THE ASIAN BULLETIN OF BIG DATA MANAGMENT
Vol. 6. Issue 1 (2026)
https://doi.org/10.62019/5t3k4c10

An Efficient Approach for Security and Privacy Preserving based on Machine Learning and Federated Learning (FL): Analysis and Performance Optimization for Secure Multiparty Computing

Ammar Ahmed, Amna Saleem Sheikh, Nasir Ayub, Umair Ghafoor, Asfar Ali, Hamayun Khan,

Chronicle

Article history
Received: Feb 15, 2026
Received in the revised format: March 10. 2026
Accepted: March 20, 2026
Available online March 28, 2026

Ammar Ahmed* & **Hamayun Khan** is currently affiliated with the Faculty of Computer Science & IT Superior University Lahore, 54000, Pakistan.
Email:ammarahmed9917@gmail.com
Email: hamayun.khan@superior.edu.pk

Amna Saleem Sheikh is currently affiliated with the Department of Computer Science, Forman Christian College, University, Lahore, Pakistan.
Email:
281134184@formanite.fccollege.edu.pk

Nasir Ayub and Umair Ghafoor is currently affiliated as Deputy Head of Engineering at Calrom Limited, M1 6EG, United Kingdom
Email: nasir.ayyub@hotmail.com
Email: umairghafoor@hotmail.com

Asfar Ali is currently affiliated with the Information Technology Department of LHC, and with the Department of Information Technology, Superior University Lahore, 54000, Pakistan.
Email: asfarali761@gmail.com

Abstract

Federated Learning (FL) is an approach that allows numerous users to train a single machine learning model with the oversight of a central server, and with their training data stored locally on their devices. The approach is relevant in alleviating the risks associated with violations in data privacy. It is a process by which a pool of clients collaborates towards solving machine learning problems, with a central coordinator being the one who coordinates the entire process. The paper will review the latest advances in privacy-preserving federated learning and discuss it in the context of machine learning. It assesses privacy-related solutions, which are already in existence, such as secure aggregation, meta-learning, blockchain technology, decentralized training, searchable encryption, and data privacy mechanisms and zero-knowledge proofs. Federated learning (FL) is an emerging technology that can be used in the realm of the intelligence of the Internet of Things. However, the information that is model-related can be shared in FL and reveal the sensitive data of the participants. In this regard, we propose a new privacy-preserving FL framework, which is founded on a new chained secure multiparty computing technique, which we call chain-PPFL. The scheme we are proposing is based mostly on two mechanisms: 1) a single-masking mechanism, which protects the information that is exchanged between participants in a serial chain frame and 2) a chained-communication mechanism, which allows the masked information to be communicated between participants in a serial chain frame. We run large-scale experiments with respect to simulation by comparing the training accuracy and the leak defence to other state-of-the-art schemes with two publicly available data sets (MNIST and CIFAR-100). We established data sample distributions (IID and NonIID), and training models (CNN, MLP and L-BFGS) in our experiments. The experiment results show that the chain-PPFL scheme can offer a realistic privacy preservation (which is the same as the various privacy with ϵ to near zero) to FL at the cost of communication, and without compromising the accuracy and convergence rate of the training model.

Corresponding Author*

Keywords: Machine Learning, Collaborative Learning, Zero Knowledge Proofs, Blockchain Technology, Decentralized Learning, Federated Averaging.

INTRODUCTION

Federated Learning has become a leading paradigm for collaboratively training models across distributed data sources while maintaining data confidentiality. It is a decentralized type of machine learning where the models are trained together on many machines or servers, each having its local dataset [1]. The current paper reviews the recent advances in privacy-aware methods used in federated learning and their implication in machine learning. It explores the privacy-sensitive methods, such as Differential Privacy (DP), Secure Multi-Party Computation (SMPC), Homomorphic

Encryption (HE), and federated learning with encrypted data. This will reduce the fears of unauthorized access to data and privacy violations [2, 3]. Federated Learning is privacy assured, and through it, different parties can collaborate securely in even areas like finance and telecommunication. In addition, the privacy protection in federated learning promotes user confidence, leading to increased involvement and cooperation in the federated ecosystems [4, 5]. Homomorphic Encryption (HE) is a powerful cryptographic method that enables computing with encrypted data, and the confidentiality is maintained even during the processing stage [6]. Despite these advantages, Federated Learning is faced with a number of challenges that include expensive communication, unequal local data, and susceptibility to adversarial attacks. Suppose that there are several clients, n, {P1, P2., Pn) and that raw data I1, I2 are data possessed by a client.

The primary benefit of FL is that it ensures privacy because all sensitive data is stored locally in users' devices [7, 8]. However, Federated Learning continues to be vulnerable to privacy threats. Training may lead to the accidental leakage of sensitive information when model updates are sent, therefore, requiring more privacy-sensitive training systems [9]. The purpose of this paper is to discuss the existing strategies and emerging trends to strengthen privacy in federated learning. In this paper, various privacy-enhancing techniques in FL will be taken into account, such as Differential Privacy, which adds random noise to model updates to obscure the effect of individual data, and Secure Multi-Party Computation, which allows joint computation without exchanging personal inputs. Similarly, the Homomorphic Encryption also provides an additional security as it enables the processing of encrypted data, thus ensuring confidentiality at any stage of the calculations [9].

Federated Learning is vulnerable to privacy-related vulnerabilities, despite these techniques. Model parameters can be sent during training, so the personal information can be disclosed unknowingly; this is why the high-sophistication privacy-preserving solutions are significant [10, 11]. As the new uses of FL continue to grow, including medical, financial, and IoT, the need to have powerful and reliable privacy controls is more urgent than ever. This review includes a comprehensive discussion of the current state of privacy-saving approaches in FL, categorizing and comparing the merits and demerits of each approach. The study will contribute to enlightening scholars and practitioners as it will determine the existing trends and the gaps in the research to come up with more secure and efficient FL systems [12]. This review bridges the gap between theory and practice, since, through a detailed discussion of the possible strategies and their applications, one can safely apply FL to sensitive data environments. Lastly, the work is among the main sources that promote the advances of privacy-preserving federated learning [13].

Protecting privacy through multi-party machine learning allows participants to learn on the data of other participants, and do so in a fashion that does not in any way identify their own data set [14, 15]. This plan has offered immense learning performance, which is beneficial to the clients and their sensitive details are secured and monitored, especially in a place that is likely to be hacked [16].

