

Homomorphic Encryption for Secure Federated Learning: A PRISMA-Based Systematic Review

Dinko Dinkov

Nikola Vaptsarov Naval Academy, Varna, Bulgaria
d.dinkov@naval-acad.bg

Abstract: Federated learning (FL) enables collaborative training without sharing raw data but remains vulnerable to privacy leakage, poisoned gradients, and incorrect aggregation. Homomorphic encryption (HE) supports secure aggregation over encrypted updates, yet existing solutions are heterogeneous and lack systematic comparison. This paper presents a PRISMA-based systematic review of 104 studies on HE-enabled security mechanisms in FL, analyzed within the confidentiality–integrity–availability (CIA) framework. The results show a growing focus on poisoned-gradient robustness and verifiable aggregation, while only few integrated approaches address all CIA dimensions. These findings outline current limitations and guide future development of secure and trustworthy federated learning systems.

Keywords: homomorphic encryption, network security, federated learning, systematic review.

Received 18 November 2024

Accepted 3 December 2024

Published 15 January 2025

1. Introduction

Federated learning has emerged as a prominent paradigm for collaborative model training without centralizing sensitive data, enabling distributed participants to jointly build machine learning models while maintaining local data ownership [1, 2]. Despite this decentralized design, numerous studies demonstrate that standard FL protocols remain vulnerable to privacy leakage, model poisoning, and aggregation manipulation [3, 4, 5, 6]. Consequently, cryptographic protection mechanisms are increasingly integrated into FL systems to provide stronger confidentiality, integrity, and availability guarantees [7].

Among existing privacy-preserving technologies, HE has attracted particular attention due to its ability to enable direct computation over encrypted model updates [7, 8]. By allowing aggregation to be performed in the ciphertext domain, HE prevents the central server from accessing individual client parameters while preserving model accuracy. As a result, HE-based secure aggregation has become one of the most actively investigated directions in privacy-preserving federated learning [9, 10, 11].

In recent years, the research landscape has expanded rapidly, producing a large number of heterogeneous solutions that employ different homomorphic schemes, key management strategies, aggregation protocols, and robustness mechanisms [8, 12, 13]. However, these approaches are typically evaluated under inconsistent threat models, performance metrics, and experimental settings, which complicates direct comparison and limits the ability to identify practically applicable designs. Existing surveys [13, 14] predominantly provide narrative

or conceptual overviews, focusing on architectural or theoretical aspects rather than a systematic and reproducible synthesis of the evidence.

To address this limitation, this study conducts a systematic review of HE-based security mechanisms in federated learning using the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) [15] methodology. The objective is to objectively identify, filter, and analyse relevant scientific publications and to provide a structured comparison of contemporary approaches according to their security guarantees, computational overhead, and practical applicability within the CIA framework.

The main contributions of this work are as follows:

- systematic identification and screening of recent HE-based FL research using transparent inclusion and exclusion criteria;
- structured taxonomy of approaches for enhancing confidentiality, integrity, and availability;
- comparative analysis of cryptographic schemes, aggregation mechanisms, and robustness techniques;
- identification of open challenges and directions for future research.

The remainder of the paper is organized as follows. Section 2 describes the PRISMA-based methodology and study selection process. Sections 3–6 present the comparative analysis of approaches addressing confidentiality, integrity, availability, and integrated protection. Finally, the paper summarizes key findings and outlines future research directions.

2. Systematic review methodology

The analysis of contemporary approaches to enhancing security in federated learning was performed using the PRISMA methodology [15]. The goal of this process is to systematically identify, filter, and select relevant scientific publications that examine the use of homomorphic



© The Author(s). Published by CIEES Association Press. This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivs 4.0 Generic License.

algorithms to protect the confidentiality, robustness, and correctness of aggregation in FL environments.

The Scopus database was used as the main search source due to its wide coverage of peer-reviewed scientific journals and conferences in the fields of computer science, cryptography, and artificial intelligence. The search covers the period 2022–2025 in order to include the most recent scientific developments on the topic. The search process was carried out using the advanced features of Scopus, applying a language filter for publications in English.

Keywords and phrases related to federated learning and homomorphic encryption were used to identify relevant studies, including "homomorphic encryption," "federated learning," "privacy preserving," "secure aggregation," "poison resistance," and "verification." The key terms were combined using Boolean operators, with the final search expression taking the following form: ("homomorphic encryption") AND ("federated learning") AND ("privacy preserving" OR "secure aggregation" OR "poison resistance" OR "verification").

The initial search identified 634 scientific publications, which were exported for further processing. After removing 13 duplicate (preprint) records, 621 unique articles remained. In the next stage, the titles and abstracts were reviewed, resulting in 385 publications being excluded due to a lack of direct relevance to the research objectives. Of the remaining 236 articles, 109 were excluded due to a lack of access to the full text.

A subsequent applicability check led to the exclusion of another 23 publications in which homomorphic encryption was only mentioned peripherally, without being the main research focus. As a result of this multi-stage process, in accordance with the PRISMA methodology, 104 scientific publications were selected that fully met the inclusion criteria and were used for an in-depth comparative analysis of contemporary approaches to protection in FL.

The process of identifying, filtering, and final selection of publications is summarized in a PRISMA diagram, shown in Figure 1, which visualizes the number of included and excluded studies at each stage of the analysis.

3. Confidentiality mechanisms in federated learning

Within the CIA triad, HE is used in FL as the primary mechanism for ensuring the confidentiality of transmitted client gradients and parameters. Encrypting local updates prevents the direct disclosure of sensitive information during aggregation, as the central server operates entirely on ciphertexts. Along with these advantages, the practical application of HE in FL introduces specific vulnerabilities related mainly to cryptographic key management.

One of the main threats in this context is the "collusion attack", in which one or more clients collaborate with the aggregating server in order to reveal the individual local updates of the other participants [16]. This vulnerability is mainly characteristic of shared key pair schemes, in which all clients have the same private key for decrypting the aggregated result [17]. In such a configuration, compromising even a single client can lead to a complete

loss of confidentiality, as it becomes possible to decrypt the individual encrypted gradients.

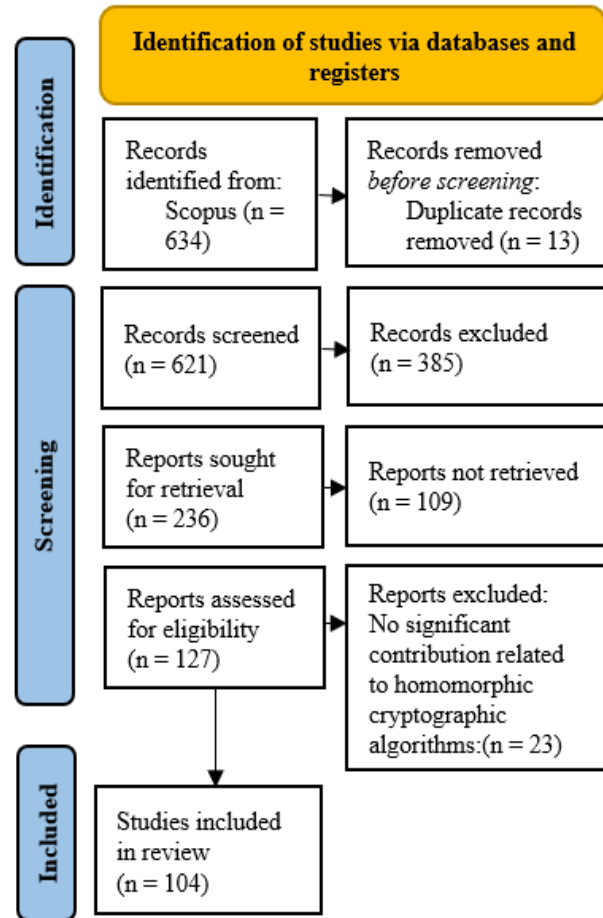


Fig 1. PRISMA-based study selection process.

3.1. Approaches to protection against collusion attacks

In order to limit collusion attacks in FL, various cryptographic and protocol mechanisms have been proposed in the scientific literature. A major group of solutions includes threshold cryptographic schemes and multi-key approaches, which eliminate the single point of trust by requiring the joint participation of a predetermined number of clients in decrypting the aggregated model [18]. In parallel, methods are being developed to neutralize collusive attacks within shared-key schemes, which introduce additional protective mechanisms without compromising the compatibility of HE. Table 1 shows the articles studied, sorted by key scheme.

