Frontiers in Computing and Intelligent Systems
ISSN: 2832-6024 | Vol. 17, No. 1, 2026

The Third-Generation Cross-Institutional Encrypted Collaboration: A Review of MPC-TEE Fusion in Medical Privacy AI

Chenyu Liu *

College of Mathematics and Information Science, Zhangjiakou University, Zhangjiakou, Hebei, 075000, China
*** Corresponding author Email:** liuchenyu070748@outlook.com

Abstract: With the increasingly stringent global data protection regulations and the growing demand for cross-institutional collaboration, traditional privacy computing technologies can hardly meet the requirements for efficient, secure and scalable collaboration. The third-generation cross-institutional encryption technology takes the fusion of Secure Multi-Party Computation (MPC) and Trusted Execution Environment (TEE) as the core, and better balances security and performance through the collaborative design of software and hardware. In the fields of healthcare, financial services, the Internet of Things and others, MPC-TEE fusion technology can realize efficient collaboration while ensuring data privacy, further promoting the industrialization of privacy AI. However, this technology still faces challenges such as side-channel attacks, insufficient standardization and high costs. This paper systematically reviews the latest research progress of MPC-TEE fusion technology, deeply analyzes its technical foundation, fusion principles and core architecture design, compares and analyzes the application performance and scenario adaptability of mainstream technical frameworks in the medical field, and discusses the security threats faced by the technology and multi-level defense mechanisms. It also looks forward to the development trends and research directions under the fusion of post-quantum cryptography, edge computing and other technologies, providing a reference for the large-scale implementation, optimization and upgrading of this technology in the field of medical privacy AI.

Keywords: Secure Multi-Party Computation; Trusted Execution Environment; Privacy Computing; Medical Privacy.

1. Introduction

1.1. Privacy Protection Challenges in Cross-Institutional Data Collaboration

With the rapid development and widespread application of artificial intelligence technologies, the demand for cross-institutional data collaboration is growing steadily [1]. The balance among data collaboration, privacy protection and data sovereignty, the trade-off between performance and security, as well as the interoperability of heterogeneous systems have become the core challenges for cross-institutional collaboration [2,3].

1.2. Limitations of Traditional Privacy Computing Technologies

Traditional privacy computing technologies mainly fall into three categories: Secure Multi-Party Computation (MPC), Homomorphic Encryption (HE) and Trusted Execution Environment (TEE). Nevertheless, these technologies exhibit obvious limitations in practical applications, which are specified as follows:

- MPC enables multiple parties to perform joint computation without disclosing raw data, featuring strong security but incurring high computational and communication overhead [4].
- HE allows computation to be conducted on encrypted data, yet it suffers from extremely low efficiency and a high ciphertext expansion rate [5].
- TEE is highly efficient but relies on hardware and is vulnerable to side-channel attacks [6].

1.3. Importance and Challenges of Applications in the Medical Field

The healthcare field is one of the most promising application scenarios for MPC-TEE fusion technology, while also confronting extremely complex technical and ethical challenges. The high sensitivity of medical data, stringent privacy protection laws, and complex requirements for cross-institutional collaboration render traditional data sharing and analysis models unable to meet the needs of practical applications [5]. Meanwhile, the particularity of medical data determines the paramount importance of privacy computing technologies in this field.

Cross-institutional collaboration in the medical field is faced with multiple challenges, among which data heterogeneity, compliance requirements with laws and regulations (GDPR, HIPAA), and the lack of technical standards are the primary ones [5,7,8].

2. Technical Foundation and Fusion Principles

2.1. Technical Foundations of MPC and TEE

2.1.1. Technical Foundation of Secure Multi-Party Computation (MPC)

Secure Multi-Party Computation is an important branch of cryptography, whose core objective is to enable multiple participants to jointly complete the computation of specific functions without disclosing their respective input data [4]. Its theoretical origin can be traced back to the "Millionaires' Problem" proposed by Academician Andrew Chi-Chih Yao in 1982, which laid the theoretical foundation for secure two-party computation. Later, Goldreich, Micali and Wigderson

extended it to the N-party scenario and proposed the GMW protocol based on arithmetic circuits [9].

The core technical principle of MPC is the secret sharing mechanism. By splitting secret data and distributing the shares to multiple participants, the original value can only be reconstructed when a sufficient number of shares are combined, thus realizing the secure distribution and joint computation of data [4]. In practical applications, data providers perform secret sharing of data among N participants, with the shares stored in local databases and put into use after MPC preprocessing [10,11].

2.1.2. Technical Foundation of Trusted Execution Environment (TEE)

Trusted Execution Environment is a hardware-based security technology, whose core advantage lies in hardware-level security isolation, which can protect the security of code and data in an untrusted operating system and environment. Mainstream CPU manufacturers all provide TEE support, including Intel SGX, Intel TDX, AMD SEV and ARM CCA, etc. These technologies can tolerate compromised operating systems, hypervisors and even some physical attacks. Newer TEEs such as SEV-SNP, TDX and CCA further encapsulate the entire virtual machine, improving the convenience of software migration [12].

The core of TEE's working principle is the remote attestation mechanism. It verifies whether a virtual machine is running in a genuine TEE and whether the initial memory state matches the expected secure hash value through attestation protocols. Upon successful attestation, the virtual machine can obtain the required cryptographic materials for identity authentication to remote participants and access to sealed data. Its security relies on the integrity of the vendor certificate chain, proprietary hardware and firmware [13].