Important privacy-preserving mechanisms of federated learning are identified in Table 1, and their assurances, threats mitigation, computational requirements, communication requirements, impact on model performance, and scalability are compared. Different Privacy (DP) secures the information of clients by introducing controlled noise to the gradients or updates that minimize the risk of disclosing the personal information. It is principally resistant to membership inference and partial

reconstruction attacks. On one hand, DP is characterised by low to moderate computational cost, namely, gradient clipping, noise addition, and on the other hand, low communication cost, namely, no significant change in message sizes. Higher privacy rates can decrease the accuracy of the model, yet DP is very scalable and can be used by large clients. Secure Multi-Party Computation (SMPC) allows several parties to perform the computation of model updates together without sharing their data.

Table 1.
Comparative Analysis of Existing Privacy-Preserving Techniques in Federated Learning

Technique	Privacy guarantee	Threats covered	Computational cost (client/server)	Communication overhead	Impact on model utility	Scalability	Maturity
Differential Privacy (DP)	Introduces controlled noise into gradients or updates to restrict information disclosure.	Protects against membership inference and limited data reconstruction attacks.	Low to moderate due to gradient clipping and noise addition.	Low	Medium tighter privacy budgets generally reduce accuracy.	High	High-widely studied & applied.
Secure Multi-Party Computation (SMPC)	Cryptographic techniques apply to jointly compute results without revealing individual data.	Prevents exposure of raw updates under honest-but-curious threat models.	High, involving secret sharing and intensive cryptographic computations.	High.	Minimal effects since aggregation remain exact.	Moderate.	Moderate - proven but heavy.
Homomorphic Encryption (HE)	Keeps updates encrypted while enabling computation directly on encrypted data.	Prevents strong protection against an untrusted or curious server.	Extremely high due to encryption, decryption, and homomorphic operations.	Extremely high	Low impact overall, though approximations may be needed for complex models.	Good	Moderate -active research; improving but costly.
Secure Aggregation (SA)	Ensure that only the combined model update is visible to the server.	Guards against leakage of individual client contributions.	Moderate, relying on masking techniques.	Moderate	Very low; exact aggregation preserves model accuracy.	High	High-adopted in practice (Google, etc.).

It defends against honest-but-curious servers that want to access raw updates. Computationally intensive (as cryptographic operations) SMPC and communication is also costly in terms of extra interaction rounds. Aggregation is accurate, but model performance does not change much, as scaling to a large number of participants is more complicated and consumes more resources. Homomorphic Encryption (HE) is highly confidential, with the capability to make calculations with encrypted updates and, therefore, the server can not have access to raw data. This is extremely computationally expensive, necessitating encryption, decryption and homomorphic operations, and much more expensive in communications as ciphertexts are huge. Mostly, it preserves model utility, but complicated calculations might need approximations. HE can serve a large number of clients and deal with dropouts, thus it is moderately scalable even with its resource intensity. Secure Aggregation (SA) enables the server to accept only the result of the aggregation of the client updates, and does not reveal the individual information. It is computationally moderate and requires extra communication steps due to masking and cryptographic activities. Due to the precision of aggregation, the accuracy of the model is not determined to a

greater extent. SA is very scalable, and its effectiveness and feasibility render it an everyday application in large-scale federated learning.

It is aggregated at a small number of hierarchical levels, which reduces the level of communication overhead, as well. They are individually added to the data details of every client and, thus, individual updates are guaranteed. Secure Multi-Party Computation (SMPC) helps to perform operations on confidential data by more than two parties without disclosing it, thereby maintaining confidentiality in aggregating model updates in FL [17,18]. Homomorphic Encryption (HE) is a cryptographic method whereby the calculations are executed on encrypted data, known as ciphertext, to produce encrypted data, which on decryption would produce the same results as the calculations run on the unprotected data, also known as plaintext [19, 20]. In Federated Learning, every client encrypts his/her local model with HE, enabling the central aggregator to perform the computations without having ever seen the actual model parameters [21, 22]. In the recent past, the development of computational hardware and data acquisition methods has greatly increased the performance of machine learning, increasing its effectiveness as well as its applications in the real world [23]. Federated Learning is a rather new technology originally suggested by Google.

Google aimed to create machine learning models using data shared among various devices and reduce the chances of data leakage. The most recent developments in Federated Learning have concerned addressing both statistical issues [24, 25]. Research on how federated learning models can be tailored to the requirements of individual clients has also been done. FL reduces the privacy risk and solves the data silo problem by decentralizing the training procedure and by doing the computations locally on the data source. This structure ensures that its source has sensitive information [26-31]. FL will also implement contemporary privacy-preserving techniques to offer an extra measure of security on information when updating and aggregating models, such as Homomorphic Encryption, Differential Privacy and Secure Multi-Party Computation [32- 35]. Currently, research on Federated Learning technology is evolving and being enhanced. As per the existing literature, FL research is faced with three major challenges, which include threats to privacy and security, heterogeneity of data amongst participants, and high communication overheads [36]. Although it has made some advancements, FL is still susceptible to parameter leaks and malicious attacks against the update process of the model [37].

Federated Learning is still developing, which allows using it in the most diverse ways, and it aims to address the current challenges. The recent use of FL methods has gained a lot of popularity in various applications, including intelligent healthcare [38], recommendation systems, smart cities, financial and insurance, edge computing [39] and intrusion detection systems. Formally, n number of clients {P1, P2., Pn} want to calculate a global function f {I1, I2., In} from their individual datasets. A protocol is said to be SMPC when it satisfies the conditions in [40]): (i) the function f{I1, I2., In} is correct, and (ii) no personal information of In is revealed to the other participants. Machine Learning has been getting more and more significant with the rapid evolution and popularization of artificial intelligence. Machine learning models highly rely on the quantity of the data that they have. However, this has proved to be more challenging as large amounts of data can now be accessed with the constantly rising privacy issues and institutional limitations in accessing data. Google presented the Federated Learning model in 2017 [41] to overcome these problems.

