody by distributing cryptographic keys, thereby mitigating the risk of unauthorized access. Microsoft’s Confidential Consortium Framework integrates Trusted Execution Environments with blockchain technology to ensure data privacy in enterprise applications (ShubhraS, 2022). Early implementations, such as the Danish Sugar Beet Auction, further validate the feasibility of SMPC in securing financial transactions, demonstrating its potential to revolutionize data privacy in decentralized financial ecosystems.

Despite its advantages, the widespread adoption of SMPC in financial DLS is hindered by challenges related to scalability, computational efficiency, and interoperability. The complexity of SMPC protocols introduces substantial computational and communication overhead, particularly in large-scale financial transactions (Gamiz et al., 2024). Ongoing research aims to optimize these protocols to enhance efficiency, reduce latency, and improve transaction throughput (Bautista et al., 2023; Rahaman et al., 2024). Additionally, interoperability remains a critical concern, necessitating the development of standardized SMPC frameworks to facilitate integration across diverse financial systems.

Regulatory compliance plays a pivotal role in the adoption of SMPC within financial DLS. The European Central Bank’s 2024 cyber stress test revealed significant cybersecurity shortcomings, underscoring the urgent need for improved privacy protocols (European Central Bank, 2024). Stringent regulatory frameworks, including the General Data Protection Regulation (GDPR), the Financial Stability Board guidelines, and the cybersecurity mandates of the United States Securities and Exchange Commission, impose rigorous data protection requirements on financial institutions (Gounari et al., 2024). Non-compliance with these regulations can result in severe financial penalties and reputational harm, reinforcing the necessity of privacy-preserving technologies such as SMPC to align with evolving legal and industry standards. The integration of SMPC within DLS presents a promising approach to mitigating confidentiality risks in financial transactions. By enabling privacy-preserving computations and secure data-sharing mechanisms, SMPC enhances the security and efficiency of financial processes while maintaining regulatory compliance.

However, addressing the challenges associated with scalability, computational efficiency, and interoperability remains crucial for its widespread adoption. Continued advancements in cryptographic research and regulatory adaptation will be essential in ensuring the effective integration of SMPC, thereby fortifying the financial sector against emerging cybersecurity threats. This research aims to investigate the effectiveness and feasibility of employing Secure Multi-Party Computation (MPC) to enhance confidentiality and data protection within Distributed Ledger Systems (DLS) for financial applications, while considering performance, security, and regulatory compliance, by achieving the following objectives:

1. Analyzes the specific confidentiality challenges and vulnerabilities inherent in current DLS implementations for financial data, identifying the types of sensitive information at risk and the potential consequences of data breaches.
2. Compares the different MPC protocols and techniques in terms of their suitability for addressing the identified confidentiality challenges in DLS for financial applications, considering computational complexity, communication overhead, and security guarantees.
3. Explores real-world applications and case studies demonstrating the integration of SMPC in financial Distributed Ledger Systems.
4. Assesses the scalability, computational efficiency, and regulatory implications of implementing SMPC in financial transactions within DLS.

**2. Literature Review**

Distributed Ledger Systems (DLS) have gained prominence in the financial sector due to their decentralized and immutable frameworks, which enhance transparency, security, and efficiency in financial transactions. Antal et al. (2021) argues that DLS function as shared databases distributed across multiple nodes, ensuring that each participant maintains an identical copy of the ledger. This decentralized architecture reduces the risk of a single point of failure, thereby strengthening system resilience and eliminating the need for a central authority (Jimmy, 2024; Balogun, 2025). Moreover, de la Roche et al. (2025) posits that the immutability of DLS reinforces financial record integrity, as recorded data cannot be modified without network consensus, fostering trust and accountability in financial operations.

DLS are generally categorized into permissioned and permissionless blockchains, each possessing distinct implications for financial applications. According to Bellaj et al. (2024), permissionless blockchains, such as Bitcoin and Ethereum, operate as open networks that allow unrestricted participation, exemplifying decentralization by distributing control across numerous nodes. This model ensures transparency, as all transactions remain publicly verifiable (Dong et al., 2023; Olutimehin et al., 2025). However, Wylde et al. (2022) contends that the lack of access controls presents challenges related to scalability and regulatory compliance, particularly in financial contexts where data privacy is crucial. Conversely, permissioned blockchains restrict participation to authorized entities, such as financial institutions, ensuring improved performance and regulatory compliance (Mustafa et al., 2024; Obioha-Val et al., 2025). Daah et al. (2024) avers that this controlled environment enhances transaction validation security but introduces centralization risks, as governing institutions retain significant control over the network.

Despite these advantages, Ojha and Thakur (2025) alludes to the confidentiality challenges posed by DLS transparency, particularly regarding sensitive financial data. This issue, often referred to as the "transparency paradox," arises from the conflict between maintaining an open, verifiable system and protecting confidential financial information (van Zeeland & Pierson, 2024; (Balogun et al., 2025). Sarfaraz et al. (2023) states that on-chain storage of sensitive data exposes it to all network participants, increasing the risk of unauthorized access. Even with pseudonymization techniques, sophisticated inference attacks can correlate blockchain data with external sources, potentially revealing private financial details (Makhdoom et al., 2024; Obioha-Val et al., 2025).

To address these concerns, various security mechanisms have been proposed. Encryption-based solutions, such as homomorphic encryption and zero-knowledge proofs (ZKPs), offer promising approaches to safeguarding financial data. Hamza et al. (2022) contends that homomorphic encryption enables computations on encrypted data without requiring decryption, facilitating secure analysis while preserving confidentiality. However, its computational overhead presents efficiency challenges. Similarly, Zhou et al. (2024) posits that ZKPs allow transaction validity verification without exposing sensitive details, ensuring privacy while maintaining auditability.

Another approach involves Trusted Execution Environments (TEEs), which create isolated environments for processing sensitive data. In the view of Muñoz et al. (2023), TEEs enhance security by protecting data during computation, yet they rely on hardware-based trust assumptions and remain vulnerable to specific attack vectors. Furthermore, Kumar et al. (2024) argues that Secure Multi-Party Computation (SMPC) is increasingly explored as a confidentiality solution, enabling secure computations on encrypted inputs without revealing underlying information.

As Ataullah and Chauhan (2024) states, the expanding adoption of DLS in financial applications necessitates ongoing research into privacy-preserving technologies that balance transparency, security, and scalability. Addressing these challenges remains essential to ensuring that DLS effectively supports financial transactions while safeguarding sensitive data from emerging cybersecurity threats.

### **Secure Multi-Party Computation (SMPC) as a Confidentiality Solution**

### Secure Multi-Party Computation (SMPC) is a cryptographic framework that enables multiple parties to collaboratively compute a function over their respective inputs while preserving data confidentiality. Batan (2024) posits that unlike conventional cryptographic techniques that primarily focus on securing communication channels, SMPC directly addresses the challenge of performing collaborative computations without exposing individual data. Its conceptual foundations can be traced to the late 1970s through secure game-playing protocols, later formalized by Andrew Yao in the 1980s with the introduction of secure two-party computation (Chainlink, 2024; Kolade et al., 2025).

### Several cryptographic primitives underpin SMPC’s functionality. According to Alam et al. (2024), secret sharing schemes, such as Shamir's Secret Sharing, distribute a secret among multiple participants, ensuring that only authorized subsets can reconstruct the original data. Oblivious transfer allows a sender to transmit one of many pieces of information to a receiver without knowledge of the specific selection, preserving privacy. Yao’s Garbled Circuits facilitate two-party computations by encoding logic gates into encrypted formats, enabling function evaluation without revealing inputs (Xu & Joshi, 2020; Balogun et al., 2025). Additionally, homomorphic encryption supports computations on encrypted data, allowing results to be obtained without exposing raw information. Batan (2024) contends that these cryptographic building blocks collectively enable SMPC to provide confidentiality in distributed computing environments.