TEE technology also faces a variety of security challenges, and the relevant attack types will be elaborated in Section 4.1 [14]. In response to these threats, researchers have proposed a variety of defense mechanisms, such as implementing memory permission management and integrity assurance through specific technologies, adapting to specific device scenarios and adopting isolation protection measures [15].

2.2. Complementary Mechanisms and Synergistic Effects of MPC-TEE Fusion

Faced with the respective advantages and limitations of MPC and TEE, combining the two to form an MPC-TEE fusion architecture has become an important development direction of privacy-preserving computation in the medical field. Its core idea is to dynamically allocate computing tasks according to the characteristics and security requirements of the tasks, and specifically achieve the balance between security and performance through collaborative mechanisms such as hybrid encryption, dynamic task scheduling and collaborative verification.

In medical applications, this fusion technology has demonstrated significant synergistic effects:

- In federated learning scenarios, medical institutions use MPC protocols for secure aggregation of model parameters and TEE technology to accelerate local model training.
- In genomic data analysis, MPC technology is used to identify common patients and TEE technology to achieve high-performance sequence alignment and variant detection.

Both realize the dual goals of privacy protection and computational efficiency [5].

2.3. Core Design Paradigms of MPC-TEE Fusion

The fusion design of MPC and TEE is centered on addressing the secure computing needs in privacy-sensitive scenarios such as healthcare through the complementary adaptation of the two technologies. The three core design paradigms are not isolated, but present a logical relationship of complementary progression and scenario adaptation.

- MPC-in-TEE Architecture: Takes TEE as the foundation and superimposes the advantages of MPC to achieve a balance between high performance and basic security.
- TEE-protected-by-MPC Architecture: Takes MPC as the support and strengthens TEE security, adapting to high security level requirements.
- Dynamic Collaborative Architecture: Breaks through the fixed modes of the previous two, realizing dynamic scheduling of resources of both and adapting to complex and variable computing scenarios.

The three paradigms correspond to different security requirements, performance goals and deployment environments respectively, and together constitute a complete design system of MPC-TEE fusion technology.

2.3.1. MPC-in-TEE Architecture: HT2ML Framework and Its Practice

The MPC-in-TEE architecture is one of the important design paradigms of MPC-TEE fusion technology, whose core idea is to run MPC protocols within the secure execution environment provided by TEE, combining the hardware-level security protection of TEE with the advantages of secure multi-party computation of MPC protocols. Typical representatives of this framework include the HT2ML framework and the STAMP framework. Among them, STAMP (Small TEE Assisted MPC), as a lightweight TEE-assisted MPC protocol, has made important progress in privacy-preserving machine learning inference in the medical field, and the specific details will be elaborated in Section 3.1 [5].

2.3.2. TEE-protected-by-MPC Architecture: Multi-Party Attestation and Lightweight Applications

The TEE-protected-by-MPC architecture adopts an opposite design idea to the MPC-in-TEE architecture, which enhances the security of TEE through MPC protocols and addresses the trust limitations and side-channel attacks inherent in TEE. This architecture is particularly suitable for medical application scenarios with extremely high security requirements. The lightweight TEE-assisted MPC design adopted by the STAMP framework further confirms the adaptability of this fusion architecture in medical scenarios [16,17].

In this architecture, MPC protocols are used to verify the execution results of TEE to ensure the correctness and integrity of computation. Specifically, multiple participants jointly generate and verify the input parameters of TEE using MPC protocols, and conduct multi-party attestation on the output results of TEE. Even if a TEE instance is compromised, an attacker cannot forge correct output results because the correctness of the output needs to be confirmed through multi-party attestation [18]. In medical applications, the TEE-

protected-by-MPC architecture demonstrates unique advantages, enabling multiple participants to collaboratively complete secure computation, and the entire system can still maintain security even if the TEE of a single participant is attacked.

Lightweight TEE applications are another important direction of the TEE-protected-by-MPC architecture. Although traditional TEE provides strong security protection, it has strict requirements on hardware platforms and high resource occupancy. Lightweight TEE achieves deployment in resource-constrained environments by simplifying security functions and reducing resource occupancy [19,20].

2.3.3. Dynamic Collaborative Architecture: Task-Aware Resource Allocation and Hybrid Computing Mode

The dynamic collaborative architecture realizes the dynamic balance between MPC and TEE through intelligent task scheduling and resource allocation strategies [20,21]. This architecture can real-time adjust the usage ratio of MPC and TEE according to the characteristics of computing tasks, security requirements and system load, maximizing system performance while ensuring security.

The task-aware resource allocation strategy is its core, which intelligently determines the execution allocation of tasks between MPC and TEE by analyzing the characteristics of computing tasks such as computational complexity, communication requirements and security sensitivity [19,22]. The hybrid computing mode is another important feature, which allows flexible switching between MPC and TEE execution modes in the same computing process, realizing data exchange and result verification between the two.

In addition, the dynamic collaborative architecture also has adaptability and learning capabilities. It can continuously optimize the task allocation strategy by monitoring the system performance and security status in real time, adapt to different workloads and security threats, and flexibly respond to various security risks and performance requirements [16].