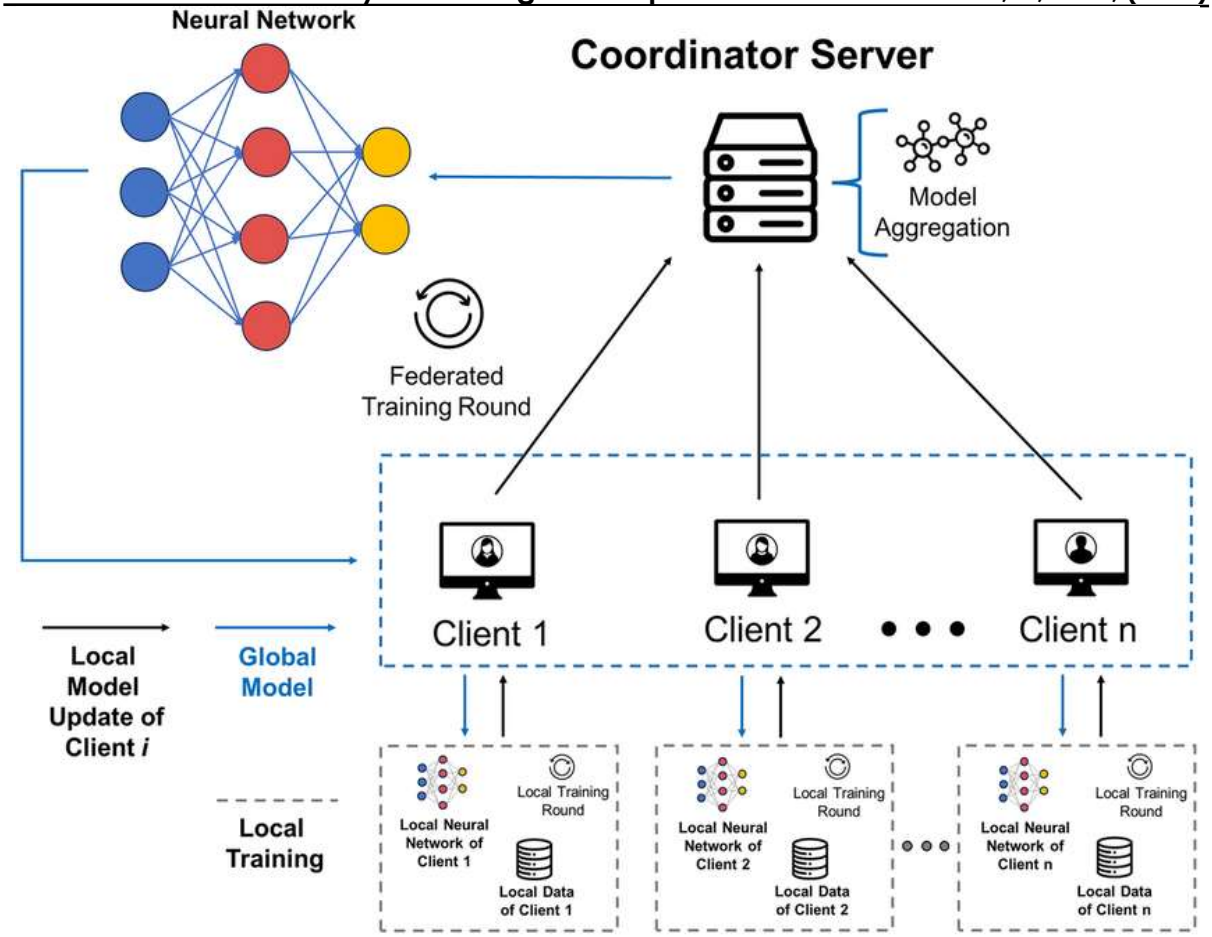

Figure 1.
Basic Architecture of FL

Core Architecture of FL

This equation 1 indicates that the federated learning is defined as the minimization of a global loss function F(theta), where theta represents the shared model parameters that are jointly learned by a number of distributed participants. The expectation term Ek p [Fk (θ) is the expected sum of local objective functions, where p is underlying distribution of clients involved.

$$\ln fl_{it}^{+} = \sum_{j=0}^{t} \Delta \ln W^{T} x + \quad b_{it}^{+} = \sum_{j=0}^{t} \max(\Delta W^{T}{}_{ij,0}) + \epsilon_{it} \qquad \text{Eq (1)}$$

This is an expectation that can also be represented as a weighted summation of all k clients and the contribution of each client is weighted by the factor nk N. In this case, nk is the number of training examples that a client with number k has, and N = nk is the sum of all the examples of all participants. Federated Learning can be used in a variety of industries, such as healthcare and finance. Therefore, mobile devices like smartphones and automobiles generate huge volumes of user data in a variety of formats [42]. FL has a number of advantages, such as safe data transmission, increased privacy protection, effective use of bandwidth, better communications, and low latency [43].

Table 2.
Comparative Analysis of Existing Privacy-Preserving Techniques in Federated Learning

Technique	Privacy guarantee	Threats covered	Computational cost (client/server)	Comm overhead	Impact on model utility	Use-cases	Maturity
Federated Averaging (FedAvg)	Inherently it does not ensure privacy protection.	Assumes an honest-but-curious server that can observe client updates.	Comparatively low; computation is mainly on the client side.	Low to moderate due to sharing of model parameters.	High, as no privacy mechanisms affect accuracy.	Common baseline for cross-device federated learning in low-risk scenarios.	Well-established and widely used in practice.
Trusted Execution Environments (TEE)	Provides confidentiality and integrity via secure hardware isolation.	It depends on trust in hardware vendor and enclave attestation process.	Low to moderate overhead.	Low communication cost.	Minimal impact on model accuracy.	Suitable when performance and hardware-based trust are prioritized.	Moderate mature; adoption increasing but hardware dependent.
Hybrid methods (DP+SMPC/ HE+DP / TEE+ DP)	Offers both cryptographic protection and differential privacy guarantees.	Requires reduced trust compared to single-technique solutions.	High due to combined privacy mechanisms.	High because of integrated protocol overhead.	Improved balance between privacy and utility.	Appropriate for highly sensitive applications.	Emerging research domains with many proposed frameworks.

LITERATURE REVIEW

The aspect of data security and privacy has gained prominence as one of the biggest issues of concern worldwide, with various megabanks still languishing when it comes to the issue of user information security [44].

FL enhances data security and, at the same time, minimizes the communication load. Although the traditional systems are unprotected against any external attacks, FL may play a crucial role in ensuring privacy and the primary purpose of this is to eliminate data theft among participants [45]. The centralized machine learning algorithms have transformed data management and analysis in different industries. They simplify workflows, automate routine and provide useful insights which can enhance the effectiveness of decision making [46]. The generation is a major step towards the privacy-saving approach, as it overcomes the prior constraints and brings new insights into the confidentiality of data. These generations can also be integrated, e.g., MPC, DP and TEE can be used together with FL to produce hybrid approaches, e.g., FL-MPC, FL-DP and FL-TEE.

$$\ln fl_{it}^{+} = \Sigma_{j=1}^{s} \Delta \ln W^{T} x + \quad b_{it}^{+} = \Sigma_{j=1}^{s} \max(\Delta W^{T}{}_{ij,1}) + \epsilon_{it} \qquad \text{Eq (2)}$$

Equation 2 is the secret sharing scheme and is the operation that breaks up a secret into a number of shares. And s is an original secret value (e.g., gradient or update of model) and W is the Threshold value, which is the minimum number of shares that is needed. U is a set of all the clients involved. And T is an element of the set. In this eq is the secret share of participant u. Su, u ∈ U is the collection of all secret shares. This equation outlines the secrets sharing in SMPC where a secret value is shared in multiple shares, and each holder holds a partial share of the secret and does not in itself, give any information about the original secret. The fraction of user u is represented as su; U

is the collection of all the participants, u is a member of U. The t parameter is the reconstruction threshold i.e. the least number of shares needed. It is represented as follows: this arrow ( ) means that assuming a minimum of t valid shares of users in U, the original secret S can be successfully reconstructed.