Some solutions for protection against collusion attacks employ masking and obfuscation of local updates. In the scheme proposed in [17], each client adds a random mask to their homomorphically encrypted gradients before sending them to the aggregation server. To prevent the masks from being revealed in the event of collusion, the mask values are distributed among the participants through verifiable secret sharing, so that neither the server nor a limited coalition of clients has enough information to recover them. Upon aggregation, the masks are summed and correctly neutralized, allowing for the correct aggregate result to be obtained without

Table 1. Key schemes.

Key scheme	Collusion resistant	2022	2023	2024	2025
Shared key	No	[19, 20, 21, 22, 23]	[6, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33]	[34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57]	[58, 59, 60, 11, 61, 62, 63, 64, 65, 66, 67, 68, 69]
Shared key	Yes	[18, 70]	[71]	[9, 16, 17, 72, 73]	
Threshold cryptography	Yes	[74, 75]	[76]	[77, 78, 79, 80, 81, 82, 83, 84]	[85, 86, 87, 88, 89, 90, 91, 92, 93]
Multi-key	Yes	[94, 95, 96, 97]	[98, 99, 100, 101]	[5, 10, 102, 103, 104, 105, 106]	[107, 108, 109, 110, 111, 112, 113, 114]

revealing the individual gradients. Similarly, the schemes presented in [18] and [70] use blinding factors pre-generated by a trusted party, which are constructed so that their sum is zero. Thanks to this property, the factors are automatically canceled during homomorphic aggregation, ensuring the correctness of the result and protection against collusion between the server and the participants.

Other approaches, such as the schemes proposed in [16] and [71], combine HE with differential privacy by applying Gaussian or Laplace noise to the local gradients so that even with collusion, the original individual data cannot be recovered.

The schemes proposed in [9] and [16] introduce local protection parameters in the form of individual coefficients that are unique to each client and distributed through a trusted third party. These parameters are directly involved in the calculation of local updates and are not known to the aggregating server or other participants. As a result, even in the event of collusion between the server and multiple clients, the lack of information about the individual coefficients limits the ability to reconstruct local gradients and extract sensitive information.

Finally, solutions such as [73] combine HE with additive secret sharing, whereby local models are divided into multiple encrypted shares distributed among different computing nodes under the control of a trusted institution. This approach ensures that no single node or aggregator has enough information to recover the local parameters, thereby providing resistance to collusion attacks and eliminating single points of compromise.

A disadvantage of schemes relying on trusted third parties is the introduction of an additional point of trust—compromising these entities can lead to a complete security breach. In approaches based on differential privacy, noise in the data reduces the accuracy of the model, and in obfuscation techniques, there is an additional communication and computational overhead, in addition to the fact that these techniques must be controlled by a third party. The secret sharing-based mechanism, although highly secure, requires a high degree of coordination and synchronization among participants, making it less applicable in large-scale scenarios.

updates that may indicate collusion or fake identities. Together, these approaches enhance resilience against

4. Integrity protection and poisoned-gradient robustness

Integrity as an element of the CIA triad in FL refers to ensuring the correctness and reliability of the learning process and the resulting global model. Unlike threats to confidentiality, where the goal is to extract sensitive information, attacks on integrity are aimed at manipulating training by submitting incorrect, manipulated, or maliciously constructed updates. Such attacks can lead to a deterioration in convergence, a significant reduction in accuracy, or the introduction of targeted undesirable behavior into the model (e.g., backdoor functionality).

The main source of risk to integrity are the so-called Byzantine clients, which do not follow the training protocol and send modified gradients in order to influence the final result. Due to the decentralized nature of federated learning and the lack of direct access to local data, detecting and neutralizing such attacks is a significant challenge. In response to this, numerous mechanisms for robust aggregation have been proposed in the scientific literature, which aim to limit the impact of malicious updates and preserve the correctness of the global model.

4.1. Robust aggregation with plaintext gradients

When the aggregator has access to gradients in plaintext form, robust aggregation techniques are employed to mitigate the influence of malicious or anomalous clients while tolerating a limited number of Byzantine participants. These methods aim to preserve the stability and convergence of the global model despite adversarial updates. Representative approaches include distance-based schemes such as Krum and Multi-Krum [115], which select or average gradients that are closest to the majority, thereby reducing the impact of outliers, although they remain vulnerable to coordinated Sybil attacks. Statistical techniques, including Trimmed Mean and Geometric Median [116], improve robustness by removing extreme values or estimating a central tendency, at the cost of higher computational complexity. Additional protections rely on norm bounding (clipping) [59] to constrain excessively large updates, as well as Euclidean, Manhattan, or cosine similarity metrics [50], [85] to detect and down-weight suspicious gradients that deviate from the main cluster. Finally, Anti-Sybil mechanisms [117] restrict groups of overly similar independent malicious behavior but remain less effective against well-coordinated adversaries.

These approaches significantly increase the resilience of federated learning with unencrypted gradients, but their transfer to the context of encrypted data is challenging due to the need for operations such as sorting, comparison, and median, which are computationally heavy or impossible with homomorphic encryption.

4.2. Robust mechanisms over encrypted gradients

This section analyzes 21 scientific publications that present mechanisms for improving the integrity of federated learning against poisoned gradients in the context of homomorphically encrypted local updates. The studies reviewed in Table 2 seek to integrate the cryptographic confidentiality provided by homomorphic encryption with reliable strategies for protecting the global model from malicious clients capable of sending manipulated or structurally incorrect gradients. The central challenge outlined in the literature is the inability to apply traditional algorithms directly to encrypted data due to the computational limitations of homomorphic schemes. Therefore, the approaches discussed develop adapted cryptographic and statistical mechanisms that allow the detection, suppression, or compensation of harmful updates while preserving the confidentiality and integrity of the training process. The first and most extensive group includes approaches based on encrypted distance and similarity metrics, which evaluate the deviation of local updates from a reference or expected model. In a number of schemes such as [85, 89, 112], encrypted Manhattan or Euclidean distance is used, while [5, 51, 78, 86] rely on cosine similarity or correlation measures calculated directly on homomorphically encrypted texts.

The second group of approaches includes clustering and statistical methods for anomaly detection. Reference [35] uses K-means on encrypted cosine similarities, [59] integrates the DBSCAN protocol, which groups gradients based on density and direction. In [90], SNN-based clustering is applied, where the algorithm uses the density of similarity between shared nearest neighbors to identify and filter potentially malicious ones. These mechanisms use group patterns in the data to distinguish between benign and malicious updates, even when the latter are disguised by small deviations.

A third approach involves models that use cryptographic verification through zero-knowledge proofs (ZKP) and virtual environments with provable integrity. The references [19] and [41] apply ZKP to verify that local updates are calculated correctly and do not contain arbitrary values. The most rigorous version of this approach [31] uses a zero-knowledge virtual machine that executes trusted code and generates ZKP in real time for the correctness of the computations, allowing the aggregator to accept only updates with valid proofs.

Another important class of approaches aims to adapt aggregation mechanisms that are resistant to malicious client updates to a homomorphic encryption environment. Reference [55] enables algorithms such as Krum, Multi-Krum, and Median to be executed entirely on encrypted gradients through an interactive masked sorting mechanism, while [50] implements distributed Multi-Krum logic on the Paillier cryptosystem. In this way, classical robust aggregation mechanisms are adapted to work in an encrypted data environment without compromising their efficiency.

Table 2. Integrity.

Category	Method	2022	2023	2024	2025
Distance	Manhattan distance				[85, 112]
	Euclidean distance			[82]	[89, 109]
	Cosine similarity			[5, 35, 51, 78, 82]	[59, 86, 111]
Similarity	Correlation coefficient	[94]		[103]	[69, 90]
Clustering	K-means			[35]	[109, 111]
	SNN				[90]
	DBSCAN				[59],
Statistics	Average distance				[89, 109]
	Inner product				[69]
Zero-knowledge	ZKP	[19]		[41]	
	ZKVM		[31]		
Robust aggregation	Krum			[55]	
	Multi-Krum			[50]	
	Median			[55]	
	Dynamic thresholds				[85, 89, 109]
Dynamic trust	Adaptive weights	[94]		[82]	[59, 69, 112]
	Reputation			[50, 103]	[85, 86, 90, 111]
Blockchain				[50]	[59, 109, 111]
Decentralisation				[35]	
Multi-server schemes		[19, 94]		[5, 78, 103]	[59, 85, 86, 89, 112]

The next direction involves dynamic trust schemes, adaptive weighting, and participant management.