3. Comparative Analysis of Mainstream Frameworks in Medical Applications

3.1. HT2ML Framework: A Typical Representative of MPC-in-TEE Architecture

HT2ML (Hybrid Framework for Privacy-preserving Machine Learning using HE and TEE), as a typical representative of the MPC-in-TEE architecture, proposes an innovative hybrid architecture that combines optimized homomorphic encryption matrix multiplication with SGX enclaves, enabling efficient and secure execution of machine learning workloads. Its design concept is to protect HE-friendly functions with homomorphic encryption and execute them outside the enclave, while performing all other operations in an oblivious manner inside the enclave, thus achieving the optimal balance between security and performance.

In terms of matrix operation optimization, HT2ML uses ciphertext packing and SIMD technologies, combined with optimized matrix arrangement strategies, reducing the complexity of matrix multiplication to O(s).This optimization allows HT2ML to maintain high performance when processing large-scale medical data [5].

However, HT2ML has three main limitations:

(1) Relying on Intel SGX technology limits its deployment and application on other platforms.

(2) The memory capacity limitation of SGX may become a bottleneck in processing ultra-large-scale medical data [5,23].

(3) Assuming the SGX enclave is fully trusted may bring risks in some security-sensitive medical applications [5].

3.2. TFHE Framework: Application of Fully Homomorphic Encryption in Medical Image Analysis

TFHE (Fast Fully Homomorphic Encryption over the Torus) is a fully homomorphic encryption scheme based on the Ring-Learning-with-Errors (RLWE) problem, whose main advantage lies in its fast bootstrapping operation, exhibiting obvious advantages in processing complex functions that require a large number of multiplication operations [5,24].

In the field of medical image analysis, researchers have proposed a privacy-preserving machine learning framework based on TFHE, which realizes both privacy protection and medical image classification by quantizing the Fully Connected Neural Network (FCNN) combined with TFHE for encrypted inference [24]. In telemedicine diagnosis systems, TFHE enables doctors to make diagnoses without accessing patients' raw medical images: encrypted medical images are transmitted to the cloud, and doctors conduct diagnostic operations in the encrypted domain and return encrypted results, which not only protects patients' privacy but also optimizes the allocation of medical resources [25].

Nevertheless, TFHE faces several challenges in medical applications[26]:

(1) High computational overhead: Imposing a heavy performance burden when processing large-scale medical data.

(2) Precision loss: Based on integer operations and requiring quantization to process floating-point numbers, which may affect the precision requirements in medical practice.

(3) Large key size: The storage and transmission of keys require a lot of resources.

3.3. SEAL Framework: Advantages of Somewhat Homomorphic Encryption in Medical Data Processing

Microsoft SEAL (Simple Encrypted Arithmetic Library) is an easy-to-use and powerful homomorphic encryption library that supports two main homomorphic encryption schemes (BFV and CKKS), and has attracted much attention for its flexibility and high performance [27,28].

In medical data processing, SEAL has prominent advantages:

(1) It can realize the encrypted storage and transmission of sensitive medical data, and directly complete data analysis in the encrypted state without decryption [29,30].

(2) In the Internet of Medical Things (IoMT), it supports wearable devices to encrypt and transmit physiological signals and realize secure cloud detection [27,28].

(3) Its CKKS scheme adapts to the real number operation requirements in the medical field, capable of performing high-precision floating-point operations in the encrypted state and adapting to medical image processing scenarios [31,32].

3.4. Framework Comparison: Performance, Security and Medical Scenario Adaptability

To comprehensively compare the application value of the three privacy computing frameworks in medical scenarios, this paper analyzes them from five core dimensions: performance, security, medical scenario adaptability, ease of use and deployment complexity, and scalability and ecosystem. The specific indicator differences of each framework are shown in Table 1 [5].

Table 1. Comparison of Core Dimensions of Three Mainstream Privacy Computing Frameworks

Comparison Dimension	HT2ML Framework	TFHE Framework	SEAL Framework
Performance	Optimal performance in machine learning tasks, CNN inference is more than 100 times faster than pure HE; high efficiency in matrix operation; limited by SGX memory, unable to process ultra-large-scale data	Fast encryption/decryption speed (29.1ms for encryption, 1.8ms for decryption); extremely high homomorphic operation overhead (2308697.2ms)	Balanced performance, high floating-point precision of CKKS (error of $$10^{-6$$); only supporting addition and multiplication operations, low efficiency in nonlinear processing
Security	Based on SGX hardware security + MPC cryptographic security; assuming the SGX enclave is fully trusted, with the risk of hardware vulnerabilities	Based on the RLWE problem, with cryptographic security proof; quantum-computation attack resistant; no hardware dependence, avoiding single point of failure	128/192/256-bit security level with improved noise management; somewhat homomorphic feature, requiring linear approximation for nonlinear operations with the risk of precision leakage
Medical Scenario Adaptability	Training and inference of complex medical AI models (medical image diagnosis, pathological analysis)	Encrypted inference of medical images; telemedicine diagnosis; genetic disease risk assessment	Statistical analysis of electronic health records; encrypted query of genomic data; physiological signal processing in IoMT; drug dosage calculation
Ease of Use & Deployment Complexity	Extremely high deployment complexity; requiring mastery of MPC/TEE/HE three technologies; dependent on Intel SGX hardware	High use complexity; requiring in-depth understanding of mathematical principles and parameter configuration; needing debugging and optimization in the quantization process	Optimal ease of use; complete documents and APIs; PySEAL binding lowering the development threshold; supporting flexible parameter configuration
Scalability & Ecosystem	Research prototype stage with low commercialization level; only supporting Intel platforms; limited ecological resources	Highly active open-source community; supporting multiple programming languages; few extension libraries for machine learning	Most complete ecosystem; official C++ implementation + PySEAL; rich industry extension libraries; continuously maintained and upgraded by Microsoft

From the comprehensive comparison results, the three frameworks have clear application positioning:

(1) HT2ML: Has an exclusive advantage in machine learning performance, adapting to medical AI scenarios with high performance requirements, moderate security requirements and based on Intel hardware platforms (e.g., collaborative diagnosis of medical images in Grade A tertiary hospitals, joint training of regional medical AI models).

