International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 13 Issue 5 ǁ May 2025 ǁ PP. 168-173

Enhancing the Privacy and Security in Federated Learning through Advanced Cryptographic Techniques: A Literature Review

Sheela M S[1], Ankur Khare[2] and Praveen Kumar K[3]
[1]*Research Scholar, Department of Computer Science and Information technology, Rabindranath Tagore University, Raisen, India*
[2]*Assistant Professor, Department of Computer Science and Information technology, Rabindranath Tagore University, Raisen, India*
[3]*Assistant Professor, Department of Computer Science, B S Channabasappa First Grade College, Devangere University, Devangere, India*
Corresponding Author: khareankur94@gmail.com

Abstract
Federated Learning (FL) has appeared as a paradigm swing in machine learning, empowering collaborative model exercise while preserving data privacy by custody data decentralized across devices. Though, despite its potential, FL faces important privacy and safety challenges, particularly concerning data escape, model inversion attacks, and protected aggregation. Addressing these concerns necessitates integrating advanced cryptographic techniques to improve data privacy and protected collaborative learning. This literature evaluation explores the current state of privacy-preserving methods in federated knowledge, focusing on advanced cryptographic explanations, including homomorphic encryption, secure multiparty multiplication, and differential privacy. Complete an analysis of recent educations, this review discusses the effectiveness, scalability, and computational trade-offs connected with these techniques. By consolidating visions from recent advancements, this paper goals to provide a widespread understanding of the cryptographic explanations available and identify examination gaps that could guide upcoming work toward a safer and privacy-preserving federated learning environment.
Keywords: *Cryptographic Techniques, Federated Learning, Machine Learning, Privacy, Security.*

Date of Submission: 12-05-2025 Date of acceptance: 26-05-2025

I. Introduction

Federated Learning (FL) is a regionalized machine learning framework intended to train representations across distributed data foundations without centralizing raw data. This method aligns with the increasing need for data privacy in several applications, from healthcare to economics, where regulations like GDPR petition strict data handling procedures [2]. Different traditional machine learning models that trust on aggregated datasets, FL permits training across edge devices or administrative servers, allowing respectively to retain and use its own information. However, the reorganized nature of FL introduces unique safety and privacy concerns, as allocation model updates, rather than information, remains susceptible to outbreaks. Adversaries may attempt to restructure sensitive information from model limitations, compromising individual privacy [8].

Towards address these vulnerabilities, cryptographic techniques have been assimilated into FL systems to protected the information and model parameters during and afterwards training. Homomorphic encryption permits computations on encrypted data, protected multiparty computation enables joint multiplications without data exposure, and discrepancy privacy adds controlled noise to defend individual contributions. This literature review examines the current scenery of these cryptographic techniques in amalgamated learning, analysing their usefulness in enhancing privacy and safety [15]. We aim to manufacture key findings from recent readings, assess challenges related to application and computational costs, and summary future directions to improve the toughness of federated learning outlines.

II. Literature Review

Here's a widespread explanation of the prior research papers concentrating on attractive privacy and security in federated learning (FL) concluded advanced cryptographic approaches, data quality management, blockchain incorporation, and privacy-preserving frameworks.

D. Mao et al. (2024) [3] offerings EPFed, a amalgamated learning framework planned to balance privacy with computational competence. This model leverages adaptive secrecy measures tailored to unlike data sensitivity levels, combining homomorphic encryption and protected aggregation techniques. The learning shows that EPFed meaningfully reduces computation time whereas maintaining privacy standards, offering an ascendable solution for privacy-sensitive FL presentations.

H. Wang et al. (2024) [4] speeches the confidentiality risks associated with low-quality information during FL training. They recommend a selective data-sharing procedure that prevents low-quality data from manipulating model outcomes while improving privacy by reducing data experience. The approach uses differential secrecy to mask data contributions and fractional secure aggregation to prevent extrapolation attacks on low-quality datasets.

L. Wang et al. (2024) [8] discovers a blockchain-integrated arrangement for healthcare information sharing, facilitating secure and privacy-preserving amalgamated learning with frequent documents updates. The authors propose a hybrid model by means of homomorphic encryption to protected data while permitting incremental updates and blockchain for tamper-proof information logging. This explanation addresses both the security and the real-time informing requirements of healthcare FL presentations.

S. K. M. et al. (2024) [15] determines the grouping of blockchain with associated learning for enhanced security. They examine a model that leverages cryptographic conventions within a blockchain arrangement, utilizing secure multiparty computation and zero-knowledge testimonies. This approach goals to ensure data integrity, secrecy, and auditability within federated schemes, making it suitable for use belongings that demand robust information protection and transparency.