### In the context of Distributed Ledger Systems (DLS), SMPC serves as a critical tool for safeguarding data privacy while enabling secure computations over financial transactions. Almusawi et al. (2023) argues that although initially designed for two-party scenarios, Yao’s Garbled Circuits have been extended to multi-party settings, facilitating collaborative computations without compromising individual data privacy. The Goldreich-Micali-Wigderson (GMW) protocol further enhances these capabilities by incorporating secret sharing and oblivious transfer for secure Boolean circuit computation (Allaart et al., 2024; Mayeke et al., 2024). Additionally, additive and multiplicative secret sharing schemes allow for secure arithmetic operations, a crucial feature in financial applications requiring aggregation and analysis of sensitive transactional data (Ali et al., 2024; Olutimehin, 2025).

### A comparison of SMPC with alternative privacy-preserving techniques highlights key distinctions. Chi et al. (2023) avers that Zero-Knowledge Proofs (ZKPs) enable a party to verify knowledge of a value without disclosing the value itself, making them effective for verification but unsuitable for collaborative computation. Differential privacy, which introduces noise into datasets to obscure individual data points, is beneficial for statistical analysis but lacks precision for financial calculations (Janghyun et al., 2022; Obioha-Val, 2025). Federated learning allows decentralized model training without exposing raw data; however, Zhang et al. (2021) posits that it does not inherently prevent information leakage through model updates. In contrast, SMPC provides an exact computational framework while preserving confidentiality, making it particularly suited to financial applications (Rahaman et al., 2024; Olutimehin, 2025).

### Despite its advantages, SMPC presents challenges related to computational efficiency and practical deployment. Gamiz et al. (2024) contends that the computational complexity of SMPC protocols significantly increases processing times, as encrypted operations require greater computational resources than plaintext computations. Additionally, extensive cryptographic exchanges among parties introduce communication overhead, particularly in high-latency networks (Shirali et al., 2023; Obioha-Val et al., 2025). Although SMPC ensures that no information beyond the intended output is disclosed, this security guarantee often comes at the cost of increased algorithmic complexity and resource consumption. In the views of Batan (2024), optimizing these protocols for efficiency without compromising security remains essential for their integration into real-world financial systems. Ongoing research into advanced cryptographic techniques continues to refine SMPC, reinforcing its viability as a privacy-preserving solution in DLS applications (Prabowo et al., 2025; Zhou et al., 2024; Olutimehin, 2025).

### **Adoption of SMPC in Financial Distributed Ledger Systems**

Secure Multi-Party Computation (SMPC) has gained increasing recognition in the financial sector due to its potential to enhance data confidentiality within Distributed Ledger Systems (DLS). According to Shinde et al. (2023), SMPC facilitates secure collaborative computations while preserving privacy, making it particularly valuable in fraud detection, secure asset custody, and confidential transaction processing. Several case studies highlight its role in strengthening financial security and regulatory compliance (Liu, 2024; Tamilselvi et al., 2024; Alao et al., 2024).

One notable implementation of SMPC was demonstrated in Inpher’s collaboration with the UK's Financial Conduct Authority (FCA) during the Global Anti-Money Laundering (AML) and Financial Crime TechSprint. Inpher (2023) contends that this initiative explored how privacy-enhancing technologies could improve fraud detection and AML compliance by allowing financial institutions to analyze transaction data collaboratively without exposing individual records. This approach facilitated the identification of suspicious activities while ensuring adherence to data protection regulations, reinforcing SMPC’s value in financial crime detection.

Similarly, Parfin has employed SMPC in digital asset custody since 2019. In the view of Parfin (2024), by distributing cryptographic keys across multiple parties, Parfin ensures that no single entity has complete control over stored digital assets, mitigating unauthorized access risks. This implementation underscores SMPC’s effectiveness in enhancing security and regulatory compliance in digital asset management. Another significant development is Microsoft's Confidential Consortium Framework (CCF), which integrates Trusted Execution Environments (TEEs) with blockchain technology. ShubhraS (2022) argues that by creating secure enclaves for transaction processing, CCF ensures data confidentiality even during computation, demonstrating how SMPC can be combined with other privacy-enhancing technologies to strengthen financial DLS security.

The adoption of SMPC in financial applications offers several advantages. Rahaman et al. (2024) posits that one of its primary benefits lies in its ability to support privacy-preserving fraud detection and AML compliance. By allowing institutions to analyze data without exposing individual records, SMPC improves fraud detection accuracy while maintaining compliance with stringent data protection regulations. Moreover, Batan (2024) avers that SMPC facilitates secure data collaboration, enabling financial entities to share intelligence and develop comprehensive risk assessments without compromising client confidentiality.

Despite its benefits, integrating SMPC into DLS presents several challenges. According to Zhou et al. (2024), computational complexity remains a significant concern, as cryptographic operations in SMPC can increase processing times, particularly in high-frequency financial transactions where speed is critical. Scalability is another major issue, as SMPC protocols often require extensive communication between parties, increasing operational overhead in large-scale deployments. Additionally, interoperability with existing financial infrastructures poses challenges, as legacy systems may not seamlessly integrate with SMPC protocols, necessitating modifications or middleware solutions (Ahmed & Alabi, 2024; Joseph, 2024). Furthermore, Khatiwada et al. (2024) contends that widespread adoption requires greater awareness of SMPC’s advantages and extensive stakeholder education regarding its implementation.

Addressing these challenges requires collaboration among technologists, regulators, and industry leaders. Zhou et al. (2024) posits that standardization initiatives, protocol optimizations, and user-friendly implementations are critical to improving the efficiency and scalability of SMPC. As research advances, its integration into financial DLS is expected to become more streamlined, providing institutions with a robust solution for enhancing data privacy while maintaining the transparency and security inherent in DLS (Makhdoom et al., 2024; Kolade et al., 2024; Ajayi et al., 2025).

### **Regulatory and Compliance Considerations**

The integration of Distributed Ledger Systems (DLS) in financial services presents significant regulatory challenges, particularly concerning data privacy and cybersecurity. According to Labadie and Legner (2022), the General Data Protection Regulation (GDPR) of the European Union mandates strict controls over personal data processing, emphasizing principles such as data minimization and the "right to be forgotten." Similarly, SEC (2023) states that in the United States, the Securities and Exchange Commission (SEC) requires financial institutions to disclose material cybersecurity incidents and outline risk management strategies. Furthermore, FSB (2023) contends that the Financial Stability Board (FSB) has issued guidance on regulatory considerations for digital currencies and FinTech, underscoring the necessity of robust data protection, cybersecurity, and financial stability measures. These frameworks collectively aim to safeguard consumer data and enhance the resilience of financial systems.

Despite these regulatory mechanisms, compliance within decentralized financial ecosystems remains particularly challenging. Khan et al. (2019) argues that traditional data protection frameworks are designed for centralized financial systems, whereas DLS operates on a decentralized model with no singular authority. This structural difference complicates data governance, particularly in assigning accountability for regulatory adherence (Janssen et al., 2020; Val et al., 2024). Moreover, Arabsorkhi and Khazaei (2024) posits that the immutability of blockchain records conflicts with GDPR provisions, which grant individuals the right to request data deletion, raising concerns about compliance feasibility. The cross-border nature of DLS transactions further exacerbates these challenges, as regulatory inconsistencies across jurisdictions complicate enforcement and compliance obligations (Rong et al., 2025; Salako et al., 2024).