(2) TFHE: Performs prominently in encryption/decryption speed and quantum-resistant security, adapting to medical scenarios with extremely high security requirements, the need for fully homomorphic operations and no hardware dependence (e.g., joint analysis of rare disease genetic data across countries/regions, high-end telemedicine diagnosis).

(3) SEAL: Has obvious advantages in ease of use/deployment and numerical precision, adapting to medical scenarios with high ease of use requirements, relatively simple computing tasks and the need for precise floating-point calculation (e.g., statistical analysis of electronic health records in primary medical institutions, data processing in IoMT, encrypted query of genomic data).

In practical cross-institutional collaboration scenarios in the medical field, a single framework is often unable to meet full-dimensional requirements, and the fusion of multiple frameworks has become a future development trend. For example, SEAL is used for encrypted storage and transmission of medical data, HT2ML for training and inference of complex AI models, and TFHE for fully homomorphic protection of core sensitive data. Through the collaborative cooperation of multiple frameworks, the full-life-cycle privacy protection of medical data is realized.

4. Security Threats and Defense Mechanisms

MPC-TEE fusion technology achieves the balance between security and performance through the collaborative design of software and hardware. However, due to the complexity of its architecture, the heterogeneity of components and the high sensitivity of medical data, this technology faces multiple security threats from the TEE side, MPC side and fusion architecture side, and various threats have the risk of mutual

superposition and collaborative attacks. This chapter sorts out the typical security threats of MPC-TEE fusion technology from three dimensions [6].

4.1. TEE Side-Channel Threats and Defense Mechanisms

TEE is the high-performance computing core of the MPC-TEE fusion architecture, whose security relies on the underlying hardware design and isolation mechanism. Side-channel attacks are the most major and difficult-to-defend security threats faced by TEE. Instead of targeting the mathematical vulnerabilities of encryption algorithms, side-channel attacks reverse-derive sensitive information by analyzing the physical characteristics such as timing, power consumption and electromagnetic radiation generated during the operation of TEE, featuring low attack cost, high concealment and strong destructiveness. The attack risk is more prominent in resource-constrained scenarios such as medical implantable devices and wearable devices.

4.1.1. Typical TEE Side-Channel Security Threats

Typical TEE side-channel threats mainly include software side-channel attacks and physical-assisted attacks. The specific attack methods, attack principles and risks in medical scenarios are shown in Table 2 [33-37]:

Table 2. Typical TEE Side-Channel Attacks and Risks in Medical Scenarios

Attack Type	Attack Principle	Medical Scenario Risk
Timing Attack	Reverse-deriving patients' sensitive data and encryption keys by analyzing the time differences in TEE's execution of encryption operations and data processing	Prominent risks in medical implantable devices (e.g., pacemakers)
Power Analysis Attack	Divided into Simple Power Analysis (SPA) and Differential Power Analysis (DPA), obtaining keys by monitoring the power consumption fluctuations of TEE during operation	Portable medical devices have lower anti-attack capability due to simplified encryption mechanisms
Electromagnetic Radiation Attack	Stealing patients' sensitive data and device control instructions by analyzing the electromagnetic radiation characteristics of TEE components	The strong electromagnetic environment of large medical devices (e.g., MRI) is more likely to become an attack vector
Fault Injection Attack Fault Injection Attack	Artificially introducing faults to induce TEE anomalies, leaking confidential information or destroying system functions, which can be combined with software side-channels for attacks	Able to break through traditional protection and threaten the security of life support devices
Memory Encryption Vulnerability Attack	Stealing sensitive information by exploiting the leakage paths in the TEE deterministic memory encryption mechanism in scenarios of physical tampering or kernel compromise	Stealing core privacy data such as patients' medical records and keys by tampering with the system kernel or physically contacting medical devices to bypass memory encryption protection

4.1.2. TEE Side-Channel Defense Mechanisms

In response to the typical security threats on the TEE side, the current defense measures focus on multi-level and full-process protection, combining various means such as hardware hardening, software optimization and algorithm design to defend from the source, process and result of attacks, while taking into account the real-time performance and resource constraints of medical devices. The specific defense mechanisms are as follows:

(1) Anti-timing attack: Eliminate timing differences through branchless logic, data-independent memory access and unified loop structures to adapt to the real-time requirements of medical devices [38].

(2) Anti-power analysis attack: Combine masking technology and obfuscation technology to realize the statistical independence between leaked information and raw data, and cover the real power consumption mode.

(3) Anti-electromagnetic radiation attack: Construct a Faraday cage structure to achieve >100dB attenuation in the 1GHz frequency band, optimize PCB layout, filter design and grounding system to improve electromagnetic compatibility [35].