T. Chu et al. (2024) [16] attentions on safeguarding model aggregation in associated learning. The authors propose an unconventional secure aggregation protocol that usages both homomorphic encryption and demonstrable computation techniques to safeguard against potential data leaks throughout aggregation. Their findings suggest better-quality robustness and privacy in FL, level under scenarios with confrontational participants.

Z. Alsulaimawi (2024) [20] presents an adaptive consensus-based endorsement mechanism to support model integrity in FL. The model authentication process participates consensus protocols, ensuring that individual reliable and validated model apprises are aggregated. This approach is specifically relevant for applications with strict information integrity and sanctuary requirements.

M. Gu et al. (2024) [11] recommends a original database-backed approach to track information provenance in FL schemes. By storing data lineage and typical updates in a protected database, they enhance transparency and responsibility within FL. This background uses blockchain to ensure information integrity and provenance, thereby educating traceability and model transparency.

R. Aziz et al. (2023) [12] proposals a proportional study of privacy-preserving procedures such as homomorphic encryption and difference privacy in federated learning. The dramatists explore the trade-offs amongst these techniques and provide strategies for selecting optimal methods grounded on application-specific needs, such as correctness, computational load, and privacy glassy.

A. Alazab et al. (2023) [1] explores the usage of FL for privacy-preserving imposition detection. It combines joined averaging with differential privacy to protected data while training models crossways distributed sources. The authors determine that this approach can improve cybersecurity by enabling cooperative model training without exposing complex network data.

H. Zhang et al. (2023) [5] recommends a hybrid FL outline combining local information processing with privacy-preserving model apprises. Using homomorphic encryption and discrepancy privacy, the framework is calculated for secure collaboration between financial institutions. The study designates that this approach improves the sturdiness of FL models in racket detection without compromising client information privacy.

J. Ma et al. (2023) [6] suggests a split-learning technique utilizing functional encryption to protected intermediate computations in FL. This method addresses secrecy concerns related to split education, where intermediate layers are communicated between clients and servers. PPSFL demonstrations potential for applications necessitating both strong privacy and inferior computational demands.

B. Zhang et al. (2023) [2] recommend an FL organization that incorporates demonstrable computation to enhance trust in perfect updates. This approach powers homomorphic encryption to secure information during computation and verifiable subtraction to ensure result integrity, which is important for applications with strict audit and compliance necessities.

J. Park et al. (2022) [7] discovers the usage of homomorphic encryption to safeguard model updates in FL. The reading finds that this method can effectively secure FL systems deprived of significant computational above, making it a practical option for industries like economics and healthcare where data sensitivity is extraordinary.

R. Xu et al. (2021) [13] presents FedV, a agenda for FL completed vertically partitioned datasets. This learning focuses on scenarios where information from multiple sources needs to be shared for training. By means of secure multiparty computation, FedV empowers secure FL while preventing information leaks between sources, which is model for cases where information ownership is split.

X. Zhang et al. (2021) [19] converses hybrid FL procedures combining local and dominant computations to balance secrecy, communication efficiency, and model correctness. Their implementation highlights the adaptableness of hybrid FL systems in numerous scenarios, including healthcare and sponsorship, where information privacy is paramount.

W. Ou et al. (2020) [18] offerings a perpendicular FL model using homomorphic encryption for information privacy in danger management applications. This learning shows that using homomorphic encryption empowers accurate collaborative training while protective each participant's data, lecturing privacy concerns in sensitive requests like insurance and credit danger assessment.

S. Truex et al. (2019) [14] propositions a hybrid FL method that associations homomorphic encryption and differential secrecy to secure collaborative learning. This explanation balances privacy with computational competence, allowing FL to measure across larger and more heterogeneous atmospheres.

T. Li et al. (2019) [17] A complete impression of FL challenges and probable solutions, including privacy and sanctuary issues. The authors identify encryption methods, secure aggregation, and discrepancy privacy as promising avenues for ornamental FL.

L. T. Phong et al. (2018) [9] presents homomorphic encryption for protected deep knowledge. This technique enables computations on encrypted information, significantly improving concealment in distributed learning environments without exposing sensitive information.