Table 2 highlights that Federated Averaging (FedAvg) is a basic federated learning, but, in itself, does not ensure formal privacy protection. It is implemented under the assumption of a truthful-but-inquisitive server that adheres to the protocol and still can modify the client-side model. The procedure has relatively low computation and communication costs as training is largely carried out on client devices with periodically shared parameters. This does not impact the performance of the models significantly because no explicit privacy-preserving mechanisms is used. Due to this fact, FedAvg is commonly employed as a baseline technique, particularly in cases where data sensitivity is limited, and has been viewed as a notable, production-ready approach. The secure hardware enclave is known as Trusted Execution Environments (TEE), which is used to ensure privacy and integrity of the aggregation process. In this strategy, one puts his/her faith in the hardware manufacturer and the attestation of the enclave. Both computational and communication overheads are minimal and this helps to maintain the accuracy of the model with minimal degradation. TEE-based solutions particularly fit well into the application situations where efficiency and hardware-supported trust is more important than heavy cryptographic methods. They are also being more and more utilized, yet they remain, by definition, dependent on trusted hardware infrastructures. Such hybrid systems with a mixture of Differential Privacy (DP) and Secure Multi-Party Computation (SMPC), Homomorphic Encryption (HE), or TEE are supposed to offer more powerful and far-reaching privacy guarantees. These techniques cut off the dependency on any single trust assumption by making use of statistical privacy in combination with cryptographic protection.

However, the accumulating nature of these techniques comes at the cost of large computational and communication overhead. These costs are worth making hybrid solutions highly adaptable to highly sensitive applications, though, and offer a more balanced trade-off between model utility and privacy preservation. These are new and dynamic research areas in federated learning. FL has become popular in sectors where data confidentiality is essential, such as healthcare and finance, due to its strong privacy-preserving characteristics. Federated Learning offers a viable substitute to collaborative training in a distributed environment that is motivated by the continuous improvement in privacy protection, communication optimization, and scaling. The s in this equation is the original secret value that is recovered in the reconstruction phase. The f (0) is what is obtained by the analysis of the polynomial at zero, which gives the constant term giving the secret. The index j is the sum of all shares applied in the reconstruction and the symbol of summation is to indicate that all the selected shares are applied in the outcome. The value of yj is the output of the polynomial at the input, xj, the j th share. The product notation represents the product of the terms of interpolation by all but one of the indices m, by the condition m 6=j. xm and xj are the various values of the input to the various shares in the portfolio and the denominator xm- xj ensures that there is the correct weighting in the interpolation. All the computations are done in modulo p and maintain their integrity and safety within the finite field. This is to preserve privacy and, at the same time, enable joint training of models among the different participants [57]. In the paper [58], some of the most significant innovations that can be applied in various areas are presented, and especially in the sphere of healthcare. Nevertheless, handling great volumes of sensitive medical information poses many challenges in terms of security and privacy.

Federated Learning (FL) is a powerful option as it allows training machine learning models without exchanging raw data between institutions. The study [59]

Machine Learning Perspective within Federated Learning

The Exponential Linear Unit (ELU) activation function is typically applied in neural networks to apply non-linearity. The f(x) represents the output of the activation function in this equation and x is the input value that is fed into a neuron. The a is a positive constant parameter (a>0) that is the saturation of negative inputs. Where the input x is negative, the function has been defined as f(x) = a(exp (x-1)) where exp(x) is the exponential function. This element can convert the negative inputs to produce smooth, non-zero outputs, which can then be utilized to reduce the bias shift problem and improve the stability of learning. In the scenario in which the input x is not less than 0, the function is linear i.e., f(x) = x iathe output is identical to the input. Overall, this stepwise definition causes ELU to behave linearly on positive values and in a scaling manner on negative values to a limited range that yields a faster convergence rate and better performance compared to the conventional activation functions like ReLU. The second term of the equation is the expression of the output at the situation where x is positive. It means that when the value of the input is non-negative, the ELU activation function is an identity, i.e. the value of the output is the value of the input. In [60], the authors redefine the concept of Federated Learning and introduce a novel concept, which they call Secure Federated Learning (SFL) the aim of which is to come up with reliable and privacy-friendly artificial intelligence systems that safeguard intellectual property rights. Their work includes a detailed analysis of the available literature and categorizes threats, attacks, and defense mechanisms in each phase of the FSL lifecycle. The author of [61] gives a detailed description of Federated Machine Learning, describing different architectures and privacy-saving mechanisms. The main goals of this survey are to overview the current privacy methods and find the possible uses of Federated Learning in the industrial fields. ELU – E- Linear Unit with 0 < a is

$$EI_{\mathrm{u}} = \omega^{+} TI_{it-1}^{+} + \omega^{-} TI_{it-1}^{-} \qquad \text{Eq (3)}$$

This equation 2.2 shows that f(x) is the notational expression that is constructed to share the secret among the participants. x is the variable that is employed to compute one share. a0 is the constant term of the polynomial and can be directly linked to the secret is secured. The a1, a2., and at-1 are randomly chosen elements of a non-prime field and are used to add an element of randomness and security to the scheme. t is a parameter that means the minimum number of shares to reconstruct the secret, the highest exponent t -1 is the degree of the specified polynomial and enforces the threshold property. The p is a large prime number that is used to define the finite field and the modulo operation is used to ensure that all arithmetic operations are in the field. Over the last few years, there has been an increasing mass of research on privacy-preserving machine learning. Zhou et al. suggested using Differential Privacy (DP) to safeguard user information in machine learning and implemented Secure Multi-Party Computation (SMPC) to minimize the noise brought about by the use of differential privacy [62, 63]. FL is essential in the healthcare industry, where the information of patients is highly sensitive and in maintaining privacy when it comes to joint training models [64, 65]. Beyond healthcare, Federated Learning has also proven to be a good application in Natural Language Processing (NLP) [66] and Recommendation Systems [67].