(4) Anti-fault injection attack: Introduce redundant computation (dual-core lockstep technology, multi-version programming, time redundancy), establish a multi-level error detection mechanism, and combine check code verification, fault isolation and security degradation strategies to detect and handle faults in a timely manner [36].

(5) Memory encryption protection: Combine hardware isolation and software hardening to cut off the information leakage paths caused by physical tampering and kernel tampering, and strengthen the isolation integrity of TEE.

4.2. MPC Side-Channel Threats and Defense Mechanisms

MPC is the distributed security core of the MPC-TEE fusion architecture, whose security is based on cryptographic algorithms and protocol design. Although it has no hardware dependence, due to its distributed collaboration characteristics, it faces multiple security threats such as protocol vulnerabilities, malicious behaviors of participants and communication pattern leakage. In cross-institutional collaboration scenarios in the medical field, the large number of participants, complex trust relationships and high sensitivity of medical data make the security threats on the MPC side more likely to be exploited, which may lead to the leakage of patient data and tampering of computation results, affecting the scientificity of clinical decision-making.

The comparison of MPC side-channel security threats and defense mechanisms is shown in Table 3 [39-41]:

Table 3. Comparison of MPC Side-Channel Threats and Defense Mechanisms

Attack Type	Attack Principle	Medical Scenario Risk	Core Defense Mechanism
Oblivious Transfer (OT) Abuse Attack	Stealing data by exploiting MPC side-channel vulnerabilities to abuse OT components	Leakage of patient privacy during cross-institutional collaboration	Adopting verifiable MPC protocols and integrating ZKP mechanisms
Communication Pattern Analysis Attack	Inferring sensitive information by analyzing the characteristics of communication volume, timing and routing	The regularity of communication in IoMT exacerbates the risk of information leakage	Deploying mix networks and communication padding technologies
Collusion Attack	Multiple parties collude to break through the anti-collusion mechanism	Concealed attacks, stealing core medical data	Establishing an access and audit system combined with blockchain
Malicious Input Tampering Attack	Malicious participants tamper with medical data to manipulate computation results	Leading to wrong clinical decisions or distorted scientific research data	Adopting secure protocols and ensuring data integrity through multiple verifications

4.3. Fusion Architecture Threats and Defense Mechanisms

While the TEE-MPC fusion architecture realizes high-security multi-party collaborative computation and meets the privacy protection and data sharing needs in the medical field, it also introduces new cross-domain security risks due to cross-component interaction, collaborative mechanism design and permission boundary division. The core security threats and corresponding mechanisms are shown in Table 4 [42,43]:

Table 4. Fusion Architecture Threats and Defense Mechanisms

Security Threat Type	Threat Description	Defense Mechanism
Component Side-Channel Attack	Obtaining sensitive information by exploiting interface vulnerabilities between TEE and MPC components through analyzing component interaction patterns, cache sharing mechanisms, etc.	Implementing interface isolation, combining physical and logical isolation and PBAC permission management to block attack paths, and adopting timing isolation and noise injection to interfere with component side-channel analysis
Component Interface Permission Abuse Attack	Accessing sensitive data in TEE or MPC without authorization by taking advantage of defects in interface permission design	Following the principle of least privilege, establishing a hierarchical and fine-grained permission management system, improving permission audit, and dynamically adapting to the needs of medical scenarios
Collaborative Vulnerability Attack	Launching combined attacks by exploiting collaborative defects such as disunified key management and out-of-control data flow in the fusion process to break through the protection of a single component	Building a unified key management system, and implementing two-factor authentication combined with TEE's HSM and MPC's TPM
Collusion and Input Tampering Collaborative Attack	Malicious participants combine MPC-side collusion attacks with TEE-side fault injection attacks to tamper with cross-component data flow and manipulate computation results	Integrating TEE and MPC defense mechanisms, establishing a cross-component anomaly detection system, linking audit supervision and fault isolation, and relying on the MedGuard framework to improve the overall anti-attack capability

5. Challenges and Prospects

5.1. Analysis of Technical Challenges

5.1.1. Severe Security Threats

Security threats are the primary challenge. The 2023 Platypus attack mentioned earlier exploited the design flaws of the SGX memory encryption mechanism to achieve key extraction and code tampering attacks[4]. In addition, the lack of integrity protection in AES-XTS encryption in DDR5 memory systems may also be exploited by attackers to leak sensitive information[7]. These findings pose a serious threat to privacy computing systems relying on TEE [6].

Side-channel attacks remain the main security threat to TEE. Since TEE shares the same silicon chip with the main CPU, despite "logical" isolation, it is still vulnerable to side-channel attacks such as Spectre and Meltdown and memory-based exploit. Researchers have also discovered new types of attacks against MPC-TEE fusion systems, such as attacks on

masking strategies. These attacks take advantage of the characteristic that masks must be precomputed, resulting in huge computational and storage overhead. Once the precomputed masks are exhausted, mask reuse is inevitable, leading to security vulnerabilities.

5.1.2. Unresolved Performance Bottlenecks

Although MPC-TEE fusion technology has been significantly improved compared with pure MPC, it still faces challenges in processing large-scale data and complex models, such as high computational complexity, large communication overhead and high storage requirements[4,5]. These problems directly restrict the application of the technology in large-scale medical data collaboration scenarios such as regional medical data sharing and multi-center clinical research.