Secure Multi-Party Computation (SMPC) presents a promising solution to these regulatory challenges by enabling privacy-preserving computations within decentralized systems. Goel (2024) avers that SMPC allows multiple parties to analyze encrypted data without revealing individual records, aligning with GDPR’s principles of data minimization and security. This capability is particularly advantageous in fraud detection, anti-money laundering (AML) initiatives, and secure data sharing among financial institutions. Satheesha (2021) contends that by enabling regulatory-compliant collaboration, SMPC enhances financial organizations' security posture while maintaining the confidentiality of sensitive information. Additionally, Renuka et al. (2024) posits that SMPC supports institutions in meeting SEC cybersecurity mandates by mitigating risks associated with unauthorized data exposure.

Despite its regulatory benefits, integrating SMPC within DLS requires policy adaptations. In the view of Hasani et al. (2023), existing legal frameworks may need revisions to acknowledge the role of privacy-enhancing technologies in compliance strategies. Regulators may also need to clarify liability, data governance, and cross-border data management within SMPC applications. Standardizing SMPC protocols and interoperability frameworks could further streamline compliance and facilitate broader adoption in the financial sector (Prabowo et al., 2025). Achieving these objectives necessitates collaboration among regulators, industry stakeholders, and technology experts to develop standards that balance innovation with regulatory requirements. By addressing these considerations, financial institutions can leverage SMPC to navigate compliance complexities while maintaining data privacy and security within decentralized financial ecosystems (Goel, 2024).

### **3. Methodology**

This study adopts a quantitative approach to assess confidentiality risks, SMPC efficiency, real-world applications, and scalability in financial DLS. Four datasets are used, each analyzed with a specific statistical method.

The Elliptic Bitcoin AML Dataset is utilized to evaluate confidentiality vulnerabilities in financial transactions. Anomaly Detection (Isolation Forest) identifies deviations from normal transaction behavior. The MP-SPDZ Benchmark Dataset is analyzed using One-Way ANOVA to compare computational efficiency among SMPC protocols. The R3 Corda & Hyperledger Fabric Financial Dataset is examined using Logistic Regression to predict privacy-compliant transactions. Finally, Verizon DBIR 2024 Cybersecurity Dataset undergoes Kaplan-Meier Survival Analysis and Cox Proportional Hazards Modeling to assess the scalability and regulatory risks of SMPC adoption. Table 1 below presents the mathematical models applied:

### **Table 1: Mathematical Models**

|  |  |  |
| --- | --- | --- |
| **Objective** | **Statistical Method** | **Mathematical Model** |
| **Confidentiality risks in DLS** | **Anomaly Detection (Isolation Forest)** | $$s\left(x\right)=2-^{\left(\frac{E\left(h\left(x\right)\right)}{c\left(n\right)}\right)}​$$ |
| **Comparison of SMPC protocols** | **One-Way ANOVA** | $$F=\sum\_{i=1}^{k}\frac{\frac{n\_{i}​​\left(X\_{i}​- Xˉ​\right)^{2}}{k-1}}{\sum\_{i=1}^{k}\sum\_{j=1}^{n\_{i}}\frac{\left(X\_{ij }- X\_{i}\right)^{2}}{N-k}}$$ |
| **Real-world SMPC applications** | **Logistic Regression** | $$P\left(X\right)=\frac{e^{\left(β\_{0}​+\sum\_{i=1}^{n}β\_{i}​X\_{i}​​\right)}}{1+e^{\left(β\_{0}​+∑i=1n​β\_{i}​X\_{i} \right)}​}$$ |
| **Scalability & regulatory risks** | **Kaplan-Meier Survival Analysis** | $$S\left(t\right)=\prod\_{​i:t\_{i}​\leq t}^{}\left(1-\frac{d\_{i}​​}{n\_{i}​}\right)$$ |
| **Scalability & regulatory risks** | **Cox Proportional Hazard Model** | $$h\left(t\right)=h\_{0}​\left(t\right)e^{\left(β\_{1}​X\_{1}​+β\_{2}​X\_{2}​+…+β\_{n}​X\_{n}​\right)}$$ |

Each statistical approach ensures a robust, empirical assessment of SMPC in financial DLS, supporting the study’s objectives with quantifiable evidence.

**4. Results and Discussion**

### **Confidentiality Risks in Distributed Ledger Systems: An Analysis Using Anomaly Detection**

The integration of Distributed Ledger Systems (DLS) in financial transactions has enhanced transparency and security. However, the decentralized nature of DLS poses significant confidentiality risks, particularly concerning unauthorized data exposure and financial privacy vulnerabilities. This study examines these risks by identifying anomalous financial transactions within DLS, using statistical analysis and anomaly detection techniques. The findings provide empirical insights into the patterns of financial data breaches and their implications for security frameworks in decentralized systems. The results reveal significant disparities between normal and anomalous transactions in DLS, highlighting areas of potential data vulnerabilities.

##### **Transaction Volume and Frequency Disparities**

Analysis of transaction attributes indicates that anomalous transactions exhibit significantly higher volumes and frequencies compared to normal transactions. The mean transaction volume for anomalous activities was 4,084.99, while that of normal transactions was 937.33, reflecting a 336.1% increase in financial activity for flagged transactions. A similar trend was observed in transaction frequency, where anomalous transactions recorded an average of 11.78 transactions compared to 9.96 for normal activities. The elevated volume and frequency suggest possible illicit financial movements, increasing the risk of unauthorized disclosure of transactional data.

Table 2 presents a summary of the key statistical variations in financial transactions.

##### **Table 2:** Comparative Statistics for Normal and Anomalous Transactions

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Anomaly Label** | **Transaction Volume (Mean)** | **Transaction Frequency (Mean)** | **Counterparties (Mean)** | **Risk Score (Mean)** | **Count** |
| **Anomalous** | 4,084.99 | 11.78 | 22.43 | 0.455 | 4,000 |
| **Normal** | 937.33 | 9.96 | 25.03 | 0.500 | 196,000 |

The variance in counterparties is also a notable concern. While normal transactions maintain a relatively stable counterparties mean of 25.03, anomalous transactions have a lower mean of 22.43. This suggests that suspicious financial transactions tend to involve a limited number of entities, increasing the risk of data correlation attacks that could compromise confidentiality.

##### **Visualization of Anomaly Detection Patterns**

To further illustrate the scale and structure of confidentiality risks, Figure 1 presents a Parallel Coordinates Plot, highlighting the contrast between anomalous and normal transactions across multiple financial parameters.



##### **Figure 1:** *Parallel Coordinates Plot of Transaction Attributes in DLS*

The figure clearly distinguishes anomalous transactions (red lines) from normal transactions (blue lines), with higher transaction values clustering within high-risk regions. This differentiation is essential in detecting confidentiality vulnerabilities and establishing proactive security frameworks for DLS-based financial transactions.

##### **Risk Score and Transaction Structure**

The Risk Score metric, which quantifies the likelihood of a transaction exposing sensitive financial data, was higher in anomalous transactions (0.455) compared to normal transactions (0.500). This indicates that financial transactions flagged as anomalous tend to have a structured pattern, potentially utilizing obfuscation techniques to evade standard detection mechanisms.

To visualize the structural representation of risk exposure, Figure 2 presents a Radial Bar Chart, mapping the variations in financial parameters.



##### **Figure 2:** *Radial Bar Chart Representation of Transaction Risks*

This visual representation further confirms that anomalous transactions consistently exceed normal activity levels across risk parameters, reinforcing the need for enhanced cryptographic privacy techniques in financial DLS environments.

##### **Anomalous Transactions and Confidentiality Exposure**

The study also examined the flow and distribution of transactions to identify points of vulnerability in DLS. Figure 3 presents a Chord Diagram, demonstrating the transactional movement between normal and anomalous financial flows.