Differential Privacy (DP) Techniques for Privacy Preservation

First, FL was a distributed training system, introduced by Google and operated on mobile devices and only local model updates are transmitted to a central server to be aggregated [68]. Data sharing and data privacy. The old dilemma between privacy and the sharing of data can be resolved with the emergence of Federated Learning. Data locality implies that the data is not centralized and consequently FL is particularly useful in situations where sensitive data, such as industrial or mobile applications, are being used and the aggregation of data may be restricted by privacy laws [69]. In Federated Learning, multiple clients, such as smartphones or edge devices, share information to train a common model. The server then aggregated the locally trained models and the raw training data was kept decentralized. This leads to distributed training of deep neural networks, as well as other learning approaches, with distributed datasets available on multiple edge nodes. Under this decentralized model, FL constructs a global model on the central server with the aggregated model parameters but not raw data. This type of setup significantly reduces the risk of privacy, the cost of communication and computation of traditional centralized machine learning [70].

$$\Delta f_{t_i} = \sum_{j=1}^{n-1} \alpha j \, \Delta GERG_{it-1} + \sum_{j=0}^{n2} (\pi^{j+} \Delta EU_{it-j}^{+} \qquad \text{Eq (4)}$$

Homomorphic Encryption (HE)

Privacy-preserving techniques of Federated Learning (FL) seek to protect sensitive user data, but permit decentralized and distributed sources to collaboratively train models. Different methods have been devised, such as Homomorphic Encryption (HE), Secure Multi-Party Computation (SMPC), Federated Learning with Encrypted Data, Zero-Knowledge-Proofs (ZKPs), Differential Privacy (DP), Secure Aggregation, and Data Masking and Perturbation [71]. Differential Privacy can ensure that the overall statistical properties of the data are maintained, and no single record is exposed due to the introduction of statistical noise or processing of sampled sets of data. In this approach, attackers are not able to determine the correct value of a single data point by making consecutive queries. With each training step, noise is typically added to the output to ensure the user-level privacy [72]. In the case of Federated Learning, DP provides resistance to membership inference attacks and reduces weight leakage during training. DP is implemented with the help of the two main strategies. The sensitivity-based approach, as described in [73], describes how much one record can affect a function output and the exponential distribution-based approach between discrete data values, as discussed in [74].

Secure Multi-Party Computation (SMPC)

SMPC is a cryptographic method that allows multiple parties to jointly compute a function on their respective inputs without revealing their respective inputs to each other. Federated Learning applies SMPC to allow model training in a collaborative approach and raw data is confidential. This model plays an essential role in the preservation in the context of medical and healthcare use [80]. Secret sharing mechanism is a typical method in SMPC-it separates a secret value into several shares and spreads them among the participants, and re-creates the secret from the set of shares. Depending on the secret sharing, different privacy-saving aggregations in FL do not involve any additional pre-processing before transmitting masked updates. Chain PPFL [81] is an example of mechanism security in communication through a combination of two mechanisms. A chained communication mechanism and one masking mechanism, where the clients can send encrypted data in the form of chains. Similarly, Group Signature Federated Learning (GSFL) scheme [82] enhances privacy through the assistance of Homomorphic Encryption and zero-Knowledge

Proofs of knowledge (ZKPok). This method significantly reduces the cost of computations and transfer and ensures the identity of clients and the privacy of information.

Federated Learning with Encrypted Data

Federated Learning with Encrypted Data is another adaptation of traditional FL, putting the focus on the necessity of privacy protection through the encryption of information before its sharing outside of the local devices. This ensures that data is secure during model training [83, 84]. FLED, with the assistance of Homomorphic Encryption, enables operations to be performed on encrypted data, such as addition and multiplication, since operations can be performed on encrypted data sets. Table 3 gives the same results as those that would have been obtained using plaintext data [85, 86].

Table 3.
Techniques for Privacy Preservation: A Summary

Techniques	Advantages	Disadvantages	Ref
Secure Multi-Party Computation (SMPC)	Maintains data confidentiality without exchanging raw information and supports complex computational operations.	Incurs high computational and communication overhead.	[87]
Homomorphic Encryption	Ensures data privacy during computations and supports various mathematical operations on encrypted data.	It has significant computational costs and limited operational scope.	[88]
Federated Learning with Encrypted Data	Protects sensitive data during model training and allows collaboration among untrusted parties.	Provides Limited support for complex model structures and requires specialized encryption algorithms.	[89]
Differential Privacy	Offers strong theoretical privacy guarantees.	Can lower data utility and involve complex noise calibration.	[90]

Privacy-Preserving Techniques Overview

A summary of key privacy-preserving and secure computation techniques that are popular in distributed and collaborative learning systems is presented in Table 4. Secure Multi-Party Computation (SMPC) allows two or more parties to undergo computation without sharing raw information as they consider their own datasets classified information. Though it has strong confidentiality guarantees and capable of supporting complex operations, SMPC poses huge computational and communication overheads, which can potentially affect the performance of the system. Homomorphic Encryption (HE) enables operations to be performed on encrypted data and, therefore, provides the privacy of the processing phase. This is quite efficient in keeping the sensitive information safe, it is also associated with high computational cost and has a limited number of operations it is capable of, thereby not being as useful in complex or large-scale tasks. Federated Learning with Encrypted Data allows training a federated model using local data of multiple participants without exposing their local data. It helps in ensuring the safety of the untrusted environment by integrating encryption systems. The technique, however, has numerous challenges with a difficult model structure and uses special encryption functions and therefore, implementation is more complicated. Differential Privacy (DP) provides privacy guarantees in a formal and mathematically proven way, introducing noise to data or model updates in a well-regulated fashion to reduce the chances of the leakage of personal data. Even though it is good at protecting privacy, noise may negatively impact the utility of data and model accuracy, and

noise parameter selection is challenging.

$$\Delta f_{t_1} = \sum_{j=0}^{n3} (\tau^{j+} \Delta FD_{it-j}^{+} + \tau_j^{-} \Delta FD_{it-j}^{-}) \qquad \text{Eq (5)}$$

Privacy-preserving techniques are developed in federated learning to ensure that sensitive information is not revealed, but enable machines to learn collaboratively and analyze meaningful information.