5.1.3. Insufficient Standardization

Insufficient standardization is an important factor restricting technological development. TEE implementations of different manufacturers are quite different with a lack of unified interface standards; MPC protocol implementations are also diverse with poor interoperability. This fragmented status increases development costs, hinders the large-scale promotion of the technology, and makes it difficult to realize seamless collaboration between different medical institutions and different technical platforms[5].

5.1.4. High Application Costs

Cost issues are also a practical challenge. High-performance TEE hardware is costly, for example, Intel processors supporting SGX are several times more expensive than ordinary processors; MPC computation requires a lot of CPU and memory resources, increasing operational costs. These cost factors limit the application of the technology in resource-constrained scenarios such as primary medical institutions and grassroots healthcare systems[5].

5.2. Future Development Trends and Research Directions

Faced with the current challenges, the future development of MPC-TEE fusion technology presents several important directions, which will further promote the application and innovation of the technology in the medical field:

5.2.1. Fusion with Post-Quantum Cryptography

With the progress of quantum computing technology, traditional cryptographic algorithms are facing the risk of being cracked. MPC-TEE fusion technology needs to integrate post-quantum cryptographic algorithms such as lattice-based cryptography and hash-based cryptography. Researchers have begun to explore relevant protocols and authentication mechanisms, which is the key to ensuring the long-term security of medical data in the quantum era.

5.2.2. Combination of Edge Computing and 5G/6G Networks

MPC-TEE fusion technology can take advantage of edge computing to distribute computing tasks to edge nodes, reducing the transmission of sensitive medical data and improving the level of privacy protection. 5G/6G network slicing technology can also provide isolation protection for medical applications with different security levels, realizing the on-demand allocation of network resources and further improving the security and efficiency of cross-institutional medical data collaboration.

5.2.3. In-Depth Integration of Artificial Intelligence and Privacy Computing

Applying AI technology to the optimization of privacy computing protocols can realize adaptive security strategies, intelligent resource scheduling and automated vulnerability detection. For example, using reinforcement learning to optimize the task scheduling strategy of the MPC-TEE dynamic collaborative architecture, and using deep learning to detect and defend against side-channel attacks in real time, which can effectively improve the performance and security of the fusion system.

5.2.4. Integration of Blockchain Technology

Blockchain technology provides a decentralized and tamper-proof trust foundation for cross-institutional collaboration. Recording the computation results of MPC-TEE on the blockchain can realize traceable and tamper-proof data usage, and smart contracts can also automate the collaborative process between medical institutions, improving collaboration efficiency and reducing human intervention risks.

5.2.5. Standardization and Ecosystem Construction

Establishing a unified technical standard and certification system for MPC-TEE fusion technology is the key to promoting its large-scale application. It is necessary to formulate unified interface standards, security evaluation criteria and application specifications, build a complete open-source development ecosystem, and strengthen talent training to improve the overall technical level of the industry, thus providing a solid foundation for the scalable development of the technology in the medical field.

6. Conclusion

This paper systematically reviews the application of MPC-TEE fusion technology in the field of medical privacy AI, clarifies the technical characteristics and limitations of MPC and TEE. The two technologies achieve the balance between security and performance through software and hardware collaboration, and the three formed core design paradigms (MPC-in-TEE, TEE-protected-by-MPC, dynamic collaborative architecture) can provide differentiated implementation paths for different medical scenarios, among which the dynamic collaborative architecture is more suitable for complex medical AI computing tasks.

By comparing the three mainstream frameworks (HT2ML, TFHE, SEAL), their application positioning in medical scenarios is clarified, and it is confirmed that the fusion of multiple frameworks is the key strategy for the full-life-cycle privacy protection of medical data. Meanwhile, building a full-process hierarchical defense mechanism from the TEE side, MPC side and fusion architecture side can effectively respond to various typical security attacks and improve the security applicability of the technology in high-sensitive medical scenarios.

The research finds that the implementation of this technology in the medical field still faces challenges such as difficult defense against side-channel attacks, performance bottlenecks in large-scale data processing, low standardization and high application costs. Combined with future development trends, the **core research suggestions** are as follows:

(1) Optimize the task scheduling and algorithms of the fusion architecture to break through performance bottlenecks and adapt to the processing requirements of large-scale

medical data.

(2) Accelerate the formulation of unified technical standards and evaluation frameworks to improve the interoperability between different platforms and promote the large-scale promotion of the technology.

(3) Develop lightweight fusion schemes and low-cost hardware solutions to reduce application costs and expand the application scope of the technology in primary medical institutions.

In the future, with technological optimization, standard improvement and ecosystem construction, MPC-TEE fusion technology will be more widely and large-scale implemented in the field of medical privacy AI, becoming a core technical support for safeguarding medical data privacy, releasing data value and promoting the development of smart healthcare, and ultimately realizing the goals of secure sharing and efficient utilization of medical data.

References

[1] Evans, D., Kolesnikov, V., & Rosulek, M. (2018). A pragmatic introduction to secure multi-party computation. *Foundations and Trends in Privacy and Security*, 2(2–3), 70–246. https://doi.org/10.1561/3300000019.

[2] Yang, Z. G., Wang, Z. T., Wu, D. P., et al. (2023). Research on data heterogeneous robust federated learning with privacy protection in internet of things. *Journal of Electronics & Information Technology*, 45(12), 4235–4244. https://doi.org/ 10. 11999/JEIT221193.