##### **Figure 3:** *Chord Diagram Representation of Transaction Flow in DLS*

The diagram depicts financial interactions and interdependencies, illustrating that anomalous transactions tend to cluster, forming distinct transactional loops. This supports existing research suggesting that privacy breaches often originate from clustered financial activities, where attackers exploit data traceability loopholes in decentralized ledgers.

### **Performance Analysis of Secure Multi-Party Computation (SMPC) Protocols in Distributed Ledger Systems**

The effectiveness of Secure Multi-Party Computation (SMPC) in financial Distributed Ledger Systems (DLS) is contingent on its computational efficiency and security guarantees. Given the increasing adoption of privacy-preserving technologies, this study evaluates three SMPC protocols—Shamir’s Secret Sharing, Yao’s Garbled Circuits, and the GMW Protocol—based on execution time, communication overhead, and security assurance. The findings offer critical insights into the trade-offs between efficiency and security, shaping the selection of SMPC protocols for financial applications.

##### **Computational Efficiency of SMPC Protocols**

Execution time is a crucial determinant of protocol viability in financial transactions. Table 3 presents the comparative performance of the three SMPC protocols based on execution time, communication overhead, and security guarantees.

##### **Table 3:** Statistical Performance Summary of SMPC Protocols

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Protocol | Execution Time (Mean, ms) | Execution Time (Std, ms) | Communication Overhead (Mean, KB) | Communication Overhead (Std, KB) | Security Guarantees (High Probability) |
| Shamir’s Secret Sharing | 247.10 | 17.90 | 119.73 | 9.95 | 0.73 |
| Yao’s Garbled Circuits | 180.50 | 15.16 | 91.24 | 7.83 | 0.42 |
| GMW Protocol | 222.55 | 17.06 | 104.32 | 9.42 | 0.67 |

The results indicate that Yao’s Garbled Circuits is the fastest protocol, with a mean execution time of 180.50 ms, outperforming both Shamir’s Secret Sharing (247.10 ms) and GMW (222.55 ms). However, Shamir’s Secret Sharing provides the highest security guarantees (0.73 probability of achieving high security levels), making it the most secure option despite its higher computational cost.

To further illustrate the execution time distribution across protocols, Figure 4 provides a Violin Plot, highlighting the spread of execution times within each protocol.



##### **Figure 4:** *Violin Plot of Execution Time for SMPC Protocols*

The plot confirms that Yao’s Garbled Circuits maintains a tighter execution time range, while Shamir’s Secret Sharing exhibits greater variability, reinforcing its higher computational demand.

##### **Communication Overhead and Security Implications**

The efficiency of SMPC protocols is also determined by communication overhead, which affects transaction scalability in financial DLS applications. Shamir’s Secret Sharing incurs the highest communication overhead (119.73 KB), followed by GMW (104.32 KB) and Yao’s Garbled Circuits (91.24 KB).

A comprehensive comparison of execution time, communication overhead, and security guarantees is presented in Figure 5, using a Heatmap to visualize performance differences across protocols.



##### **Figure 5:** *Heatmap Representation of SMPC Protocol Performance*

This visualization confirms that while Yao’s Garbled Circuits minimizes both execution time and communication costs, it lags in security guarantees, which may be a limiting factor for applications requiring strict confidentiality. In contrast, Shamir’s Secret Sharing offers superior security assurance but at the cost of increased computational and communication overhead.

### **Real-World Applications of Secure Multi-Party Computation (SMPC) in Financial Distributed Ledger Systems**

The adoption of Secure Multi-Party Computation (SMPC) in financial Distributed Ledger Systems (DLS) aims to enhance data confidentiality and security in transactional environments. As financial institutions integrate privacy-preserving computation models, understanding the efficacy of SMPC protocols in securing financial transactions becomes essential. This study evaluates the impact of different SMPC implementations on transaction security success rates, execution time, and cryptographic efficiency, providing empirical insights into real-world applications of SMPC in financial DLS.

#####  **Performance of SMPC-Based Secure Transactions**

The effectiveness of SMPC in financial DLS depends on its ability to ensure transaction security while maintaining computational efficiency. Table 4 presents an overview of the performance of different SMPC protocols, focusing on transaction security success rates, execution time, and cryptographic methods.

##### **Table 4:** Statistical Analysis of SMPC Transaction Security Performance

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Protocol Type | Avg. Number of Participants | Avg. Cryptographic Method | Execution Time (Mean, ms) | Execution Time (Std, ms) | Transaction Success Rate (%) |
| Shamir’s Secret Sharing | 25.63 | 2.02 | 202.56 | 48.53 | 70.63 |
| Yao’s Garbled Circuits | 26.25 | 2.00 | 201.24 | 50.84 | 70.55 |
| GMW Protocol | 25.16 | 2.01 | 201.80 | 49.76 | 71.50 |

The results indicate that all three SMPC protocols achieve over 70% success in securing financial transactions, confirming the viability of SMPC-based privacy preservation. The GMW Protocol exhibits the highest security success rate (71.50%), outperforming both Shamir’s Secret Sharing (70.63%) and Yao’s Garbled Circuits (70.55%).

To further illustrate the relationship between execution time and transaction security success rate, Figure 6 presents a Bubble Chart, where bubble sizes represent the number of participants in each protocol.



##### **Figure 6:** *Bubble Chart Depicting Execution Time vs. Success Rate of Secure Transactions*

The visualization highlights that despite slight variations in execution time, the security success rate remains relatively stable across protocols. However, GMW Protocol's slight edge in security success rate suggests that it may be better optimized for handling secure computations in real-world financial settings.

##### **Distribution of Execution Time Across SMPC Protocols**

Execution time is a critical determinant in the scalability of SMPC implementations in financial DLS. To analyze the distribution of execution time across different SMPC protocols, Figure 7 presents a Hexbin Chart, which visualizes transaction density at various execution time intervals.



##### **Figure 7:** *Hexbin Chart Illustrating Execution Time Distribution Across SMPC Protocols*

The chart confirms that execution time remains concentrated within a stable range (approximately 200-205 ms) across all protocols, reinforcing the feasibility of SMPC integration in financial DLS without excessive computational delays. The density of transactions remains higher for execution times under 210 ms, suggesting that most privacy-preserving transactions achieve security without substantial processing overhead.

### **Scalability, Computational Efficiency, and Regulatory Compliance of SMPC in Financial Distributed Ledger Systems**

The adoption of Secure Multi-Party Computation (SMPC) in financial Distributed Ledger Systems (DLS) has raised critical questions regarding its scalability, computational efficiency, and regulatory compliance. As financial institutions transition towards privacy-preserving cryptographic methods, it is necessary to evaluate whether SMPC-based systems sustain long-term operational resilience while reducing cybersecurity risks and regulatory penalties. This study examines the survival probability of financial systems employing SMPC versus those relying on traditional encryption methods, providing empirical insights into their long-term viability.

##### **Survival Time and Failure Rate of SMPC vs. Traditional Encryption**

The study assesses the mean survival time and failure occurrences of financial systems operating under SMPC encryption compared to traditional encryption techniques. Table 5 presents an overview of the comparative longevity and failure statistics of both encryption models.

##### **Table 5:** Survival Time and Failure Rate of Financial Systems Based on Encryption Type

|  |  |  |  |
| --- | --- | --- | --- |
| Encryption Type | Mean Survival Time (Months) | Survival Std (Months) | Total Failures |
| SMPC | 36.11 | 35.48 | 209 |
| Traditional | 21.91 | 21.29 | 297 |

The results indicate that financial systems utilizing SMPC sustain operations for a significantly longer period (36.11 months) compared to those relying on traditional encryption (21.91 months). Additionally, the total failure rate in SMPC-based systems (209 failures) is considerably lower than that of traditional encryption systems (297 failures), demonstrating enhanced security resilience and regulatory compliance through SMPC adoption.