M. A. Rubaie et al. (2018) [10] scrutinizes numerous threats to privacy in machine learning and recommends solutions comparable homomorphic encryption and differential secrecy. The paper highlights the significance of these techniques for amalgamated learning, offering foundational insights hooked on privacy-preserving methods. These papers collectively discourse the primary challenges in federated knowledge, proposing cryptographic techniques, hybrid representations, blockchain integration, and protected aggregation to enhance data secrecy and model security across a choice of applications from healthcare to investment and intrusion discovery.

Here's a complete table summarizing the projected methodologies, performance parameters, advantages, and boundaries of prior papers on attractive privacy and sanctuary in federated learning:

Table 1: Comprehensive Review

Authors	Proposed Methodology	Performance Parameters	Advantages	Limitations
D. Mao et al. (2024) [3]	EPFed, a privacy-preserving FL perfect harmonizing privacy and efficiency using homomorphic encryption and protected aggregation	Secrecy, computation time, efficiency	Reduces multiplication time while enhancing secrecy for sensitive data	May necessity tuning for different application wants
H. Wang et al. (2024) [4]	Discriminatory data-sharing with differential privacy and partial protected aggregation for low-quality information	Information quality, privacy level, efficiency	Progresses privacy by reducing exposure of low-quality documents	Potential for correctness loss with incomplete information
L. Wang et al. (2024) [8]	Blockchain-integrated healthcare information sharing with homomorphic encryption for incremental informs	Data honesty, update efficiency	Real-time informs and tamper-proof logging for sensitive healthcare information	High computational capacity for frequent informs
S. K. M. et al. (2024) [15]	Blockchain-based FL expending secure multiparty computation and zero-knowledge testimonies	Information integrity, transparency, privacy	Ensures information integrity and privacy in FL, with auditability	Difficulty of cryptographic protocols can influence scalability
T. Chu et al. (2024) [16]	Progressive secure aggregation protocol with homomorphic encryption for healthy privacy	Secrecy, robustness, computation time	Improved robustness against adversarial participants	May have imperfect efficiency for resource-constrained strategies
Z. Alsulaimawi (2024) [20]	Adaptive consensus-based authentication for secure model inform in FL	Model integrity, reliability, safety	Advances model reliability through consensus-based proof	Incomplete effectiveness if consensus protocol expressions delays
M. Gu et al. (2024) [11]	Database-backed method for tracking data attribution in FL, integrating blockchain for protected logging	Pellucidity, data integrity, auditability	Enhances information transparency and model liability in FL	High packing overhead and potential performance interval
R. Aziz et al. (2023) [12]	Comparative learning of homomorphic encryption and differential secrecy for secure FL	Privacy, correctness, computational trade-offs	Offers visions into trade-offs, aiding optimal method collection	May deficiency depth in specific technique application
A. Alazab et al. (2023) [1]	Federated knowledge for intrusion detection with differential secrecy and federated be around	Privacy, uncovering accuracy, efficiency	Empowers privacy-preserving intrusion detection without exposing network information	Probable reduction in model accuracy due to noise calculation

Authors	Proposed Methodology	Performance Parameters	Advantages	Limitations
H. Zhang et al. (2023) [5]	Hybrid FL outline using homomorphic encryption and discrepancy privacy for economic crime detection	Safety, fraud detection accuracy	Strong discretion for financial data and upgraded fraud detection	Computational difficulties increase with information complexity
J. Ma et al. (2023) [6]	Split FL expending functional encryption to protected intermediate computations	Secrecy, computational efficiency	Decreases computational demands while preserving privacy of halfway data	Limited applicability to huge datasets or high-dimensional information
B. Zhang et al. (2023) [2]	Demonstrable computation in FL using homomorphic encryption to safeguard data integrity	Documents integrity, privacy, trustworthiness	Safeguards integrity and privacy in critical requests requiring high trust	Great computational and storage overhead for verifying informs
J. Park and H. Lim (2022) [7]	Privacy-preserving FL expending homomorphic encryption	Secrecy, computation time, scalability	Offers secrecy with minimal computation above for sensitive applications	May necessitate fine-tuning for different FL jobs
R. Xu et al. (2021) [13]	FedV, privacy-preserving FL finished vertically segregated data with secure multiparty calculation	Secrecy, data partitioning efficiency	Facilitates protected data usage across numerous sources without leaks	Presentation lag due to secure cooperative computations
X. Zhang et al. (2021) [19]	Hybrid FL procedure combining local and dominant computation for privacy and efficacy	Secrecy, efficiency, model accuracy	Equilibria privacy with computational efficiency in distributed knowledge	Incomplete scalability in data-intensive applications
W. Ou et al. (2020) [18]	Perpendicular FL with homomorphic encryption for threat management	Privacy, information sharing security, efficiency	Enables safe risk assessment while protecting sensitive information	High addition cost due to encryption conventions
S. Truex et al. (2019) [14]	Hybrid privacy-preserving FL by means of homomorphic encryption and differential secrecy	Secrecy, computational efficiency	Climbable across large, heterogeneous environments	Difficulty in balancing privacy levels across distributed bulges
T. Li et al. (2019) [17]	Overview of FL tasks, proposing encryption methods and secure aggregation	Secrecy, FL challenges, future potential	Delivers foundational understanding of FL tests and solutions	Deficiencies implementation specifics on encryption methods
L. T. Phong et al. (2018) [9]	Privacy-preserving deep learning expending additively homomorphic encryption Privacy	Secrecy, computation on encrypted data	Consents computations on encrypted data, enhancing secrecy in deep learning	High computational necessities for secure additions
M. A. Rubaie et al. (2018) [10]	Examination of threats and solutions for secrecy in ML, including homomorphic encryption and difference privacy	Threats, secrecy solutions, accuracy	Delivers baseline security measures, relevant for numerous FL applications	Broad impression, may lack depth in technique-specific applications