[3] Chen, X., & Liu, J. (2021). Research on interoperability system of heterogeneous privacy computing platform based on middleware and blockchain. *Information and Communications Technology and Policy*, 47(6), 83–95.

[4] Lipp, M., Kogler, A., Oswald, D., et al. (2021). PLATYPUS: Software-based power side-channel attacks on x86. In *2021 IEEE Symposium on Security and Privacy (S&P)* (pp. 1–18). IEEE. https://doi.org/10.1109/SP51572.2021.00042.

[5] Wang, Q., Zhou, L., Bai, J., et al. (2023). HT2ML: An efficient hybrid framework for privacy-preserving machine learning using HE and TEE. *Computers & Security*, 135, 103509. https://doi.org/10.1016/j.cose.2023.103509.

[6] Zhang, F., Zhou, L., Zhang, Y., et al. (2024). Trusted execution environment: Status and prospects. *Journal of Computer Research and Development*, 61(1), 243–260. https://doi.org/10. 7544/ issn1000-1239.202221016.

[7] Li, Y., Ma, R., Li, C., et al. (2020). Secure multiparty computation for privacy-preserving drug discovery. *Bioinformatics*, 36(9), 2872–2880. https://doi.org/10.1093/ bioinformatics/ btaa038.

[8] Spence, A., & Bangay, S. (2020). Side-channel sensing: Exploiting side-channels to extract information for medical diagnostics and monitoring. *IEEE Journal of Translational Engineering in Health and Medicine*, 8, 4900213. https://doi. org/ 10.1109/ JTEHM.2020.3028996.

[9] Goldreich, O., Micali, S., & Wigderson, A. (1987). How to play any mental game. In *STOC '87: Proceedings of the 19th Annual ACM Symposium on Theory of Computing* (pp. 218–229). ACM. https://doi.org/10.1145/28395.28420.

[10] Han, S., & Jang, J. (2021). MyTEE: Own the trusted execution environment on embedded devices. In *2021 IEEE International Conference on Consumer Electronics (ICCE)* (pp. 1–6). IEEE. https://doi.org/10.1109/ICCE50685.2021.9427320.

[11] Li, Y., Ma, R., Li, C., et al. (2020). Secure multiparty computation for privacy-preserving drug discovery. *Bioinformatics*, 36(9), 2872–2880. https://doi.org/ 10.1093/ bioinformatics/ btaa038.

[12] Zhang, F., Zhou, L., Zhang, Y., et al. (2024). Trusted execution environment: Status and prospects. *Journal of Computer Research and Development*, 61(1), 243–260. https://doi.org/ 10. 7544/ issn1000-1239.202221016.

[13] Ménétrey, J., Göttel, C., Pasin, M., et al. (2022). An exploratory study of attestation mechanisms for trusted execution environments. arXiv preprint. https://doi.org/10. 48550/ arXiv. 2204.06790.

[14] Zhang, X., Wang, J., Cheng, Y., et al. (2023). Interface-based side channel in TEE-assisted networked services. *IEEE/ACM Transactions on Networking*, 32(1), 613–626. https://doi. org/ 10. 1109/TNET.2023.3294019.

[15] Zhao, W., Lu, K., Qi, Y., et al. (2020). MPTEE: Bringing flexible and efficient memory protection to Intel SGX. In *Proceedings of the 15th European Conference on Computer Systems* (pp. 1–15). ACM. https://doi.org/ 10.1145/ 3342195. 3387536.

[16] Yang, F., Zhang, Q. Y., Shi, Z. P., & Guan, Y. (2023). Survey on software side-channel attacks in trusted execution environment. *Journal of Software*, 34(1), 381–403. https://doi. org/ 10.13328/j.cnki.jos.006501.

[17] Liu, J., Li, N., & Tian, Y. (2022). STAMP: Lightweight TEE-assisted MPC for efficient privacy-preserving machine learning. arXiv preprint. https://doi.org/10. 48550/arXiv. 2210. 10133.

[18] De Haan, R., van der Sloot, B., & de Vries, B. (2024). *Privacy-preserving techniques for analysis of medical data: Secure multi-party computation*. University of Twente Press.

[19] Baker, S. B., Xiang, W., & Atkinson, I. (2017). Internet of things for smart healthcare: Technologies, challenges, and opportunities. *IEEE Access*, 5, 26321–26344. https://doi.org/10. 1109/ ACCESS.2017.2775180.

[20] Mutlag, A. W., Ghani, M. K. A., Arunkumar, N., et al. (2019). Enabling technologies for fog computing in healthcare IoT systems. *Future Generation Computer Systems*, 96, 228–240. https://doi.org/10.1016/j.future.2018.02.009.

[21] Jiang, C., Li, Y., Cao, C., & Li, J. (2021). Survey of security technologies for IoT edge stream processing based on trusted execution environment. *Journal of Cyber Security*, 6(3), 169–186.

[22] Kwon, D., Seo, J., Cho, Y., et al. (2020). PrOS: Light-weight privatized secure OSes in ARM TrustZone. *IEEE Transactions on Mobile Computing*, 19(1), 160–173. https://doi.org/10. 1109/ TMC.2019.2910861.