To further illustrate the probability of system failure over time, Figure 8 presents a Step Plot, depicting the cumulative failure rate of financial systems under both encryption models.



##### **Figure 8:** *Step Plot Depicting Cumulative Probability of System Failure Over Time*

The figure shows that SMPC-based financial systems experience a more gradual failure trajectory, confirming that SMPC enhances system longevity by reducing the likelihood of security breaches and non-compliance penalties over time.

##### **Comparative Analysis of Mean Survival Time**

To provide a more intuitive comparison of survival times between encryption methods, Figure 9 presents a Dumbbell Chart, demonstrating the difference in mean survival time between SMPC and traditional encryption.



##### **Figure 9:** *Dumbbell Chart Comparing Mean Survival Time of Financial Systems Under Different Encryption Methods*

The visualization confirms that SMPC extends system survivability, ensuring prolonged security efficiency and regulatory adherence in financial DLS environments. The substantial disparity in survival times reinforces the importance of integrating SMPC for long-term scalability and compliance stabil**ity**.

**Discussion**

The findings of this study highlight the confidentiality risks associated with Distributed Ledger Systems (DLS) and demonstrate how Secure Multi-Party Computation (SMPC) enhances security and regulatory compliance in financial applications. The confidentiality vulnerabilities inherent in DLS are evident in the transaction patterns identified through anomaly detection, revealing that anomalous transactions tend to exhibit significantly higher volumes and frequencies compared to normal transactions. The increased financial activity among flagged transactions suggests the possibility of illicit financial movements, which aligns with the concerns raised by Prakash and Garg (2024) regarding adversaries exploiting transparency loopholes in decentralized architectures. Furthermore, the lower mean number of counterparties in anomalous transactions reinforces the inference attack risks described by Agrawal et al. (2024), where attackers correlate transaction data to reconstruct sensitive financial information. The clustering of anomalous financial interactions, as illustrated in the chord diagram, suggests that illicit activities may be organized within tightly connected network loops, supporting the notion that confidentiality breaches often emerge from interdependent transactional structures (Sarfaraz et al., 2023).

The evaluation of SMPC protocols provides further insights into the efficiency-security trade-offs within privacy-preserving financial computations. The results establish that Yao’s Garbled Circuits offers the lowest execution time, making it the most computationally efficient protocol. However, the reduced execution cost comes at the expense of security, with Shamir’s Secret Sharing providing the highest probability of achieving strong security guarantees despite its higher computational burden. These findings reinforce the computational challenges discussed by Gamiz et al. (2024), who note that SMPC protocols often impose substantial overhead due to their cryptographic complexity. The heatmap representation of protocol performance further emphasizes that optimizing security often necessitates a trade-off with computational efficiency, a factor that financial institutions must consider when selecting an SMPC protocol. The performance variations across protocols underscore the argument by Rahaman et al. (2024) that different SMPC techniques must be evaluated within the specific computational constraints of financial institutions to ensure a balance between security and scalability.

Examining real-world applications of SMPC within financial DLS environments further validates its feasibility in securing financial transactions. The success rates of privacy-preserving transactions, which exceed 70% across all SMPC protocols, confirm that SMPC is a viable approach for protecting sensitive financial data. The slight advantage of the GMW protocol in transaction security success rates suggests that its specific cryptographic properties may offer enhanced confidentiality protections in multi-party financial environments. This aligns with the insights provided by Almusawi et al. (2023), who discuss how the GMW protocol leverages secret sharing and oblivious transfer mechanisms to ensure secure collaborative computations. The bubble chart representation of execution time versus transaction success rate indicates that, despite slight variations in execution efficiency, SMPC protocols consistently maintain a high level of security, which strengthens the argument made by Batan (2024) that SMPC enables precise computations without exposing raw financial data. The hexbin chart further confirms that execution times remain stable across all protocols, demonstrating that SMPC implementations do not introduce significant delays in financial DLS operations, an essential consideration for transaction-heavy financial ecosystems as outlined by Allaart et al. (2024).

The survival analysis of financial systems adopting SMPC compared to those utilizing traditional encryption methods provides critical insights into the long-term scalability and regulatory compliance implications of SMPC integration. The mean survival time for SMPC-based financial systems is significantly higher than that of traditional encryption systems, reinforcing the findings of Hasani et al. (2023), who argue that privacy-preserving cryptographic techniques contribute to long-term financial system resilience. The step plot depicting cumulative failure probability further substantiates the claim by Renuka et al. (2024) that SMPC mitigates security risks by reducing the likelihood of data breaches over time. The lower failure rate among SMPC-based systems demonstrates that privacy-enhancing techniques improve financial infrastructure stability and support regulatory adherence, reinforcing the argument by Gounari et al. (2024) that financial institutions must align with evolving data protection mandates. The dumbbell chart comparison of mean survival time highlights the tangible benefits of SMPC adoption, confirming that its implementation extends the operational longevity of financial systems. These findings are consistent with the observations of Goel (2024), who notes that SMPC enables regulatory-compliant data processing by ensuring that transactional confidentiality is preserved even in decentralized environments.

These findings provide empirical validation for the integration of SMPC in financial DLS implementations, reinforcing its role in addressing confidentiality risks, optimizing privacy-preserving computations, and ensuring long-term financial system resilience. While SMPC enhances data security, the computational costs and interoperability challenges identified in this study align with the concerns raised by Zhou et al. (2024), emphasizing the need for ongoing optimization of SMPC frameworks to facilitate broader adoption. The comparative evaluation of SMPC protocols, real-world transaction security performance, and regulatory implications offers a comprehensive perspective on its feasibility, underscoring the necessity of balancing security, efficiency, and compliance considerations in privacy-preserving financial applications.

**5. Conclusion and Recommendation**

The study establishes that Secure Multi-Party Computation (SMPC) enhances confidentiality in Distributed Ledger Systems (DLS) by mitigating unauthorized data exposure while maintaining computational efficiency and regulatory compliance. Anomaly detection reveals that illicit transactions exhibit distinct patterns that increase financial privacy vulnerabilities, reinforcing the need for cryptographic protections. Comparative analysis of SMPC protocols confirms that security and efficiency trade-offs must be balanced, with the GMW protocol demonstrating a slight edge in transaction security. Survival analysis further validates that SMPC adoption extends system longevity and minimizes cybersecurity risks compared to traditional encryption. Hence, the study suggests that:

1. Financial institutions should integrate SMPC protocols that balance execution efficiency and security, prioritizing models with lower communication overhead to enhance scalability.
2. Regulators must develop standardized SMPC frameworks to ensure interoperability and compliance across decentralized financial ecosystems.
3. Future research should optimize SMPC algorithms to reduce computational costs, improving adoption feasibility for high-frequency financial transactions.
4. Enhanced anomaly detection mechanisms should be implemented within DLS to proactively identify illicit financial activities and strengthen confidentiality measures.