Reference [86] adapts customer weights when the model deteriorates, [82] uses a composite Q score, [112] uses a

median benchmark for adaptive weighting, [90] uses customer reputation, and [69] uses dynamic adjustment of participation probability after two-stage anomaly detection. These methods not only filter out manipulated updates, but also adapt the long-term influence of participants according to their behavior.

An important subgroup consists of architectures that use blockchain or decentralization to ensure integrity and transparency. Reference [50] implements blockchain for distributed Multi-Krum verification, while the method in [111] uses blockchain to validate encrypted updates, while [35] eliminates the central server and implements fully decentralized peer-to-peer aggregation.

Two-server and multi-server cryptographic architectures, which prevent collusion by separating roles, also make a significant contribution. The references [85, 86, 59, 103, 78] use independent servers for homomorphic comparisons, normalization, decryption, or verification. Reference [5] introduces edge and auxiliary servers with split secrets, ensuring security even with asynchronous updates.

Despite significant progress, mechanisms for resilience to encrypted poisoned gradients exhibit a number of limitations. Distance and similarity metrics rely on sensitive thresholds and can be circumvented by well-masked updates or highly heterogeneous data. Clustering methods sometimes misclassify benign clients, especially with small samples. Schemes with trusted reference models or medians assume the existence of a stable reference point, which itself can be compromised. Adaptive weights and reputation systems are susceptible to slow, gradually escalating attacks. More secure ZKP solutions guarantee correctness but introduce significant complexity and more difficult integration into real-world FL environments. Decentralized and blockchain approaches increase transparency but require additional synchronization and are vulnerable to coordinated attacks.

5. Availability and reliable aggregation

Within the CIA triad, the aspect of availability in FL is closely linked to the correct and sustainable formation of the global model. A significant threat in this context is an incorrectly aggregating central server, where the aggregator does not correctly perform the intended operations on the received encrypted updates – as a result of compromise, technical malfunction, or deliberate malicious behavior [6]. Unlike the assumption of an "honest but curious" server, here the aggregator can deliberately violate the protocol by modifying, omitting, or injecting updates, leading to systematic distortion or destabilization of the learning process. When using homomorphic encryption, this threat is further complicated because the manipulations are performed on the encrypted texts and remain difficult for clients to detect, with even minimal changes causing significant deviations in the global model, especially with heterogeneous data distribution [61].

5.1. Verifiable aggregation techniques

Modern secure aggregation schemes in FL, based on HE (Table 3), demonstrate high resistance to incorrect aggregation through a combination of cryptographic mechanisms and architectural solutions. The main principle that unites most approaches is the cryptographic "binding" between local client updates and the global aggregate. This binding ensures that any change, distortion, or partial aggregation by the central server automatically violates the verifiable equations – signature, hash, or commitment-based.

Schemes that use an external trusted verifier or a specialized central authority achieve strong control over the server. An example of this is [6], where the trusted authority performs challenge-based checks on blocks of encrypted parameters and on the aggregated model, allowing the detection of partial aggregation, result substitution, or sending different models to different clients. A similar approach is found in [17], where Pedersen commitments, verifiable secret sharing, and homomorphic signatures ensure cryptographic consistency between the submitted and aggregated gradients. In [82] and [61], verification is performed using one-way functions or homomorphic hashes, ensuring that any deviation from the actual sum is detected by the clients.

Other approaches rely on decentralized client verification, which does not rely on a trusted authority in the online phase. References [18] and [70] provide a mechanism whereby clients verify the homomorphic correspondence between the aggregated signature and the individual signatures. This prevents the server from modifying, omitting, or adding updates without the verification failing. Reference [92] extends this principle by embedding hidden information in the gradients and using a linear homomorphic hash for verification – even a minimal change in the aggregated values leads to a mismatch. Similar robustness is offered by [66], which uses Lagrange interpolation and commitment verification, allowing even differentiation between incorrect and malicious server behavior.

A significant portion of the work achieves resistance to incorrect aggregation through architectural solutions that reduce reliance on a single central node. The two-server model in [64] divides the aggregation roles so that no single server can independently skew the result without violating the verification equation. Reference [113] uses a fog-cloud architecture in which homomorphic hashes and CRT compression enable verification of the aggregate regardless of manipulation by the cloud server. Edge-oriented solutions such as [32] provide digital signing of the aggregation result, while TEE-based systems such as [91] eliminate the possibility of modifying the aggregation outside the protected hardware environment.

Modern approaches to verifiable aggregation in FL with HE offer various mechanisms for detecting malicious actions by the aggregator, but each has specific limitations. Solutions based on trusted verifiers provide high security but introduce an additional point of trust that, if compromised, invalidates the entire scheme.

Table 3. Verification mechanisms.

Category	Method	2022	2023	2024	2025
Signatures	BLS signature		[6]		[61]
	Signcryption	[18, 70]			
	DTCH		[32]		
One-way functions	DS				[92]
	HF		[6, 32]	[82]	[64, 61]
	HHF				[65, 91, 92, 113]
Commitment structures	Pedersen			[17]	
	commitment				
	Commitment				[66]
Algebraic verification	Labels				[64]
	Lagrange				
	interpolation				[66]

Client-oriented checks eliminate the need for an external authority, but often burden participants with computational costs, especially in models with a large number of parameters, with only a few solutions offering verification with constant complexity. Architectural approaches such as dual-server, fog-cloud, or TEE reduce the risk of manipulation, but require additional infrastructure and do not completely eliminate the possibility of collusion.

6. Integrated security architectures for federated learning

This section discusses integrated schemes for federated learning that simultaneously ensure confidentiality, integrity and availability of the learning process by combining homomorphic encryption with mechanisms to protect against manipulated local updates and incorrect aggregation by the central server. Unlike the approaches discussed earlier, which address threats to confidentiality, integrity, or integrity separately, this section analyzes protocols that provide comprehensive protection in accordance with the CIA triad.

The PAR-FS scheme [62] combines symmetric homomorphic encryption, statistical anomaly detection, and client-side verification of aggregated gradients. Poisoned updates are mitigated using the 2-norm distance between local gradients and the mean vector, where large deviations receive lower weights, reducing the impact of malicious clients. The system employs two servers and digital signatures, enabling clients to recompute and verify the weighted aggregation against the decrypted global model. Thus, PAR-FS both filters anomalous updates and ensures aggregation correctness.

The contract-based hierarchical scheme [72] employs a three-layer architecture (training, aggregation, and consensus), where smart contracts on a blockchain replace the trusted third party. Malicious behavior is mitigated at the consensus layer by scoring aggregation domains according to model accuracy, reducing the influence of unreliable participants. Aggregation correctness and verifiability are ensured through certificate-less aggregatable signatures (CLAS) and Paillier homomorphic encryption, with secret sharing providing robustness to dropouts. Overall, the scheme combines model quality evaluation with cryptographic mechanisms to secure and validate the aggregation process.

PPVFL [49] extends this approach by combining blockchain with homomorphic encryption. Protection against poisoned gradients relies on an honest majority and consensus mechanisms that limit the impact of malicious nodes. Verifiability is ensured through ECDSA signatures that authenticate encrypted updates and a smart contract enabling nodes to compare local and global models to detect manipulation. Aggregation is performed over encrypted parameters, while the blockchain maintains a transparent and immutable record of updates.

The decentralized reputation scheme [84] removes the central server and organizes federated learning in a peer-to-peer network with a dynamically elected leader. Byzantine resilience is achieved through a reputation system that penalizes clients whose gradients deviate from the aggregate, limiting their influence and leadership eligibility. Secure aggregation is performed using SABLE, a coordinate-truncated mean over encrypted data that reduces the effect of outliers. Verifiability is provided through zero-knowledge proofs (SNIPs, zk-SNARKs) and verifiable secret sharing, enabling the leader to prove correct aggregation and clients to validate and reconstruct the global model.