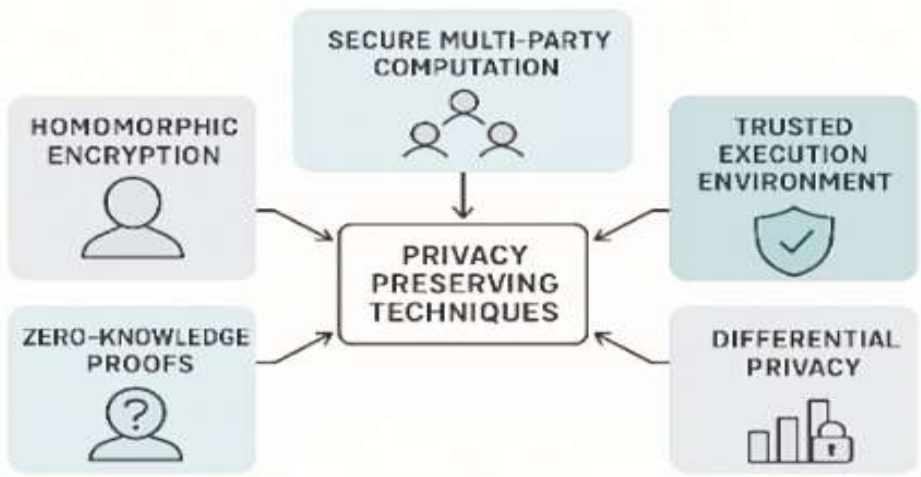

Figure 2.
Overview of Privacy-Preserving Techniques [114]

Figure 2. presents the most important approaches to maintain privacy in federated learning systems. It proves that ensuring privacy is achieved through a combination of multiple mutually supportive mechanisms. With Homomorphic Encryption, it is possible to perform operations using encrypted data. Secure Multi-Party Computation and Zero-Knowledge Proofs enable trusted and safe collaboration and authentication without displaying sensitive information. The system is also improved with the help of Differential Privacy and a Trusted execution environment that minimizes the threat of inferences and offers secure execution.

$$\Delta f_{t_2} = \sum_{j=0}^{n3} (\tau^{j+} \Delta FD_{it-j}^{+} + \tau_j^{-} \Delta FD_{it-j}^{-}) \qquad \text{Eq (6)}$$

Table 4.
Comparative Overview of Notable Approaches

Techniques	Advantages	Disadvantages	Ref
Zero-knowledge Proofs	Provides cryptographic proof without data disclosure. Supports privacy-preserving authentication.	Involves heavy computational processes and has restricted real-world use cases.	[109]
Secure Aggregation	Improves data security and compliance with privacy regulations.	Selecting the most suitable aggregation protocol can be challenging for varying needs.	[110]
Data Masking and perturbation	Complies with regulations: Supports adherence to data privacy regulations like GDPR and HIPAA.	. Vulnerable to re-identification by advanced attackers using sophisticated methods.	[111]
Hybrid Approaches	Enhanced privacy protection. Flexible in application.	May increase complexity due to integration of multiple techniques.	[112]
Trusted Execution Environment	Enhanced performance compared to centralized methods.	Faces issues with scalability and compatibility across different systems.	[113]

Table 4 gives an overview of some of the most popular privacy-saving techniques and contrasts their benefits, limitations, and suitability in secure data-driven systems. These two methods have different technical grounds on which they safeguard privacy. Zero-Knowledge Proofs enable verification of information without knowing the actual information behind the information, and thus are very suitable in privacy-related verification. However, they are limited in practice in their high computational requirements and their lack of scalability in the domain. Secure Aggregation is a significant idea applied in federated learning since it assures that the updates of individual clients are not revealed during aggregation. Though this kind of strategy can be used to meet the regulations, the optimal strategy of aggregation can be complex due to different arrangements of the systems.

$$\Delta f_{t_2} = \sum_{j=0}^{n4} (\sigma^{j+} \Delta TI + \sigma_j^{-} \Delta TI_{it-j}^{-}) + \varepsilon_{it} \qquad \text{Eq (7)}$$

Perturbation and Data Masking technologies keep sensitive information safe by manipulating or hiding data, thereby helping organizations to abide by privacy regulations, such as GDPR and HIPPA. Nevertheless, even under the condition of sophisticated analysis tools, they may be susceptible to re-identification attacks. Hybrid Approaches are a combination of different privacy-saving actions to improve increased privacy and a greater adaptability to different contexts of use. This added level of security is likely to be gained with the cost of a more complicated system and overhead on installation. TEEs are both efficient and safe in running sensitive computations, by isolating them through hardware. Despite these strengths, there are scalability and interoperability challenges with TEEs across heterogeneous computing platforms.

METHODOLOGY

The strategy to design and develop a hybrid privacy-preserving federated learning (FL) system is presented in this chapter. It presents the problem statement, data acquisition process, data analysis process and the proposed model, which is a combination of three essential privacy preservation techniques- Secure Multi-Party Computation (SMPC), Differential Privacy (DP), and Homomorphic Encryption (HE) in detail. Also, the chapter addresses the implementation plan, provides a schematic flowchart and lastly, specifies the algorithmic steps, which define how the proposed framework will operate.

Federated Learning (FL) is an emergent decentralized paradigm that allows various participants to learn a shared model together, without having to move raw data to one location. It is sort of a decentralization (but implicitly so), FL, however, is susceptible to numerous privacy security risks, such as member inference and model inversion and gradient leakage attacks, in which the attackers would seek to infer sensitive information about their users, depending on how changes to the model. The current privacy-saving frameworks tend to be based on the isolated data transfer programs such as Differential Privacy (DP), and Secure Multi-Party Computation (SMPC), or Secure Multi-Party Encryption (HE). All of these have their benefits, but are also constraining in that DP adds random noise to gradients to eliminate leakage at the cost of accuracy. SMPC guarantees safe cost increment of calculation among parties, but sacrifices on the latency and communication costs. HE can compute encrypted data, and burns much computer power to do so. Federated Learning enables sharing machine learning models to be used by different clients to learn collectively without exchanging raw data. Nevertheless, other privacy attacks, such as model inversion attacks and inference attacks, are very dangerous. The main

research question of the study is the following: How can a composite solution to Differential Privacy, Homomorphic Encryption and SMPC be handled to give Federated Learning better privacy without affecting the quality and performance of the model negatively? In the facilitation of a hybrid framework, these challenges would be resolved. This paper suggests that these challenges could be eradicated by a combination of three approaches. This is to come out with a balanced solution in order to save privacy and ensure the performance and computational efficiency in the models.

Data Collection and Data Preprocessing

The data of experimentation and model analysis were in publicly accessible, benchmarked models such as MNIST, Fashion-MNIST and CIFAR-10. These datasets were chosen to encompass diverse types of data modalities- image and tabular- to ensure the applicability of the proposed model is generalized. Each client carried out its own preprocessing steps in order to come up with its own local dataset: The numbers of data were scaled in such a way that numerical values were comparable. The categorical variables were coded using one-hot encoding. To minimize imbalance in classes, the data were balanced. Prior to model training, sensitive fields were encrypted. Exploratory Data Analysis (EDA) was performed directly on the field and only aggregate model parameters were forwarded to the central server. This shared calculation also ensured the clients were not going to be able to access the raw data directly, and it would not compromise their confidentiality. A series of proposed adversarial attacks, including gradient inversion and membership inference, was implemented to measure privacy resilience. The hybrid defense schemes turned out to be highly resistant, which led to significant reduction in the possibilities of reassembling privacy data. To mimic a federated environment, all the datasets are shared across the various clients. Other preprocessing procedures, such as normalization, resizing, and categorical encoding, are also employed where necessary. Data is saved on the devices of customers and only the updates on the models are sent to provide confidentiality.