# **References**

Agrawal, R., Singhal, S., & Sharma, A. (2024). Blockchain and fog computing model for secure data access control mechanisms for distributed data storage and authentication using hybrid encryption algorithm. *Cluster Computing*, *27*. <https://doi.org/10.1007/s10586-024-04411-9>

Ahmed, A. A., & Alabi, O. O. (2024). Secure and Scalable Blockchain-Based Federated Learning for Cryptocurrency Fraud Detection: A Systematic Review. *IEEE Access*, *12*, 102219–102241. <https://doi.org/10.1109/access.2024.3429205>

Ajayi, A. J., Joseph, S. A., Metibemu, O. C., Olutimehin, A. T., Balogun, A. Y., & Olaniyi, O. O. (2025). The Impact of Artificial Intelligence on Cyber Security in Digital Currency Transactions. *Archives of Current Research International*, *25*(2), 329–351. <https://doi.org/10.9734/acri/2025/v25i21090>

Alam, I., Alali, A. S., Ali, S., & Asri, M. S. M. (2024). A Verifiable Multi-Secret Sharing Scheme for Hierarchical Access Structure. *Axioms*, *13*(8), 515. <https://doi.org/10.3390/axioms13080515>

Alao, A. I., Adebiyi, O. O., & Olaniyi, O. O. (2024). The Interconnectedness of Earnings Management, Corporate Governance Failures, and Global Economic Stability: A Critical Examination of the Impact of Earnings Manipulation on Financial Crises and Investor Trust in Global Markets. *Asian Journal of Economics Business and Accounting*, *24*(11), 47–73. <https://doi.org/10.9734/ajeba/2024/v24i111542>

Ali, S., Wadho, S. A., Yichiet, A., Gan, M. L., & Lee, C. K. (2024). Advancing cloud security: Unveiling the protective potential of homomorphic secret sharing in secure cloud computing. *Egyptian Informatics Journal*, *27*, 100519–100519. <https://doi.org/10.1016/j.eij.2024.100519>

Allaart, C., Amiri, S., Bal, H., Belloum, A., Gommans, L., Halteren, A. van, & Klous, S. (2024). Private and Secure Distributed Deep Learning: A Survey. *ACM Computing Surveys*, *57*(4). <https://doi.org/10.1145/3703452>

Almusawi, M., Singh, A. P., Bisht, Y. S., Selvan, K. S., Jansirani, D., Esanmurodova, N., & Dev, V. (2023). Cryptography-Based Privacy-Preserving Data Analysis and Empowering Data Privacy through Secure Multi-Party Computation: Challenges and Solutions. *IEEE*. <https://doi.org/10.1109/icteasd57136.2023.10584998>

Antal, C., Cioara, T., Anghel, I., Antal, M., & Salomie, I. (2021). Distributed Ledger Technology Review and Decentralized Applications Development Guidelines. *Future Internet*, *13*(3), 62. <https://doi.org/10.3390/fi13030062>

Arabsorkhi, A., & Khazaei, E. (2024). Blockchain Technology and GDPR Compliance: A Comprehensive Applicability Model. *International Journal of Web Research*, *7*(2), 49–63. <https://doi.org/10.22133/ijwr.2024.459490.1221>

Ataullah, Md., & Chauhan, N. (2024). Exploring security and privacy enhancement technologies in the Internet of Things: A comprehensive review. *Security and Privacy*, *7*(6). <https://doi.org/10.1002/spy2.448>

Balogun, A. Y. (2025). Strengthening Compliance with Data Privacy Regulations in U.S. Healthcare Cybersecurity. *Asian Journal of Research in Computer Science*, *18*(1), 154–173. <https://doi.org/10.9734/ajrcos/2025/v18i1555>

Balogun, A. Y., Metibemu, O. C., Olutimehin, A. T., Ajayi, A. J., Babarinde, D. C., & Olaniyi, O. O. (2025). The Ethical and Legal Implications of Shadow AI in Sensitive Industries: A Focus on Healthcare, Finance and Education. *Journal of Engineering Research and Reports*, *27*(3), 1–22. <https://doi.org/10.9734/jerr/2025/v27i31414>

Balogun, A. Y., Olaniyi, O. O., Olisa, A. O., Gbadebo, M. O., & Chinye, N. C. (2025). Enhancing Incident Response Strategies in U.S. Healthcare Cybersecurity. *Journal of Engineering Research and Reports*, *27*(2), 114–135. <https://doi.org/10.9734/jerr/2025/v27i21399>

Batan, A. (2024). Designing Privacy-Preserving Mechanisms for Secure Communication in Modern Cloud Environments. *International Journal of Cybersecurity Risk Management, Forensics, and Compliance*, *8*(12), 1–11. <http://hashsci.com/index.php/IJCRFC/article/view/1>

Bautista, O. G., Akkaya, K., & Homsi, S. (2023). ReplayMPC: A Fast Failure Recovery Protocol for Secure Multiparty Computation Applications using Blockchain. *IEEE* . <https://doi.org/10.1109/smartcomp58114.2023.00033>

Bellaj, B., Ouaddah, A., Bertin, E., Crespi, N., & Mezrioui, A. (2024). Drawing the Boundaries Between Blockchain and Blockchain-Like Systems: A Comprehensive Survey on Distributed Ledger Technologies. *Proceedings of the IEEE*, *112*(3), 247–299. <https://doi.org/10.1109/jproc.2024.3386257>

Chainlink. (2024). *Secure Multi-Party Computation - Chainlink*. Chain.link. <https://chain.link/education-hub/secure-multiparty-computation-mcp>

Chi, P.-W., Lu, Y.-H., & Guan, A. (2023). A Privacy-Preserving Zero-Knowledge Proof for Blockchain. *IEEE Access*, *11*, 85108–85117. <https://doi.org/10.1109/ACCESS.2023.3302691>

Daah, C., Qureshi, A., Awan, I., & Konur, S. (2024). Enhancing Zero Trust Models in the Financial Industry through Blockchain Integration: A Proposed Framework. *Electronics*, *13*(5), 865. <https://doi.org/10.3390/electronics13050865>

de la Roche, M., Voloder, E., Banerjee, A., Guerra, C., Dell’Accio, D. C., Budris, F., Arantes Jr, G. M., Khattak, J., Wu, K.-T., Kajtazi, L., Giudici, P., Tonutti, S., Gürpinar, T., & Sedej, T. (2025). Report on Artificial Intelligence and Blockchain Convergences. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.5023415>

Dong, S., Abbas, K., Li, M. Y., & Kamruzzaman, J. (2023). Blockchain technology and application: an overview. *PeerJ*, *9*(1), e1705–e1705. <https://doi.org/10.7717/peerj-cs.1705>

European Central Bank. (2024). *ECB concludes cyber resilience stress test*. European Central Bank - Banking Supervision. <https://www.bankingsupervision.europa.eu/press/pr/date/2024/html/ssm.pr240726~06d5776a02.en.html>

FSB. (2023). *High-level Recommendations for the Regulation, Supervision and Oversight of Crypto-asset Activities and Markets: Final report*. Www.fsb.org. <https://www.fsb.org/2023/07/high-level-recommendations-for-the-regulation-supervision-and-oversight-of-crypto-asset-activities-and-markets-final-report/>

Gamiz, I., Regueiro, C., Lage, O., Jacob, E., & Astorga, J. (2024). Challenges and future research directions in secure multi-party computation for resource-constrained devices and large-scale computations. *International Journal of Information Security*, *24*(1). <https://doi.org/10.1007/s10207-024-00939-4>

Goel, P. K. (2024). Privacy-Preserving Data Storage and Processing in the Cloud. *Advances in Computer and Electrical Engineering Book Series*, 149–178. <https://doi.org/10.4018/979-8-3693-2869-9.ch009>

Gounari, M., Stergiopoulos, G., Pipyros, K., & Gritzalis, D. (2024). Harmonizing open banking in the European Union: an analysis of PSD2 compliance and interrelation with cybersecurity frameworks and standards. *International Cybersecurity Law Review*, *5*. <https://doi.org/10.1365/s43439-023-00108-8>