EVFL [56] targets industrial IoT settings and combines fully homomorphic encryption, BLS signatures, and adaptive gradient sparsification (AdaGS). Poisoned updates are mitigated by verifying the integrity of signed encrypted parameters before aggregation, with a trusted authority excluding manipulated contributions through signature and challenge-based checks. The same authority validates the correctness of the homomorphic aggregation and ensures consistent results across agents. AdaGS further reduces communication and computation by transmitting only significant gradient components.

Although they provide a high level of security, the approaches analyzed also have a number of significant drawbacks. PAR-FS [62] relies on Euclidean distance to the mean gradient, which assumes relatively "normal" behavior of the majority of clients and can be circumvented by adaptive, well-coordinated model poisoning attacks; Furthermore, client verification of the full weighted sum can become expensive for large models. Hierarchical and blockchain-based schemes [49, 72] are associated with a significant increase in communication costs due to the need for a consensus layer, smart contract support, and the additional latency inherent in blockchain

infrastructures. The decentralized reputation scheme [84] relies on the correct functioning of the reputation mechanism and may be sensitive to coalitions, Sybil attacks, or dynamic changes in behavior, while the use of ZKP, VSS, and SABLE increases cryptographic complexity. EVFL [56], on the other hand, obtains strong guarantees of confidentiality and verifiability, but the cost of full HE and BLS-based challenge verification remains high, requiring compensation through aggressive gradient smoothing, which can potentially affect accuracy.

7. Discussion

The systematic analysis reveals several clear trends in the evolution of homomorphic encryption-based security mechanisms for FL. First, while early studies primarily focused on confidentiality through secure aggregation and key management, recent research demonstrates a noticeable shift toward integrity and availability guarantees. In particular, the number of proposed solutions addressing poisoned gradient detection and robustness has increased significantly over the last two years of the analysed period as show in Figure 2. A similar growth is observed in approaches incorporating verifiable aggregation, including cryptographic commitments, homomorphic hashes, signatures, and zero-knowledge proofs that enable clients to validate the correctness of the server's behavior. This indicates a transition from purely privacy-preserving designs toward comprehensive trust-aware federated learning systems.

The quantitative distribution summarized in Table 2 and Table 3, and further illustrated through Figure 2, highlights this trend by showing a steady rise in integrity-oriented and verification-based mechanisms compared to earlier years. These results suggest that the research community increasingly recognizes that confidentiality alone is insufficient and that protection against malicious clients and aggregators is equally critical for real-world deployments, particularly in safety- and security-sensitive domains such as healthcare, finance, and industrial IoT.

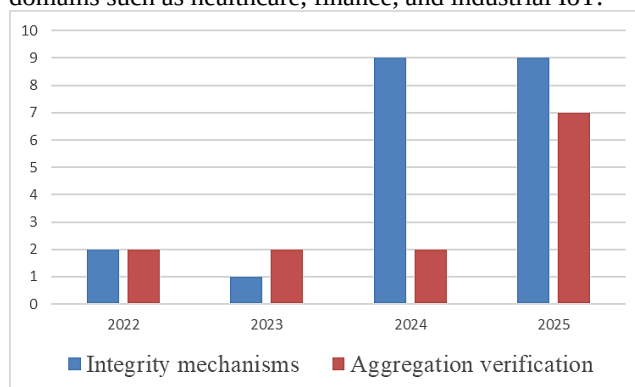


Fig 2. Number of proposed integrity and aggregation verification mechanisms in academic articles (2022–2025).

Despite this progress, the review also shows that fully integrated solutions remain limited. Only five identified models simultaneously address all three dimensions of the CIA triad – confidentiality, integrity, and availability – by combining encrypted aggregation, robustness against poisoned updates, and verifiable or decentralized aggregation protocols. This relatively small number

highlights the complexity of achieving comprehensive protection while maintaining acceptable computational and communication overhead. At the same time, it indicates a promising direction for future research. As FL systems move from experimental settings to practical applications, interest in such holistic, end-to-end secure architectures is expected to grow, motivating further work on scalable, efficient, and jointly optimized cryptographic and robustness mechanisms.

8. Conclusion

This paper presented a PRISMA-based systematic review of homomorphic encryption-enabled security mechanisms for federated learning, analysing 104 recent studies within the confidentiality–integrity–availability (CIA) framework. The results show that while early work primarily emphasized confidentiality through secure aggregation, current research increasingly targets integrity and verifiable aggregation to mitigate poisoned gradients and malicious server behaviour. Despite significant progress, only a limited number of approaches provide comprehensive protection across all CIA dimensions, highlighting the complexity of achieving end-to-end security with acceptable overhead. These findings consolidate the current state of the art and indicate that future research should focus on scalable, integrated, and practically deployable cryptographic solutions for trustworthy federated learning.

References

- [1] Konečný, J., McMahan, H. B., Yu, F. X., Richtárik, P., Suresh, A. T. & Bacon, D. (2016). Federated learning: Strategies for improving communication efficiency, *arXiv preprint*, arXiv:1610.05492, <https://arxiv.org/abs/1610.05492>.
- [2] McMahan, B., Moore, E., Ramage, D., Hampson, S. & Arcas, B. A. Y. (2017). Communication-efficient learning of deep networks from decentralized data, *Artificial Intelligence and Statistics (AISTATS)*, PMLR, pp. 1273-1282.
- [3] Zhu, L., Liu, Z. & Han, S. (2019). Deep leakage from gradients, *Proceedings of the 33rd International Conference on Neural Information Processing Systems (NeurIPS)*, Curran Associates Inc., pp. 14774-14784.
- [4] Shokri, R., Stronati, M., Song, C. & Shmatikov, V. (2017). Membership inference attacks against machine learning models, *2017 IEEE Symposium on Security and Privacy (SP)*, IEEE, pp. 3-18, <https://doi.org/10.1109/SP.2017.41>.
- [5] Zhou, A., Jiang, N. & Tang, T. (2024). Asynchronous Robust Aggregation Method with Privacy Protection for IoV Federated Learning, *World Electric Vehicle Journal*, vol. 15, no. 1, p. 18, <https://doi.org/10.3390/wevj15010018>.
- [6] Gao, H., He, N. & Gao, T. (2023). SVeriFL: Successive verifiable federated learning with privacy-preserving, *Information Sciences*, vol. 622, pp. 98-114, <https://doi.org/10.1016/j.ins.2022.11.124>.
- [7] Shalabi, E., Khedr, W., Rushdy, E. & Salah, A. (2025). A comparative study of privacy-preserving techniques in federated learning: A performance and security analysis, *Information*, vol. 16, no. 3, p. 244, <https://doi.org/10.3390/info16030244>.
- [8] Xin, W., Jiaqian, L., Xueshuang, D., Haoji, Z. & Lianshan, S. (2025). A survey of differential privacy techniques for federated learning, *IEEE Access*, vol. 13, pp. 6539-6555, <https://doi.org/10.1109/ACCESS.2024.3523909>.
- [9] Sun, H., Chen, X. & Yuan, K. (2024). FL-EASGD: Federated Learning Privacy Security Method Based on