Table 5.
Dataset and Task Classification

Dataset	Total Samples	Clients	Distribution Type	Task Type
MINIST	60,000	10	Non-IID	Image Classification
Fashion-MNIST	60,000	10	Non-IID	Image Classification
CIFAR-10	50,000	10	IID	Image classification

Proposed Model Architecture

The proposed research methodology has created a Hybrid Privacy-preserving Federated Learning (HPP-FL) framework, which incorporates SMPC, DP, and HE into a unified framework. The offloading of the local training on the client data is carried out independently, and the updates of the models are automatically secured with the help of a layered protocol: Different noise to gradients, by applying the shaping of a different amount of random noise, is added to block the inference attacks. Homomorphic Encryption (HE) encrypts noisy gradients and can be computed in an encrypted space. Secure Multi-Party Computation (SMPC) provides a safe exchange between clients and the central aggregator, but is not visible in the in-between values. This unified design provides multi-layered privacy assurance over the learning pipeline, from local computation to the global model aggregation. A hybrid privacy-preserving framework is proposed to enable a solution to the limitations of privacy solutions on the individual method, comprising DP, HE and SMPC. The architecture of the proposed system consists of: Client Nodes: Independent data

owners training local models on private data. Central Aggregator: Coordinates the global model update without accessing raw data. Hybrid Privacy Layer: Integrates SMPC, DP, and HE modules to protect information at every stage.

1. Distribute the initial global model to all clients.
2. Each clients trains locally on its dataset.
3. Apply DP noise to the resulting gradients.
4. Encrypt gradients using HE.
5. Transmit encrypted updates through SMPC protocol.
6. Aggregator performs secure aggregation on encrypted data.
7. Decrypt and update the global model.
8. Redistribute the updated model to clients.

Implementation of the proposed Model/Technique

The prototype of the hybrid FL framework was implemented using:

Programming Language: Python

Frameworks: PyTorch, PySyft, TenSEAL, and Crypten

Hardware: Multi-core CPU cluster with GPU support and 32GB RAM

Supporting Libraries: Numpy, Scikit-learn, TensorFlow Federated

Table 6.
Components and Technology utilized

Component	Technology Use
Programming Language	Python 3.x
ML Libraries	TensorFlow Federated, PyTorch
Privacy Libraries	PySyft, PyDP, TenSEAL, PySMPC
Dataset	MINIST, CIFAR-10
Hardware	Intel i7, 16 GB RAM

Implementation Steps

The implementation is carried out in the following steps:

Step 1: Experimental Setup

- Using Python with PyTorch/TensorFlow
- Simulation through Flower/FedML or custom FL environment

Step 2: Local Training

Each client trains the model on its local data for a fixed number of epochs.

Step 3: Applying Differential Privacy

DP-SGD optimizer is used with gradient clipping and noise addition.

Step 4: Homomorphic Encryption

Noised gradients are encrypted using HE schemes such as Paillier or CKKS.

Step 5: Secure Multi-Party Computation

Secret shares are generated and sent to the server for secure aggregation.

Step 6: Updating Global Model

After aggregated values are decrypted, the server updates the global model and

sends it back to clients.

Step 7: Evaluation

The system is evaluated by test accuracy, loss, privacy leakage prevention, and computational cost.

Proposed Flowchart

The flow chart below is the structure of secure and privacy-conscious federated learning. It schematically depicts these sequential characteristics of the process, which involves local model training, the application of differential privacy, encryption, secure aggregation and updating the global model. The present suggestion is the proposal of a secure federated learning system that will help in securing the users by using privacy enhancement techniques and safe computation algorithms. The architecture ensures that sensitive data in the training and aggregation processes is confidential. The initial phase involved the central server deriving an international learning model and distributing it to several clients involved. Each client trains the received model on its own local data contained in it. Since the processing is done locally on the data, there is no direct access to the server. As the local training process also entails full generation of model updates, differential privacy mechanisms are applied to them. Clipping of gradients is used to constrain the effect of individual clients in excesses and controlled random noise is introduced. This is done to minimize the possibility of individual records of data being identified through the common updates

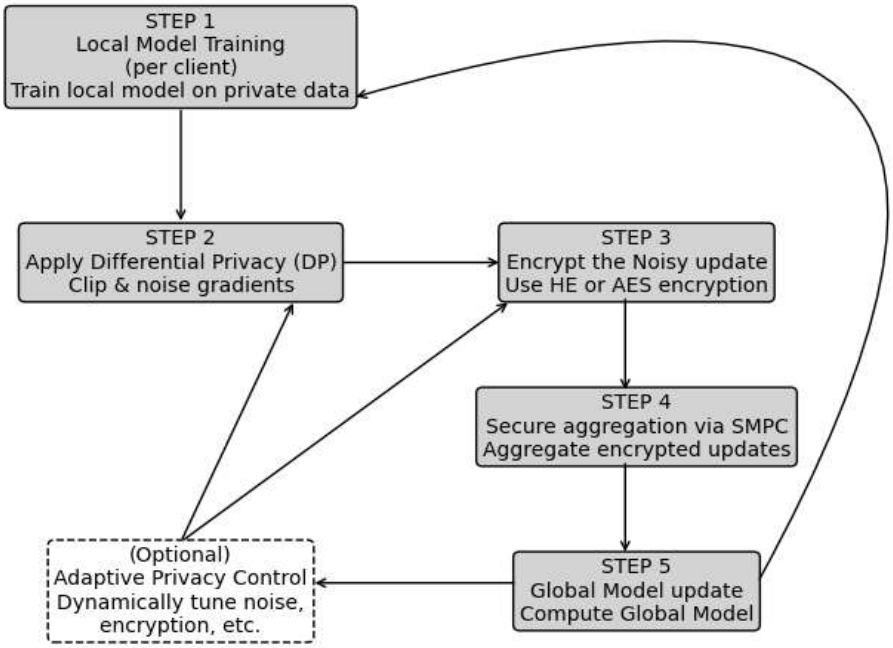

Figure 3.
Proposed Methodology Flowchart of the Hybrid Privacy-Preserving Federated Learning Model
Figure 3 is a flow chart of the structure of secure and privacy-conscious federated learning. It schematically depicts these sequential characteristics of the process, which involves local model training, the application of differential privacy, encryption, secure aggregation and updating the global model. The present suggestion is the proposal of a secure federated learning system that will help in securing the users by using privacy enhancement techniques and safe computation algorithms. The architecture ensures that sensitive data in the training and aggregation processes is

confidential. The initial phase involved the central server deriving an international learning model and distributing it to several clients involved. Each client trains the received model on its own local data contained in it. Since the processing is done locally on the data, there is no direct access to the server. As the local training process also entails full generation of model updates, differential privacy mechanisms are applied to them. Clipping of gradients is used to constrain the effect of individual clients in excesses and controlled random noise is introduced. This is done to minimize the possibility of individual records of data being identified through the common updates