[23] Intel Corporation, & Ant Group. (2025). *Better together: Intel® SGX and Intel® DL Boost power privacy-preserving machine learning*. Intel China.

[24] Selvakumar, B., & Senthilkumar, M. (2025). A privacy preserving machine learning framework for medical image analysis using quantized fully connected neural networks with TFHE based inference. *Scientific Reports*, 15(1), 12345. https://doi.org/10.1038/s41598-025-52147-8.

[25] Jin, C., Jia, W., Wan, L., et al. (2025). DMAFL: Effective defense against malicious attacker federated learning framework via blockchain and TFHE. *Journal of King Saud University – Computer and Information Sciences*, 37(8), 102567. https://doi.org/10.1016/j.jksuci.2025.102567.

[26] Liu, H., Wang, Y., & Chen, L. (2023). Challenges and optimizations of TFHE for privacy-preserving medical data analytics. *Computers & Security*, 126, 103265. https://doi.org/ 10. 1016/j.cose. 2023.103265.

[27] Wu, L., Wang, X. A., Liu, J., et al. (2025). Homomorphic encryption for machine learning applications with CKKS algorithms: A survey of developments and applications. *Computers, Materials & Continua*, 85(1), 89–119. https://doi.org/10.32604/CMC.2025.064346.

[28] Yang, Y. T., Liu, D. L., Liu, P. H., et al. (2022). BFV-Blockchainvoting: A blockchain electronic voting system supporting BFV fully homomorphic encryption. *Journal on Communications*, 43(9), 100–111. https://doi.org/ 10. 11959/j. issn.1000-436x.2022188.

[29] Xia, J., Wu, M., & Li, P. (2026). SHE-SFL: An efficient and privacy-preserving heterogeneous federated split learning architecture based on homomorphic encryption. *Future Generation Computer Systems*, 175, 108101. https://doi.org/10. 1016/j. future.2025.108101.

[30] Li, R. R., Guo, R., Zhang, Y. H., et al. (2025). A privacy protection scheme for edge federated learning based on multi-key homomorphic encryption. *Journal of Frontiers of Computer Science and Technology*.

[31] Lan, Y., Li, L., Peng, H., et al. (2025). An efficient and secure adaptive federated learning method based on CKKS for data processing in the Internet of Things. *Internet of Things*, 33, 101725. https://doi.org/10.1016/j.iot.2025.101725.

[32] Magyari, A., & Chen, Y. (2025). DARTPHROG: A superscalar homomorphic accelerator. *Sensors*, 25(16), 5176. https://doi. org/ 10. 3390/s25165176.

[33] Beytüllah, Y., Gürkan, G., Fatih, A., et al. (2023). Network fingerprinting via timing attacks and defense in software defined networks. *Computer Networks*, 232, 109850. https:// doi. org/10.1016/j.comnet.2023.109850.

[34] Le, D. H. (n.d.). Research on key technologies of circuit-level protection for cryptographic chips against power analysis attacks [Doctoral dissertation, National University of Defense Technology].

[35] Deng, G. M., Zhao, Q., Zhang, P., et al. (2009). Electromagnetic frequency-domain template analysis attacks against cryptographic chips. *Chinese Journal of Computers*, 32(4), 602–610. https://doi.org/10.3724/SP.J.1016.2009.00602.

[36] Jiang, W., Wen, L., Zhan, J., et al. (2020). Design optimization of confidentiality-critical cyber physical systems with fault detection. *Journal of Systems Architecture*, 107, 101739. https://doi.org/10.1016/j.sysarc.2020.101739.

[37] Hayes, J., & Ohrimenko, O. (2018). Contamination attacks and mitigation in multi-party machine learning. In *Advances in Neural Information Processing Systems* (Vol. 31, pp. 10212–10222). Curran Associates.

[38] Wang, Z. P., Zhu, Z. Y., & Wang, L. M. (2024). Quantitative research on defense against cache side-channel attacks. *Journal of Cyber Security*, 9(4), 107–124. https://doi.org/ 10.19363/ j.cnki. 10-1380/tp.2024.04.00.

[39] Yang, Y. G., Qiu, S., Huang, R. C., et al. (2025). All-or-nothing quantum oblivious transfer for unknown unitary operations. *Advanced Quantum Technologies*, 8(11), e2500511. https://doi. org/ 10.1002/qute.202500511.

[40] Rauzy, P., & Guilley, S. (2014). Formal analysis of CRT-RSA Vigilant's countermeasure against the BellCoRe attack: A pledge for formal methods in the field of implementation security. arXiv preprint. https://doi.org/ 10.48550/ arXiv.1401. 8172.

[41] Zhang, H., Fu, J., Liao, X., et al. (2026). Time-controlled proxy searchable re-encryption against collusion attacks. *Computer Standards & Interfaces*, 97, 104139. https://doi.org/10. 1016/j. csi. 2026.104139.

[42] Rauzy, P., & Guilley, S. (2014). Formal analysis of CRT-RSA Vigilant's countermeasure against the BellCoRe attack: A pledge for formal methods in the field of implementation security. arXiv preprint. https://doi.org/ 10.48550/ arXiv. 1401. 8172.

[43] Zhang, H., Fu, J., Liao, X., et al. (2026). Time-controlled proxy searchable re-encryption against collusion attacks. *Computer Standards & Interfaces*, 97, 104139. https://doi.org/ 10. 1016/ j.csi.2026.104139.