- Homomorphic Encryption, *Computers, Materials and Continua*, vol. 79, no. 2, pp. 2361–2373, <https://doi.org/10.32604/cmc.2024.049159>.
- [10] Liu, W., Zhou, T., Chen, L., Yang, H., Han, J. & Yang, X. (2024). Round efficient privacy-preserving federated learning based on MKFHE, *Computer Standards & Interfaces*, vol. 87, Art. no. 103773, <https://doi.org/10.1016/j.csi.2023.103773>.
- [11] Zhu, B. & Niu, L. (2025). A privacy-preserving federated learning scheme with homomorphic encryption and edge computing, *Alexandria Engineering Journal*, vol. 118, pp. 11–20, <https://doi.org/10.1016/j.aej.2024.12.070>.
- [12] Aziz, R., Banerjee, S., Bouzeffrane, S. & Le Vinh, T. (2023). Exploring homomorphic encryption and differential privacy techniques towards secure federated learning paradigm, *Future Internet*, vol. 15, no. 9, p. 310, <https://doi.org/10.3390/fi15090310>.
- [13] Feretzakis, G., Papaspyridis, K., Gkoulalas-Divanis, A. & Verykios, V. S. (2024). Privacy-Preserving Techniques in Generative AI and Large Language Models: A Narrative Review, *Information*, vol. 15, no. 11, p. 697, <https://doi.org/10.3390/info15110697>.
- [14] Manzoor, H. U., Shabbir, A., Chen, A., Flynn, D. & Zoha, A. (2024). A survey of security strategies in federated learning: Defending models, data, and privacy, *Future Internet*, vol. 16, no. 10, p. 374, <https://doi.org/10.3390/fi16100374>.
- [15] Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Moher, D. (2021). *The PRISMA 2020 statement: An updated guideline for reporting systematic reviews*. *PLOS Medicine*, 18(3), e1003583. <https://doi.org/10.1371/journal.pmed.1003583>
- [16] Wei, Q. & Rao, G. (2024). EPFL-DAC: Enhancing Privacy in Federated Learning with Dynamic Aggregation and Clipping, *Computers & Security*, vol. 143, Art. no. 103911, <https://doi.org/10.1016/j.cose.2024.103911>.
- [17] Ming, Y., Wang, S., Wang, C., Liu, H., Deng, Y., Zhao, Y. & Feng, J. (2024). VCSA: Verifiable and collusion-resistant secure aggregation for federated learning using symmetric homomorphic encryption, *Journal of Systems Architecture*, vol. 156, Art. No. 103279, <https://doi.org/10.1016/j.sysarc.2024.103279>.
- [18] Du, W., Li, M., Yang, X., Wu, L. & Zhou, T. (2022). VCFL: A verifiable and collusion attack resistant privacy preserving framework for cross-silo federated learning, *Pervasive and Mobile Computing*, vol. 86, Art. no. 101697, <https://doi.org/10.1016/j.pmcj.2022.101697>.
- [19] Ma, X., Zhou, Y., Wang, L. & Miao, M. (2022). Privacy-preserving Byzantine-robust federated learning, *Computer Standards & Interfaces*, vol. 80, Art. no. 103561, <https://doi.org/10.1016/j.csi.2021.103561>.
- [20] Wibawa, F., Catak, F. O., Sarp, S. & Kuzlu, M. (2022). BFV-Based Homomorphic Encryption for Privacy-Preserving CNN Models, *Cryptography*, vol. 6, no. 3, pp. 34, <https://doi.org/10.3390/cryptography6030034>.
- [21] Kurniawan, H. & Mambo, M. (2022). Homomorphic Encryption-Based Federated Privacy Preservation for Deep Active Learning, *Entropy*, vol. 24, no. 11, pp. 1545, <https://doi.org/10.3390/e24111545>.
- [22] Xia, L., Zheng, P., Li, J., Tang, W. & Zhang, X. (2022). Privacy-preserving gradient boosting tree: Vertical federated learning for collaborative bearing fault diagnosis, *IET Collaborative Intelligent Manufacturing*, vol. 4, no. 3, pp. 208–219, <https://doi.org/10.1049/cim2.12057>.
- [23] He, D., Du, R., Zhu, S., Zhang, M., Liang, K. & Chan, S. (2022). Secure Logistic Regression for Vertical Federated Learning, *IEEE Internet Computing*, vol. 26, no. 2, pp. 61–68, <https://doi.org/10.1109/MIC.2021.3138853>.
- [24] Wu, X., Fan, Y., Zhang, J. & Gao, Z. (2023). Federated Latent Dirichlet Allocation for User Preference Mining, *Journal of Web Engineering*, vol. 22, no. 4, pp. 639–677, <https://doi.org/10.13052/jwe1540-9589.2244>.
- [25] Fontenla-Romero, O., Guijarro-Berdiñas, B., Hernández-Pereira, E. & Pérez-Sánchez, B. (2023). FedHEONN: Federated and homomorphically encrypted learning method for one-layer neural networks, *Future Generation Computer Systems*, vol. 149, pp. 200–211, <https://doi.org/10.1016/j.future.2023.07.018>.
- [26] Deng, S., Zhang, J., Li, T., Jiang, X. & Wang, F. (2023). LSBlocFL: A secure federated learning model combining blockchain and lightweight cryptographic solutions, *Computers and Electrical Engineering*, vol. 111, Part B, Art. no. 108986, <https://doi.org/10.1016/j.compeleceng.2023.108986>.
- [27] Ghavamipour, A. R., Turkmen, F., Wang, R. & Liang, K. (2023). Federated Synthetic Data Generation with Stronger Security Guarantees, in *Proceedings of the 28th ACM Symposium on Access Control Models and Technologies (SACMAT)*, ACM, pp. 31–42, <https://doi.org/10.1145/3589608.3593835>.
- [28] Xu, Y., Hu, X., Wei, J., Yang, H. & Li, K. (2023). VF-CART: A communication-efficient vertical federated framework for the CART algorithm, *Journal of King Saud University – Computer and Information Sciences*, vol. 35, no. 1, pp. 237–249, <https://doi.org/10.1016/j.jksuci.2022.11.013>.
- [29] Mohammed, M. A., Lakhan, A., Abdulkareem, K. H., Zebari, D. A., Nedoma, J., Martinek, R., Kadry, S. & Garcia-Zapirain, B. (2023). Homomorphic federated learning schemes enabled pedestrian and vehicle detection system, *Internet of Things*, vol. 23, Art. no. 100903, <https://doi.org/10.1016/j.iot.2023.100903>.
- [30] Angulo, E., Márquez, J. & Villanueva-Polanco, R. (2023). Training of Classification Models via Federated Learning and Homomorphic Encryption, *Sensors*, vol. 23, no. 4, pp. 1966, <https://doi.org/10.3390/s23041966>.
- [31] Zhang, B., Lu, G., Qiu, P., Gui, X. & Shi, Y. (2023). Advancing Federated Learning through Verifiable Computations and Homomorphic Encryption, *Entropy*, vol. 25, no. 11, pp. 1550, <https://doi.org/10.3390/e25111550>.
- [32] Zhang, J., Liu, Y., Wu, D., Lou, S., Chen, B. & Yu, S. (2023). VPFL: A verifiable privacy-preserving federated learning scheme for edge computing systems, *Digital Communications and Networks*, vol. 9, no. 4, pp. 981–989, <https://doi.org/10.1016/j.dcan.2022.05.010>.
- [33] Huang, Y., Feng, X., Wang, W., He, H., Wang, Y. & Yao, M. (2023). EFMVFL: An Efficient and Flexible Multi-party Vertical Federated Learning without a Third Party, *ACM Transactions on Knowledge Discovery from Data*, vol. 18, no. 3, pp. 1–20, <https://doi.org/10.1145/3627993>.
- [34] Wang, Z., Yu, X., Wang, H. & Xue, P. (2024). A federated learning scheme for hierarchical protection and multiple aggregation, *Computers and Electrical Engineering*, vol. 117, Art. no. 109240, <https://doi.org/10.1016/j.compeleceng.2024.109240>.
- [35] Hijazi, N. M., Aloqaily, M. & Guizani, M. (2024). Collaborative IoT learning with secure peer-to-peer federated approach, *Computer Communications*, vol. 228, Art. no. 107948, <https://doi.org/10.1016/j.comcom.2024.107948>.
- [36] Chen, B. & Ye, J. (2024). A safe parameter aggregation method under encrypted state for federated learning, *Procedia Computer Science*, vol. 247, pp. 1257–1266, <https://doi.org/10.1016/j.procs.2024.10.151>.
- [37] Truhn, D. et al. (2024). Encrypted federated learning for secure decentralized collaboration in cancer image analysis, *Medical Image Analysis*, vol. 92, Art. no. 103059, <https://doi.org/10.1016/j.media.2023.103059>.
- [38] Stripelis, D., Gupta, U., Saleem, H., Dhinagar, N., Ghai, T., Anastasiou, C., Sánchez, R., Ver Steeg, G., Ravi, S., Naveed, M., Thompson, P. M. & Ambite, J. L. (2024). A federated learning architecture for secure and private neuroimaging