Gregorian, A. (2019). *Hacking and malware behind 75% of all data breaches in the financial services industry*. IT Security Guru. <https://www.itsecurityguru.org/2019/12/17/hacking-and-malware-behind-75-of-all-data-breaches-in-the-financial-services-industry/>

Hamza, R., Hassan, A., Ali, A., Bashir, M. B., Alqhtani, S. M., Tawfeeg, T. M., & Yousif, A. (2022). Towards Secure Big Data Analysis via Fully Homomorphic Encryption Algorithms. *Entropy*, *24*(4), 519. <https://doi.org/10.3390/e24040519>

Hasani, T., Rezania, D., Levallet, N., O’Reilly, N., & Mohammadi, M. (2023). Privacy enhancing technology adoption and its impact on SMEs’ performance. *International Journal of Engineering Business Management*, *15*, 184797902311728-184797902311728. <https://doi.org/10.1177/18479790231172874>

Inpher. (2023). *Financial Services*. Inpher. <https://inpher.io/solutions/by-industry/financial-services/>

Janghyun, K., Barry, H., Tianzhen, H., & Marc A., P. (2022). A review of preserving privacy in data collected from buildings with differential privacy. *Journal of Building Engineering*, *56*, 104724. <https://doi.org/10.1016/j.jobe.2022.104724>

Janssen, M., Brous, P., Estevez, E., Barbosa, L. S., & Janowski, T. (2020). Data governance: Organizing data for trustworthy Artificial Intelligence. *Government Information Quarterly*, *37*(3), 101493. <https://doi.org/10.1016/j.giq.2020.101493>

Jimmy, F. (2024). Enhancing Data Security in Financial Institutions with Blockchain Technology. *Deleted Journal*, *5*(1), 424–437. <https://doi.org/10.60087/jaigs.v5i1.217>

Joseph, S. A. (2024). Balancing Data Privacy and Compliance in Blockchain-Based Financial Systems. *Journal of Engineering Research and Reports*, *26*(9), 169–189. <https://doi.org/10.9734/jerr/2024/v26i91271>

Kapko, M. (2024). *New York fines Geico, Travelers $11.3M for pandemic-era breaches*. Cybersecurity Dive. <https://www.cybersecuritydive.com/news/new-york-fines-geico-travelers/734045/>

Khan, M. Y., Zuhairi, M. F., Ali, T., Alghamdi, T., & Marmolejo-Saucedo, J. A. (2019). An extended access control model for permissioned blockchain frameworks. *Wireless Networks*, *26*. <https://doi.org/10.1007/s11276-019-01968-x>

Khatiwada, P., Yang, B., Lin, J.-C., & Blobel, B. (2024). Patient-Generated Health Data (PGHD): Understanding, Requirements, Challenges, and Existing Techniques for Data Security and Privacy. *Journal of Personalized Medicine*, *14*(3), 282–282. <https://doi.org/10.3390/jpm14030282>

Kolade, T. M., Aideyan, N. T., Oyekunle, S. M., Ogungbemi, O. S., & Olaniyi, O. O. (2024). Artificial Intelligence and Information Governance: Strengthening Global Security, through Compliance Frameworks, and Data Security. *Asian Journal of Research in Computer Science*, *17*(12), 36–57. <https://doi.org/10.9734/ajrcos/2024/v17i12528>

Kolade, T. M., Obioha-Val, O. A., Balogun, A. Y., Gbadebo, M. O., & Olaniyi, O. O. (2025). AI-Driven Open Source Intelligence in Cyber Defense: A Double-edged Sword for National Security. *Asian Journal of Research in Computer Science*, *18*(1), 133–153. <https://doi.org/10.9734/ajrcos/2025/v18i1554>

Kumar, A., Sekhar Dey, N., Chennakeshwar, B., & Anuvamshitha, C. (2024). Quantum-Enhanced Secure Multi-party Computation for Cyber Security Applications. *Communications in Computer and Information Science*, *2234*, 127–145. <https://doi.org/10.1007/978-3-031-74682-6_9>

Labadie, C., & Legner, C. (2022). Building data management capabilities to address data protection regulations: Learning from EU-GDPR. *Journal of Information Technology*, *38*(1), 16–44. <https://doi.org/10.1177/02683962221141456>

Liu, T. (2024). Research on Privacy Techniques Based on Multi-Party Secure Computation. *2024 3rd International Conference on Artificial Intelligence and Autonomous Robot Systems (AIARS)*, 912–917. <https://doi.org/10.1109/aiars63200.2024.00171>

Makhdoom, I., Abolhasan, M., Lipman, J., Shariati, N., Franklin, D., & Piccardi, M. (2024). Securing Personally Identifiable Information: A Survey of SOTA Techniques, and a Way Forward. *IEEE Access*, *12*, 116740–116770. <https://doi.org/10.1109/access.2024.3447017>

Mayeke, N. R., Arigbabu, A. T., Olaniyi, O. O., Okunleye, O. J., & Adigwe, C. S. (2024). Evolving Access Control Paradigms: A Comprehensive Multi-Dimensional Analysis of Security Risks and System Assurance in Cyber Engineering. *Asian Journal of Research in Computer Science*, *17*(5), 108–124. <https://doi.org/10.9734/ajrcos/2024/v17i5442>

Muñoz, A., Ríos, R., Román, R., & López, J. (2023). A survey on the (in)security of trusted execution environments. *Computers & Security*, *129*, 103180. <https://doi.org/10.1016/j.cose.2023.103180>

Mustafa, G., Rafiq, W., Jhamat, N., Arshad, Z., & Rana, F. A. (2024). Blockchain-based governance models in e-government: a comprehensive framework for legal, technical, ethical and security considerations. *International Journal of Law and Management*, *67*(1). <https://doi.org/10.1108/ijlma-08-2023-0172>

Nookala, G. (2023). Secure Multiparty Computation (SMC) for Privacy-Preserving Data Analysis. *Journal of Big Data and Smart Systems*, *4*(1). <https://universe-publisher.com/index.php/jbds/article/view/15>

Obioha-Val, O. A. (2025). Bridging Gaps in Cybersecurity Governance: Leveraging Collaborative Digital Solutions. *Asian Journal of Research in Computer Science*, *18*(2), 82–100. <https://doi.org/10.9734/ajrcos/2025/v18i2564>

Obioha-Val, O. A., Gbadebo, M. O., Olaniyi, O. O., Chinye, N. C., & Balogun, A. Y. (2025). Innovative Regulation of Open Source Intelligence and Deepfakes AI in Managing Public Trust. *Journal of Engineering Research and Reports*, *27*(2), 136–156. <https://doi.org/10.9734/jerr/2025/v27i21400>

Obioha-Val, O. A., Lawal, T. I., Olaniyi, O. O., Gbadebo, M. O., & Olisa, A. O. (2025). Investigating the Feasibility and Risks of Leveraging Artificial Intelligence and Open Source Intelligence to Manage Predictive Cyber Threat Models. *Journal of Engineering Research and Reports*, *27*(2), 10–28. <https://doi.org/10.9734/jerr/2025/v27i21390>

Obioha-Val, O. A., Olaniyi, O. O., Gbadebo, M. O., Balogun, A. Y., & Olisa, A. O. (2025). Cyber Espionage in the Age of Artificial Intelligence: A Comparative Study of State-Sponsored Campaign. *Asian Journal of Research in Computer Science*, *18*(1), 184–204. <https://doi.org/10.9734/ajrcos/2025/v18i1557>

Ojha, N. K., & Thakur, S. (2025). Privacy Laws and Leak of Financial Data in the Era of Generative AI. *Wiley Online Library*, 265–281. <https://doi.org/10.1002/9781394271078.ch14>