Here are about key research gaps and their solutions recognized across these papers on privacy-preserving amalgamated learning and cryptographic methods:

1. **Scalability in Cryptographic Techniques**: Progressive cryptographic methods like homomorphic encryption and protected multiparty computation suggestively increase computation and communication exceeding, which limits scalability in real-world amalgamated learning applications, especially with huge data sizes or great numbers of participants. Future examination could explore lightweight cryptographic procedures that minimize resource consumption while preserving secrecy [7].

Solution: Progress hybrid encryption schemes merging homomorphic encryption with differential secrecy or approximate computation methods. For model, implementing partial homomorphic encryption proceeding critical model parameters and discrepancy privacy on non-critical information could lower computation needs. Discover quantization and model thinning techniques to reduce the computational capacity associated with secure cooperative computation and homomorphic encryption.

2. **Data Quality and Heterogeneity Management**: Management partial or low-quality data in merged learning remains an open question. As identified in [8], merged knowledge models tend to underperform in heterogeneous information settings, indicating the necessity for adaptive algorithms that continue model accuracy despite varying information quality.

Solution: Present federated learning algorithms that correct to data quality alterations, such as weighted federated be around, which gives higher weights to dependable, high-quality data sources. Usage transfer learning-based models that can study from partial or low-quality information by leveraging information from high-quality datasets without straight data sharing.

3. **Incorporation of Real-time Data Updates**: Assimilating real-time data updates into amalgamated learning frameworks while ensuring records privacy and maintaining model steadiness remains challenging. The healthcare data-sharing arrangement by [8], highpoints the potential of incremental informs but lacks support for real-time information without compromising privacy.

Solution: Instrument asynchronous federated learning models that provision staggered or real-time informs, allowing each participant to sleeper on real-time data watercourses independently before secure aggregation. Participate lightweight consensus mechanisms similar to empower faster real-time model updates while custody data private and dipping latency.

4. **Blockchain Integration Limitations**: Though blockchain enhances data transparency and immutability in merged learning, present blockchain-based privacy-preserving solutions, such as persons proposed [15], are regularly constrained by high computational prices and latency issues. More investigation is needed to progress efficient consensus mechanisms that canister support federated learning at scale.

Solution: Usage Multi-Layer scaling solutions, such as sidechains, to decrease the freight on main blockchain networks, by this means improving effectiveness and reducing latency. Present sharding-based techniques within blockchain-integrated amalgamated learning to handle the measure of distributed data and provision parallel transaction processing.

5. **Attack Resistance in Privacy-preserving Aggregation**: Protected aggregation techniques protect data after unauthorized access but often continue vulnerable to adversarial attacks, such as perfect poisoning. Methods, similar the secure aggregation framework conversed by [16], necessitate enhancements to counter such confrontational manipulations while maintaining privacy.

Solution: Progress federated learning models that comprise robust aggregation techniques identical Krum or Bulyan, which decrease the influence of outlier informs, mitigating the impact of adversarial outbreaks. Usage anomaly detection algorithms that pennant unusual model updates, thereby noticing potential model poisoning challenges and allowing for more safe aggregation.