- analysis, *Patterns*, vol. 5, no. 8, Art. no. 101031, <https://doi.org/10.1016/j.patter.2024.101031>.
- [39] Song, C., Wang, Z., Peng, W. & Yang, N. (2024). Secure and Efficient Federated Learning Schemes for Healthcare Systems, *Electronics*, vol. 13, no. 13, pp. 2620, <https://doi.org/10.3390/electronics13132620>.
- [40] Li, L., Sun, X., Shi, N., Ci, X. & Liang, C. (2024). A Stealthy Communication Model for Protecting Aggregated Results Integrity in Federated Learning, *Electronics*, vol. 13, no. 19, pp. 3870, <https://doi.org/10.3390/electronics13193870>.
- [41] Rao, G. R. K., Ghanimi, H. M. A., Ramachandran, V., Al-Qahtani, D., Dadheech, P. & Sengan, S. (2024). Enhanced security in federated learning by integrating homomorphic encryption for privacy-protected, collaborative model training, *Journal of Discrete Mathematical Sciences & Cryptography*, vol. 27, no. 2A, pp. 361–370, <https://doi.org/10.47974/JDMSC-1891>.
- [42] Anuvvarshini, B., Varshaa, D., Sujithra, M. & Devi, D. S. (2024). Preserving privacy in healthcare analytics: Federated learning for breast cancer prediction in a collaborative learning framework, *Grenze International Journal of Engineering and Technology*, vol. 10, no. 2, Part 4, pp. 5538–5544.
- [43] Ullah, I., Deng, X., Pei, X., Mushtaq, H. & Uzair, M. (2024). IoV-SFL: A blockchain-based federated learning framework for secure and efficient data sharing in the internet of vehicles, *Peer-to-Peer Networking and Applications*, vol. 18, Art. no. 34, pp. 1–20, <https://doi.org/10.1007/s12083-024-01821-9>.
- [44] Pan, Y., Chao, Z., He, W., Jing, Y., Li, H. & Wang, L. (2024). FedSHE: Privacy preserving and efficient federated learning with adaptive segmented CKKS homomorphic encryption, *Cybersecurity*, vol. 7, Art. no. 40, <https://doi.org/10.1186/s42400-024-00232-w>.
- [45] Shen, C., Zhang, W., Zhou, T., Zhang, Y. & Zhang, L. (2024). An efficient and secure privacy-preserving federated learning framework based on multiplicative double privacy masking, *Computers, Materials & Continua*, vol. 80, no. 3, pp. 4729–4748, <https://doi.org/10.32604/cmc.2024.054434>.
- [46] Xiong, R., Ren, W., Zhao, S., He, J., Ren, Y., Choo, K.-K. R. & Min, G. (2024). CoPiFL: A collusion-resistant and privacy-preserving federated learning crowdsourcing scheme using blockchain and homomorphic encryption, *Future Generation Computer Systems*, vol. 156, pp. 95–104, <https://doi.org/10.1016/j.future.2024.03.016>.
- [47] Tan, Z.-S., See-To, E. W. K., Lee, K.-Y., Dai, H.-N. & Wong, M.-L. (2024). Privacy-preserving federated learning for proactive maintenance of IoT-empowered multi-location smart city facilities, *Journal of Network and Computer Applications*, vol. 231, Art. no. 103996, <https://doi.org/10.1016/j.jnca.2024.103996>.
- [48] Rieyan, S. A., News, M. R. K., Rahman, A. B. M. M., Khan, S. A., Zaarif, S. T. J., Alam, M. G. R., Hassan, M. M., Ianni, M. & Fortino, G. (2024). An advanced data fabric architecture leveraging homomorphic encryption and federated learning, *Information Fusion*, vol. 102, Art. no. 102004, <https://doi.org/10.1016/j.inffus.2023.102004>.
- [49] Mahato, G., Mishra, B. K., Haldar, R., Roy, S. D. & Wang, G. (2024). A blockchain-based privacy-preserving federated learning for healthcare data sharing, *Computers in Biology and Medicine*, vol. 173, Art. no. 108268, <https://doi.org/10.1016/j.combiomed.2024.108268>.
- [50] Wang, N., Yang, W., Wang, X., Wu, L., Guan, Z., Du, X. & Guizani, M. (2024). A blockchain-based privacy-preserving federated learning scheme for Internet of Vehicles, *Digital Communications and Networks*, vol. 10, no. 1, pp. 126–134, <https://doi.org/10.1016/j.dcan.2022.05.020>.
- [51] Xu, R., Gao, S., Li, C., Joshi, J. & Li, J. (2024). Dual defense: Enhancing privacy and mitigating poisoning attacks in federated learning, *Advances in Neural Information Processing Systems*, vol. 37, pp. 70476–70498, doi: 10.52202/079017-2253.
- [52] Pais, V., Rao, S., Muniyal, B. & Yun, S. (2024). FedICU: a federated learning model for reducing the medication prescription errors in intensive care units, *Cogent Engineering*, vol. 11, no. 1, Art. no. 2301150, <https://doi.org/10.1080/23311916.2023.2301150>.
- [53] Al-Janabi, A., Al Janabi, S. & Al Khateeb, B. (2024). Healthcare privacy-preserving federated transfer learning using CKKS-based homomorphic encryption and PYHFELTool, *Iraqi Journal for Computer Science and Mathematics*, vol. 5, no. 3, Art. no. 30, <https://doi.org/10.52866/ijcsm.2024.05.03.029>.
- [54] Wang, M., Wang, Q. Y., Zhang, Y. H., Zhang, Z. X., Feng, Y. N. & Cao, Y. F. (2024). Preserving differential privacy in neural networks for foreign object detection with heterogeneity-based noising among distributed devices, *The Journal of Supercomputing*, vol. 80, pp. 21447–21474, <https://doi.org/10.1007/s11227-024-06243-1>.
- [55] Jiang, S., Yang, H., Xie, Q., Ma, C., Wang, S. & Xing, G. (2024). Lancelot: Towards efficient and privacy-preserving Byzantine-robust federated learning within fully homomorphic encryption, *arXiv preprint*, arXiv:2408.06197.
- [56] Wu, J., Wu, C., Chen, C., Jin, J. & Zhou, C. (2024). EVFL: Towards Efficient Verifiable Federated Learning via Parameter Reuse and Adaptive Sparsification, *Mathematics*, vol. 12, no. 16, pp. 2479, <https://doi.org/10.3390/math12162479>.
- [57] Wang, B. & Yang, F. (2024). Lightweight and privacy-preserving hierarchical federated learning mechanism for artificial intelligence-generated image content, *Journal of Real-Time Image Processing*, vol. 21, no. 4, pp. 1957–1973, <https://doi.org/10.1007/s11554-024-01524-7>.
- [58] Zhang, Y., Lu, Y., Liu, F., Li, C., Gong, Z., Hu, Z. & Xu, Q. (2025). Privacy-preserving and communication-efficient stochastic alternating direction method of multipliers for federated learning, *Information Sciences*, vol. 691, Art. no. 121641, <https://doi.org/10.1016/j.ins.2024.121641>.
- [59] Xiao, J., Nie, H., Yi, Z., Tang, X. & Lu, S. (2025). Federated learning with bilateral defense via blockchain, *Neural Networks*, vol. 185, Art. no. 107199, <https://doi.org/10.1016/j.neunet.2025.107199>.
- [60] He, Y., Wei, L., Chen, F., Zhang, H., Yu, J. & Wang, H. (2025). FedAI: Federated recommendation system with anonymized interactions, *Expert Systems with Applications*, vol. 271, Art. no. 126564, <https://doi.org/10.1016/j.eswa.2025.126564>.
- [61] Wang, R., Xiong, L., Geng, J., Xie, C. & Li, R. (2025). An effective and verifiable secure aggregation scheme with privacy-preserving for federated learning, *Journal of Systems Architecture*, vol. 161, Art. no. 103364, <https://doi.org/10.1016/j.sysarc.2025.103364>.
- [62] Zhang, C., Zhang, X., Yang, X., Liu, B., Zhang, Y. & Zhou, R. (2025). Poisoning attacks resilient privacy-preserving federated learning scheme based on lightweight homomorphic encryption, *Information Fusion*, vol. 121, Art. No. 103131, <https://doi.org/10.1016/j.inffus.2025.103131>.
- [63] Castro, F., Impedovo, D. & Pirlo, G. (2025). An efficient and privacy-preserving federated learning approach based on homomorphic encryption, *IEEE Open Journal of the Computer Society*, vol. 6, pp. 336–347, <https://doi.org/10.1109/OJCS.2025.3536562>.
- [64] Kang, Y., Tan, W., Fan, L., Chen, Y., Lai, X. & Weng, J. (2025). GHEFL: Grouping Based on Homomorphic Encryption Validates Federated Learning, *Future Internet*, vol. 17, no. 3, pp. 128, <https://doi.org/10.3390/fi17030128>.
- [65] Banerjee, A., Mahato, G. K. & Chakraborty, S. K. (2025). Securing FANET using federated learning through homomorphic matrix factorization, *International Journal of*