Olutimehin, A. T. (2025a). Advancing Cloud Security in Digital Finance: AI-Driven Threat Detection, Cryptographic Solutions, and Privacy Challenges. *Journal of Engineering Research and Reports*, *27*(3), 35–55. <https://doi.org/10.9734/jerr/2025/v27i31416>

Olutimehin, A. T. (2025b). Assessing the Effectiveness of Cybersecurity Frameworks in Mitigating Cyberattacks in the Banking Sector and its Applicability to Decentralized Finance (DeFi). *Asian Journal of Research in Computer Science*, *18*(3), 130–151. <https://doi.org/10.9734/ajrcos/2025/v18i3583>

Olutimehin, A. T. (2025c). The Synergistic Role of Machine Learning, Deep Learning, and Reinforcement Learning in Strengthening Cyber Security Measures for Crypto Currency Platforms. *Asian Journal of Research in Computer Science*, *18*(3), 190–212. <https://doi.org/10.9734/ajrcos/2025/v18i3586>

Olutimehin, A. T., Ajayi, A. J., Metibemu, O. C., Balogun, A. Y., Oladoyinbo, T. O., & Olaniyi, O. O. (2025). Adversarial Threats to AI-Driven Systems: Exploring the Attack Surface of Machine Learning Models and Countermeasures. *Journal of Engineering Research and Reports*, *27*(2), 341–362. <https://doi.org/10.9734/jerr/2025/v27i21413>

Parfin. (2024). *Custody | Parfin.io*. Custody | Parfin.io. <https://parfin.io/en/platform/custody/>

Petrosyan, A. (2024). *Average total cost of a data breach in financial industry worldwide from 2019 to 2024*. Statista. <https://www.statista.com/statistics/1324063/cost-of-data-breaches-in-financial-industry-worldwide/>

Prabowo, S., Putrada, A. G., Oktaviani, I. D., Abdurohman, M., Janssen, M., Nuha, H. H., & Sutikno, S. (2025). Privacy-Preserving Tools and Technologies: Government Adoption and Challenges. *IEEE Access*, 1–1. <https://doi.org/10.1109/access.2025.3540878>

Prakash, D., & Garg, S. (2024). Alarming Concerns Around Cyber Security in The Securities Market . *SSRN* . <https://doi.org/10.2139/ssrn.4907612>

Rahaman, M., Arya, V., Orozco, S. M., & Pappachan, P. (2024). Secure Multi-Party Computation (SMPC) Protocols and Privacy. *Advances in Information Security, Privacy, and Ethics*, 190–214. <https://doi.org/10.4018/979-8-3693-5330-1.ch008>

Renuka, O., RadhaKrishnan, N., Priya, B. S., Jhansy, A., & Ezekiel, S. (2024). Data Privacy and Protection. *Wiley Online Library*, 433–465. <https://doi.org/10.1002/9781394230600.ch19>

Rong, K., Ling, Y., Yang, T., & Huang, C. (2025). Cross-border data transfer: patterns and discrepancies. *Journal of International Business Policy*. <https://doi.org/10.1057/s42214-025-00209-7>

Salako, A. O., Fabuyi, J. A., Aideyan, N. T., Selesi-Aina, O., Dapo-Oyewole, D. L., & Olaniyi, O. O. (2024). Advancing Information Governance in AI-Driven Cloud Ecosystem: Strategies for Enhancing Data Security and Meeting Regulatory Compliance. *Asian Journal of Research in Computer Science*, *17*(12), 66–88. <https://doi.org/10.9734/ajrcos/2024/v17i12530>

Sarfaraz, A., Chakrabortty, R. K., & Essam, D. (2023). AccessChain: An access control framework to protect data access in blockchain enabled supply chain. *Future Generation Computer Systems*, *148*, 380–394. <https://doi.org/10.1016/j.future.2023.06.009>

Satheesha, S. (2021). *Evaluating Privacy Technologies in Blockchains for Financial Systems*. DIVA. <https://www.diva-portal.org/smash/record.jsf?pid=diva2:1617612>

Schappert, S. (2024). *LoanDepot finally reveals what data was exposed in Jan hack | Cybernews*. Cybernews. <https://cybernews.com/news/loandepot-finally-reveals-what-data-exposed-in-jan-hack/>

SEC. (2023a). *10-K*. Sec.gov. <https://www.sec.gov/Archives/edgar/data/1503802/000095017025022765/kpti-20241231.htm>

SEC. (2023b). *SEC.gov | SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies*. Www.sec.gov. <https://www.sec.gov/newsroom/press-releases/2023-139>

Shinde, N. K., Seth, A., & Kadam, P. (2023). Exploring the Synergies: A Comprehensive Survey of Blockchain Integration with Artificial Intelligence, Machine Learning, and IoT for Diverse Applications. *Springer*, 85–119. <https://doi.org/10.1007/978-981-99-7456-6_7>

Shirali, M., Tefke, T., Staudemeyer, R. C., & Pohls, H. C. (2023). A Survey on Anonymous Communication Systems With a Focus on Dining Cryptographers Networks. *IEEE Access*, *11*, 18631–18659. <https://doi.org/10.1109/access.2023.3242870>

ShubhraS. (2022). *Microsoft introduces preview of Azure Managed Confidential Consortium Framework*. TECHCOMMUNITY.MICROSOFT.COM. <https://techcommunity.microsoft.com/blog/azureconfidentialcomputingblog/microsoft-introduces-preview-of-azure-managed-confidential-consortium-framework/3648986>

Tamilselvi, P., Lathika, V., Jayachitra, S., Arunkumar, S., Balasubramani, M., & Kalaichelvi, V. (2024). Secure Multi-Party Computation for Collaborative Data Analysis in Network Security. *IEEE*, 1–5. <https://doi.org/10.1109/iitcee59897.2024.10467913>

Uberoi, A. (2024). *Understanding the Evolve Bank Cyber Attack: A Timeline*. Cm-Alliance.com. <https://www.cm-alliance.com/cybersecurity-blog/understanding-the-evolve-bank-cyber-attack-a-timeline>

Val, O. O., Kolade, T. M., Gbadebo, M. O., Selesi-Aina, O., Olateju, O. O., & Olaniyi, O. O. (2024). Strengthening Cybersecurity Measures for the Defense of Critical Infrastructure in the United States. *Asian Journal of Research in Computer Science*, *17*(11), 25–45. <https://doi.org/10.9734/ajrcos/2024/v17i11517>

van Zeeland, I., & Pierson, J. (2024). Changing the whole game: effects of the COVID-19 pandemic’s accelerated digitalization on European bank staff’s data protection capabilities. *Financial Innovation*, *10*(29). <https://doi.org/10.1186/s40854-023-00533-y>

Wylde, V., Rawindaran, N., Lawrence, J., Balasubramanian, R., Prakash, E., Jayal, A., Khan, I., Hewage, C., & Platts, J. (2022). Cybersecurity, Data Privacy and Blockchain: A Review. *SN Computer Science*, *3*(2). <https://link.springer.com/article/10.1007/s42979-022-01020-4>

Xu, R., & Joshi, J. (2020). Revisiting Secure Computation Using Functional Encryption: Opportunities and Research Directions. *2020 Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, 226–235. <https://doi.org/10.1109/tps-isa50397.2020.00038>

Zhang, C., Xie, Y., Bai, H., Yu, B., Li, W., & Gao, Y. (2021). A survey on federated learning. *Knowledge-Based Systems*, *216*, 106775. <https://doi.org/10.1016/j.knosys.2021.106775>

Zhou, L., Diro, A., Saini, A., Kaisar, S., & Hiep, P. C. (2024). Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities. *Journal of Information Security and Applications*, *80*, 103678–103678. <https://doi.org/10.1016/j.jisa.2023.103678>