6. **Adaptive Consensus Mechanisms**: Prevailing adaptive consensus-based approaches [20], principally focus on the correctness of informs rather than the strength of consensus in highly distributed atmospheres. There is a gap in manipulative consensus models that can energetically adjust to moving network conditions and participant behaviour's.

Solution: Generate adaptive consensus algorithms that highlight nodes based on their standing or accuracy scores, attractive the consensus process's resilience to vacillations in network conditions and malicious performers. Device a dynamic consensus model anywhere consensus requirements adjust grounded on network size and dependability, optimizing resource use while preserving system integrity.

7. **Transparent Data Provenance Tracking**: As confirmed [11], tracking information provenance and ensuring classical transparency are essential for hope in federated learning. However, information provenance techniques often introduce noteworthy complexity. Future studies could attention on simplifying provenance tracking instruments while maintaining model transparency.

Solution: Usage blockchain-based provenance solutions with Merkle tree constructions to track classical update history efficiently deprived of bloating the blockchain. Progress lightweight, distributed provenance-tracking schemes that leverage Zero-Knowledge Proofs (ZKPs) for improved transparency and low complication.

8. **Limited Usability of Homomorphic Encryption**: Notwithstanding its strong privacy-preserving capabilities, homomorphic encode, such as that used in trainings [7, 12], is computationally challenging and unsuitable aimed at resource-constrained devices. Research could discover hybrid techniques that association partial encryption with lightweight secrecy methods to support constrained devices.

Solution: Usage homomorphic encryption selectively for complex data attributes, while smearing differential privacy to other information, reducing the computational overhead while upholding a balance of privacy and safety. Assimilate a federated model split, everywhere local device computations minimize information exposure, sending only detailed encrypted attributes for aggregation to decrease device-side computational demand.

9. **Interoperability across Distributed Environments**: Several current federated learning frameworks scrap with cross-environment interoperability, particularly in cloud or multi-cloud situations. Equally noted in frameworks like persons [13], attaining privacy-preserving interoperability that respects information residency and regulatory requirements remainders an open area for innovation.

Solution: Service federated architecture that provisions multi-cloud and edge environments, expending containerization and APIs to simplify cross-platform data compatibility while protecting information privacy. Improve privacy-preserving federated learning middleware by built-in support for different information formats and encryption ideals across platforms, enhancing interoperability without compromising information protection.

10. **Limited Exploration of Hybrid Approaches**: Hybrid federated studying models, which syndicate multiple cryptographic and non-cryptographic secrecy techniques, are relatively underexplored. Trainings [2, 5], recommend the effectiveness of hybrid methods then highlight the need for wide-ranging frameworks that balance numerous privacy techniques with computational efficacy.

Solution: Progress an integrated framework that association's homomorphic encryption with difference privacy, creating hybrid protocols that apply multi-layered secrecy protections according to information sensitivity. Contrivance federated learning algorithms that apply adaptive hybrid methods, permitting the system to switch

amongst different privacy techniques (e.g., converting from differential privacy to protected aggregation) based on real-time supply availability and model requirements.
These solutions can guide future research in making a more secure, ascendable, and efficient federated instruction ecosystem.

III. Conclusion and Future Work

This literature review has explained the evolving scenery of privacy and sanctuary in Federated Learning (FL), importance advanced cryptographic techniques that address key susceptibilities in data secrecy and secure model aggregation. Homomorphic encryption, protected multiparty computation, and difference privacy have emerged as dangerous solutions, each offering exceptional benefits and challenges. While these cryptographic approaches have demonstrated efficiency in enhancing data security and minimalizing leakage, they often present computational overheads and scalability restrictions, which may limit their applied application in resource-constrained environments. Despite these tasks, advancements in cryptography remain to strengthen FL's aptitude to resist threats such as information leakage and model overturn attacks, making collaborative learning more safe and private. This evaluation consolidates the effectiveness of present approaches, identifies gaps in real-world scalability, and highlights the necessity for optimizing cryptographic techniques to address FL's safety needs deprived of compromising efficiency. Future investigation should focus on developing adaptive and frivolous cryptographic solutions that can encounter the scalability stresses of diverse FL applications, pavement the way toward a healthy and resilient federated learning system.