- Information Technology, vol. 17, no. 1, pp. 17–36, <https://doi.org/10.1007/s41870-024-02197-y>.
- [66] Xie, D. & Li, D. (2025). Privacy-Preserving and Verifiable Personalized Federated Learning, *Symmetry*, vol. 17, no. 3, pp. 361, <https://doi.org/10.3390/sym17030361>.
- [67] Asiri, M., Khemakhem, M. A., Alhebshi, R. M., Alsulami, B. S. & Eassa, F. E. (2025). RPFL: A reliable and privacy-preserving framework for federated learning-based IoT malware detection, *Electronics*, vol. 14, no. 6, Art. no. 1089, <https://doi.org/10.3390/electronics14061089>.
- [68] Liang, X., Xu, Y., Lin, Y., Chen, L., Zhang, Z., Wang, H. & Liu, J. (2025). Federated split learning via dynamic aggregation and homomorphic encryption on non-IID data, *The Journal of Supercomputing*, vol. 81, Art. no. 63, <https://doi.org/10.1007/s11227-024-06612-w>.
- [69] Bai, F., Zhao, Y., Shen, T., Zeng, K., Zhang, X. & Zhang, C. (2025). FedOPCS: An optimized poisoning countermeasure for non-IID federated learning with privacy-preserving stability, *Symmetry*, vol. 17, no. 5, p. 782, <https://doi.org/10.3390/sym17050782>.
- [70] Du, W. & Gao, S. (2022). A Homomorphic Signcryption-Based Privacy-Preserving Federated Learning Framework for IoT, *Security and Privacy*, Art. no. 8380239, <https://doi.org/10.1155/2022/8380239>.
- [71] Zhao, J., Huang, C., Wang, W., Xie, R., Dong, R. & Matwin, S. (2023). Local differentially private federated learning with homomorphic encryption, *The Journal of Supercomputing*, vol. 79, pp. 19365–19395, <https://doi.org/10.1007/s11227-023-05378-x>.
- [72] Wei, Q., Rao, G. & Wu, X. (2024). Contract-based hierarchical security aggregation scheme for enhancing privacy in federated learning, *Journal of Information Security and Applications*, vol. 85, Art. no. 103857, <https://doi.org/10.1016/j.jisa.2024.103857>.
- [73] Saidi, A., Amira, A. & Nouali, O. (2024). Securing decentralized federated learning: cryptographic mechanisms for privacy and trust, *Cluster Computing*, vol. 28, no. 2, <https://doi.org/10.1007/s10586-024-04957-8>.
- [74] Sav, S., Bossuat, J.-P., Troncoso-Pastoriza, J. R., Claassen, M. & Hubaux, J.-P. (2022). Privacy-preserving federated neural network learning for disease-associated cell classification, *Patterns*, vol. 3, no. 5, Art. no. 100487, <https://doi.org/10.1016/j.patter.2022.100487>.
- [75] Park, J. & Lim, H. (2022). Privacy-Preserving Federated Learning Using Homomorphic Encryption, *Applied Sciences*, vol. 12, no. 2, pp. 734, <https://doi.org/10.3390/app12020734>.
- [76] Grivet Sébert, A., Checchi, M., Stan, O., Sirdey, R. & Gouy-Pailler, C. (2023). Combining homomorphic encryption and differential privacy in federated learning, in *Proceedings of the 20th Annual International Conference on Privacy, Security and Trust (PST)*, IEEE, pp. 1–7, <https://doi.org/10.1109/PST58708.2023.10320195>.
- [77] Tian, H., Wen, Y., Zhang, F., Shao, Y. & Li, B. (2024). Lattice based distributed threshold additive homomorphic encryption with application in federated learning, *Computer Standards & Interfaces*, vol. 87, Art. no. 103765, <https://doi.org/10.1016/j.csi.2023.103765>.
- [78] Zhang, F., Huang, H., Chen, Z. & Huang, Z. (2024). Robust and privacy-preserving federated learning with distributed additive encryption against poisoning attacks, *Computer Networks*, vol. 245, Art. no. 110383, <https://doi.org/10.1016/j.comnet.2024.110383>.
- [79] Liu, Q.-X., Zhang, J.-G. & Tan, B. (2024). Financial fraud recognition model based on privacy preserving and federated learning, *Journal of Network Intelligence*, vol. 9, no. 4, pp. 2360–2374.
- [80] Mohandas, R., Veena, S., Kirubasri, G., Thusnavis Bella Mary, I. & Udayakumar, R. (2024). Federated Learning with Homomorphic Encryption for Ensuring Privacy in Medical Data, *Indian Journal of Information Sources and Services*, vol. 14, no. 2, pp. 17–23, <https://doi.org/10.51983/ijiss-2024.14.2.03>.
- [81] Shen, C., Zhang, W., Zhou, T. & Zhang, L. (2024). A security-enhanced federated learning scheme based on homomorphic encryption and secret sharing, *Mathematics*, vol. 12, no. 13, Art. no. 1993, <https://doi.org/10.3390/math12131993>.
- [82] Wang, H., Wang, Q., Ding, Y., Tang, S. & Wang, Y. (2024). Privacy-preserving federated learning based on partial low-quality data, *Journal of Cloud Computing*, vol. 13, Art. no. 62, <https://doi.org/10.1186/s13677-024-00618-8>.
- [83] Wang, H., Yang, T., Ding, Y., Tang, S. & Wang, Y. (2024). VPPFL: Verifiable privacy-preserving federated learning in cloud environment, *IEEE Access*, vol. 12, pp. 1–14, <https://doi.org/10.1109/ACCESS.2024.3472467>.
- [84] Chakraborty, O. & Boudguiga, A. (2024). A decentralized federated learning using reputation, in *Proceedings of the 10th International Conference on Information Systems Security and Privacy (ICISSP)*, SciTePress – Science and Technology Publications, pp. 799–806, <https://doi.org/10.5220/0012428300003648>.
- [85] Chen, X., Tian, Y., Wang, S., Yang, K., Zhao, W. & Xiong, J. (2025). DBFL: Dynamic Byzantine-Robust Privacy Preserving Federated Learning in Heterogeneous Data Scenario, *Information Sciences*, vol. 700, Art. No. 121849, <https://doi.org/10.1016/j.ins.2024.121849>.
- [86] Zuo, S., Xie, Y., Yao, H. & Ke, Z. (2025). TPFL: Privacy-preserving personalized federated learning mitigates model poisoning attacks, *Information Sciences*, vol. 702, Art. no. 121901, <https://doi.org/10.1016/j.ins.2025.121901>.
- [87] Cao, S., Liu, S., Yang, Y., Du, W., Zhan, Z., Wang, D. & Zhang, W. (2025). A hybrid and efficient federated learning for privacy preservation in IoT devices, *Ad Hoc Networks*, vol. 170, Art. no. 103761, <https://doi.org/10.1016/j.adhoc.2025.103761>.
- [88] Shen, R., Zhang, H., Chai, B., Wang, W., Wang, G., Yan, B. & Yu, J. (2025). BAFL-SVM: A blockchain-assisted federated learning-driven SVM framework for smart agriculture, *High-Confidence Computing*, vol. 5, Art. no. 100243, <https://doi.org/10.1016/j.hcc.2024.100243>.
- [89] Alamer, A. & Basudan, S. (2025). A Privacy-Preserving Federated Learning With a Feature of Detecting Forged and Duplicated Gradient Model in Autonomous Vehicle, *IEEE Access*, vol. 13, pp. 38484–38501, <https://doi.org/10.1109/ACCESS.2025.3545786>.
- [90] Xu, W., Xu, X. & Wang, H. (2025). Fed-HA: A Privacy-Preserving Robust Federated Learning Scheme based on Homomorphic Assessment, *Journal of Information Security and Applications*, vol. 93, Art. no. 104144, <https://doi.org/10.1016/j.jisa.2025.104144>.
- [91] Bouamama, J., Benkaouz, Y. & Ouzzif, M. (2025). V-FLEX: Verifiable cross-silo federated learning using trusted execution environment, *Progress in Artificial Intelligence*, <https://doi.org/10.1007/s13748-025-00386-9>.
- [92] Lai, P., Zhang, M., Tang, Y., Yue, Y. & Di, F. (2025). VPAFL: Verifiable Privacy-Preserving Aggregation for Federated Learning Based on Single Server, *Computers, Materials & Continua*, vol. 84, no. 2, pp. 2935–2957, <https://doi.org/10.32604/cmc.2025.065887>.
- [93] Alzahrani, B. & Yang, D. (2025). PrivHFL: A privacy-preserving scheme for hierarchical federated learning, *Computer Networks*, vol. 273, Art. no. 111764, <https://doi.org/10.1016/j.comnet.2025.111764>.
- [94] Wang, J., Xia, Z., Chen, Y., Hu, C. & Yu, F. (2022). Intrusion detection framework based on homomorphic encryption in AMI network, *Frontiers in Physics*, vol. 10, Art. no. 1102892, <https://doi.org/10.3389/fphy.2022.1102892>.
- [95] Liu, Z., Chen, S., Ye, J., Fan, J., Li, H. & Li, X. (2022). DHSAs: Efficient Doubly Homomorphic Secure Aggregation

- for Cross-silo Federated Learning, *The Journal of Supercomputing*, vol. 79, pp. 2819–2849, <https://doi.org/10.1007/s11227-022-04745-4>.
- [96] Ma, J., Naas, S.-A., Sigg, S. & Lyu, X. (2022). Privacy-preserving federated learning based on multi-key homomorphic encryption, *International Journal of Intelligent Systems*, vol. 37, no. 9, pp. 5880–5901, <https://doi.org/10.1002/int.22818>.
- [97] Chen, Q.-X., Yao, L., Wang, X., Lin Jiang, Z., Wu, Y. & Ma, T. (2022). SecMDGM: Federated Learning Security Mechanism Based on Multi-Dimensional Auctions, *Sensors*, vol. 22, no. 23, Art. no. 9434, <https://doi.org/10.3390/s22239434>.
- [98] Pham, C.-H., Huynh-The, T., Sedgh-Gooya, E., El-Bouz, M. & Alfalou, A. (2024). Extension of physical activity recognition with 3D CNN using encrypted multiple sensory data to federated learning based on multi-key homomorphic encryption, *Computer Methods and Programs in Biomedicine*, vol. 243, Art. no. 107854, <https://doi.org/10.1016/j.cmpb.2023.107854>.
- [99] Wang, B., Li, H., Guo, Y. & Wang, J. (2023). PPFLHE: A privacy-preserving federated learning scheme with homomorphic encryption for healthcare data, *Applied Soft Computing*, vol. 146, Art. no. 110677, <https://doi.org/10.1016/j.asoc.2023.110677>.
- [100] Walskaar, I., Tran, M. C. & Catak, F. O. (2023). A practical implementation of medical privacy-preserving federated learning using multi-key homomorphic encryption and Flower framework, *Cryptography*, vol. 7, no. 4, Art. no. 48, <https://doi.org/10.3390/cryptography7040048>.
- [101] Yu, X., Feng, J., Zhao, W., Yang, H. & Tang, D. (2023). Peer-to-peer privacy-preserving vertical federated learning without trusted third-party coordinator, *Peer-to-Peer Networking and Applications*, vol. 16, pp. 2242–2255, <https://doi.org/10.1007/s12083-023-01512-x>.
- [102] Li, Y., Lai, J., Zhang, R. & Sun, M. (2024). Secure and efficient multi-key aggregation for federated learning, *Information Sciences*, vol. 654, Art. no. 119830, <https://doi.org/10.1016/j.ins.2023.119830>.
- [103] Chen, D., Qu, H. & Xu, G. (2024). AegisFL: Efficient and Flexible Privacy-Preserving Byzantine-Robust Cross-silo Federated Learning, in *Proceedings of the 41st International Conference on Machine Learning (ICML)*, Proceedings of Machine Learning Research, vol. 235, pp. 7207–7219.
- [104] Shen, J., Zhao, Y., Huang, S. & Ren, Y. (2024). Secure and flexible privacy-preserving federated learning based on multi-key fully homomorphic encryption, *Electronics*, vol. 13, no. 22, Art. no. 4478, <https://doi.org/10.3390/electronics13224478>.
- [105] Pedrouzo-Ulloa, A., Boudguiga, A., Chakraborty, O., Sirdey, R., Stan, O. & Zuber, M. (2023). Practical multi-key homomorphic encryption for more flexible and efficient secure federated average aggregation, in *Proceedings of the 2023 IEEE Conference on Security and Privacy (CSR)*, pp. 1–7, <https://doi.org/10.5281/zenodo.8081556>.
- [106] Chen, Y., Wang, B., Jiang, H., Duan, P., Ping, Y. & Hong, Z. (2024). PEPFL: A framework for a practical and efficient privacy-preserving federated learning, *Digital Communications and Networks*, vol. 10, no. 2, pp. 355–368, <https://doi.org/10.1016/j.dcan.2022.05.019>.
- [107] Kumbhar, H. R. & Srinivasa Rao, S. (2025). Federated learning enabled multi-key homomorphic encryption, *Expert Systems with Applications*, vol. 268, Art. no. 126197, <https://doi.org/10.1016/j.eswa.2024.126197>.
- [108] Park, S., Lee, J., Harada, K. & Chi, J. (2025). Masking and homomorphic encryption-combined secure aggregation for privacy-preserving federated learning, *Electronics*, vol. 14, no. 1, Art. no. 177, <https://doi.org/10.3390/electronics14010177>.
- [109] Deng, Y., Guo, B. & Chen, S. (2025). Privacy-preserving approach to edge federated learning based on blockchain and fully homomorphic encryption, *Electronics*, vol. 14, no. 2, Art. no. 361, <https://doi.org/10.3390/electronics14020361>.
- [110] Bai, Y., Rao, Y., Wu, H., Wang, J., Yang, W., Xing, G., Yang, J. & Yuan, X. (2025). Using homomorphic proxy re-encryption to enhance security and privacy of federated learning-based intelligent connected vehicles, *IET Information Security*, Article ID 4632786, <https://doi.org/10.1049/ise2/4632786>.
- [111] Firdaus, M., Larasati, H. T. & Rhee, K. H. (2025). Blockchain-based federated learning with homomorphic encryption for privacy-preserving healthcare data sharing, *Internet of Things*, vol. 31, Art. no. 101579, <https://doi.org/10.1016/j.iot.2025.101579>.
- [112] Wei, Z., Wang, J., Zhao, Z. & Zhao, Z. (2025). Byzantine-robust federated learning considering distributed Non-IID data in privacy-sensitive scenarios, *Information Fusion*, vol. 124, Art. No. 103345, <https://doi.org/10.1016/j.inffus.2025.103345>.
- [113] Wang, H., Feng, J., Bu, M., Ding, Y., Tang, S. & Yang, C. (2025). MVFL: verifiable privacy-preserving federated learning using multi-key homomorphic encryption, *The Journal of Supercomputing*, vol. 81, no. 8, p. 915, <https://doi.org/10.1007/s11227-025-07419-z>.
- [114] Zhang, L., Li, C., Hu, Q., Lang, J., Huang, S., Hu, L., Leng, J., Chen, Q., & Lv, C. (2023). *Enhancing Privacy in Large Language Model with Homomorphic Encryption and Sparse Attention*. Applied Sciences, 13(24), 13146. <https://doi.org/10.3390/app132413146>.
- [115] Blanchard, P., El Mhamdi, E. M., Guerraoui, R. & Stainer, J. (2017). Machine learning with adversaries: Byzantine tolerant gradient descent, in *Proceedings of the 31st International Conference on Neural Information Processing Systems (NeurIPS)*, Curran Associates Inc., pp. 119–129.
- [116] Tukey, J. W. (1977). *Exploratory Data Analysis*, Addison-Wesley, Reading, MA, 688 p.
- [117] Fung, C., Yoon, C. J. M. & Beschastnikh, I. (2020). The limitations of federated learning in Sybil settings, in *Proceedings of the 23rd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2020)*, USENIX Association, pp. 301–316.