References

[1]. A. Alazab, A. Khraisat, S. Singh and T. Jan, "Enhancing Privacy Preserving Intrusion Detection through Federated Learning", Electronics, MDPI, Vol. 12 (3382), pp. 1-16, 2023.
[2]. B. Zhang, G. Lu, P. Qiu, X. Gui and Y. Shi, "Advancing Federated Learning through Verifiable Computations and Homomorphic Encryption", Entropy, MDPI, Vol. 25 (1550), pp. 1-15, 2023.
[3]. D. Mao, Q. Yang, H. Wang, Z. Chen, C. Li, Y. Song and Z. Qin, "EPFed: Achieving Optimal Balance between Privacy and Efficiency in Federated Learning", Electronics, MDPI, Vol. 13 (1028), pp. 1-18, 2024.
[4]. H. Wang, Q. Wang, Y. Ding, S. Tang and Y. Wang, "Privacy-preserving Federated Learning based on Partial Low-Quality Data", Journal of Cloud Computing: Advances, Systems and Applications, Vol. 13 (62), pp. 1-16, 2024.
[5]. H. Zhang, J. Hong, F. Dong, S. Drew, L. Xue and J. Zhou, "A Privacy Preserving Hybrid Federated Learning Framework for Financial Crime Detection", cs.LG, pp. 1-10, 2023.
[6]. J. Ma, X. Lyu, Y. Yu and S. Sigg, "PPSFL: Privacy Preserving Split Federated Learning via Functional Encryption", Journal of Latex Class Files, Vol. 14 (8), pp. 1-12, 2023.
[7]. J. Park and H. Lim, "Privacy Preserving Federated Learning using Homomorphic Encryption", Applied Sciences, MDPI, Vol. 12 (734), pp. 1-17, 2022.
[8]. L. Wang, X. Liu, W. Shao, C. Guan, Q. Huang, S. Xu and S. Zhang, "A Blockchain based Privacy Preserving Healthcare Data Sharing Scheme for Incremental Updates", Symmetry, MDPI, Vol. 16 (89), pp. 1-17, 2024.
[9]. L. T. Phong, Y. Aono, T. Hayashi, L. Wang and S. Moriai, "Privacy Preserving Deep Learning via Additively Homomorphic Encryption", IEEE Transactions on Information Forensics and Security, Vol. 13 (5), pp. 1333-1345, 2018.
[10]. M. A. Rubaie and J. M. Chang, "Privacy Preserving Machine Learning: Threats and Solutions", IEEE Security and Privacy Magazine, pp. 1-18, 2018.
[11]. M. Gu, R. Naraparaju and D. Zhao, "Enhancing Data Provenance and Model Transparency in Federated Learning Systems - A Database Approach", cs.CR, pp. 1-14, 2024.
[12]. R. Aziz, S. Banerjee, S. Bouzefrane and T. L. Vinh, "Exploring Homomorphic Encryption and Differential Privacy Techniques towards Secure Federated Learning Paradigm", Future Internet, MDPI, Vol. 15 (310), pp. 1-25, 2023.
[13]. R. Xu, N. Baracaldo, Y. Zhou, A. Anwar, J. Joshi and H. Ludwig, "FedV: Privacy Preserving Federated Learning over Vertically Partitioned Data, cs.LG, pp. 1-16, 2021.
[14]. S. Truex, N. Baracaldo, A. Anwar, T. Steinke, H. Ludwig, R. Zhang and Y. Zhou, "A Hybrid Approach to Privacy Preserving Federated Learning", cs.LG, pp. 1-11, 2019.
[15]. S. K. M., S. Nicolazzo, M. Arazzi, A. Nocera, R. R. K. A., V. P. and M. Conti, "Privacy Preserving in Blockchain based Federated Learning Systems", cs.CR, pp. 1-44, 2024.
[16]. T. Chu, D. Isler and N. Laoutaris, "Strengthening Privacy in Robust Federated Learning through Secure Aggregation", Workshop on AI Systems with Confidential Computing (AISCC), pp. 1-6, 2024.
[17]. T. Li, A. K. Sahu, A. Talwalkar and V. Smith, "Federated Learning: Challenges, Methods and Future Directions", cs.LG, pp. 1-21, 2019.
[18]. W. Ou, J. Zeng, Z. Guo, W. Yan, D. Liu and S. Fuentes, "A Homomorphic Encryption based Vertical Federated Learning Scheme for Rick Management", Computer Science and Information Systems, Vol 17 (3), pp. 819-834, 2020.
[19]. X. Zhang, W. Yin, M. Hong and T. Chen, "Hybrid Federated Learning: Algorithms and Implementation", cs.LG, pp. 1-8, 2021.
[20]. Z. Alsulaimawi, "Enhancing Security in Federated Learning through Adaptive Consensus based Model Update Validation", cs.CR, pp. 1-9, 2024.