Stepwise Process

I. Start
II. Initialize the global model
III. Distributes the model among clients.
IV. Perform local training on private data.
V. Apply DP noise for privacy preservation.
VI. Encrypt model updates using HE.
VII. Execute SMPC-based secure aggregation.
VIII. Decrypt and update the global model.
IX. Redistribute the updated parameters.
X. Repeat until model convergence is achieved.
XI. End

Algorithm 1: Hybrid Privacy Federated Learning

```
Input: Initial global model G, client datasets D1…Dn, total rounds T
Initialize global model G
For     t = 1 to T do:
          For    each selected client I:
                   Train local model on Di using current G
                   Compute local gradients gi
                   Add DP noise → gi'
                   Encrypt   noisy gradients using HE → Ei
                   Create SMPC shares of Ei → Si
                   Send Si to server
      Server aggregates encrypted shares **weighted by client dataset size |Di|**
      Server decrypts aggregated result → plain aggregated gradients:
            G ← G + η * aggregated gradient
End For
Return G
```

Secure Aggregation and Model Update

The target algorithm presents a privacy-aware federated learning framework that enables a group of clients to simultaneously learn a shared model without sharing their sensitive data. The method relies on Differential (DP), Homomorphic Encryption (HE), and secure Multi-Party Computation (SMPC), as means of high data protection.

The inputs of the algorithm are: G - The received sets of a receiver at the server. The distributed locally-client data sets D1, D2, D3., DN is locally stored. There is an agreed number of training rounds T. Every round will involve the following steps that the chosen clients follow:

All of the global models received in each client are trained using their local data; raw data is not passed out of the client device. During training, the client computes local gradients, that is, the updates to the model. Differential Privacy.--Differential Privacy uses a certain amount of controlled noise on the gradients to prevent sensitive

information leakage. Sorrow, such operations are then coded in Homomorphic Encryption to permit operations to be made on the loud gradients without knowing them. Secure Multi-Party Computation techniques from the encrypted gradients are divided into multiple shares in order to be more secure. There are these enhanced shares that are sent to the central server, not the actual updates. The encrypted bits that all client machines receive are added up by the server. To balance the contributions, the significance of the update will be different depending on the size of the client dataset that it represents. The server aggregates the result and then, the result is decrypted before the aggregated gradients are added to the global model when the aggregation is completed. The same process is carried out in the subsequent round, where the final product is the international model G that has undergone the perfecting procedure. The privacy of different values decreases the possibility of recreating sensitive information. Homomorphic Encryption provides updates in models when sent and computed. SMPC offers an opportunity to implement the process of aggregation in a safe manner, whereby the individual updates would not be revealed. Federated learning allows college learning and retention is centralized.

Evaluation Metrics

To assess the performance and effectiveness of the proposed model, the following evaluation metrics were employed:

Accuracy (ACC): Measures predictive performance.

Privacy Leakage Rate (PLR): Quantifies the exposure risk of sensitive data.

Computation Time (CT): Evaluates the efficiency of encryption and aggregation.

Communication Cost (CC): Assesses network resource utilization during training.

Analysis of proposed Model/ Block Diagram

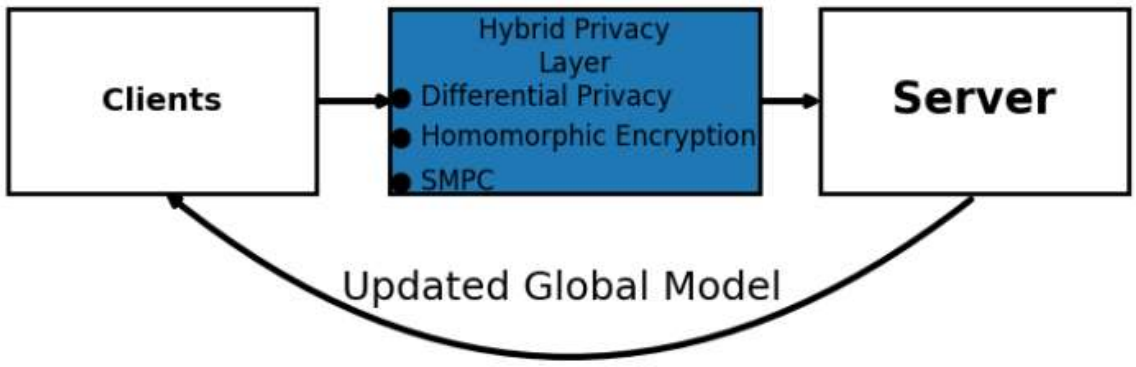

Figure 4.
Proposed Hybrid Privacy-Preserving Federated Learning Framework

The proposed model in Figure 4 is based on a privacy-aware federated learning model that incorporates a hybrid privacy mechanism to ensure secure and confidential training. The system prevents direct data sharing by allowing clients to collaborate without exposing their raw datasets.

System Architecture

The model is composed of three key entities:

- Distributed clients

- A hybrid privacy layer
- A central server
- Clients communicate securely with the server, and only refined global models are exchanged. Sensitive user data always remains on the client side.

The report contrasts the performance of the suggested hybrid framework and the current/existing federated learning models by the presence or absence of a privative mechanism of individual privacy. Three trendy benchmark datasets, namely, MNIST, Fashion-MNIST and CIFAR-10 were experimented on to be able to compare the work with a wide selection of images. The learning model is a Convolutional Neural Network (CNN). It has been configured in 3 different ways: Standard federated learning (no privacy guarantees), Federated learning (with personal privacy mechanisms (DP, HE, SMPC)) and Federated Learning (with the hybrid privacy framework (DP, HE and SMPC)). This comparison is made based on the effect of both approaches on accuracy, precision, recall, and F1-score, and illustrates the trade-offs between privacy-preservation and model performance.

The results indicate that the hybrid solution is typically better than privacy solutions used independently and general federated solutions, which provide a mediocre answer and have the capability to ensure generous data protection and high predictive outcomes. The privacy-preserving federated learning proposed is compared and contrasted with the existing methods. A normal CNN-based federated learning system with no privacy mechanisms is called as the baseline model. This benchmark is compared to either models whose privacy method is univariate Differential Privacy, Homomorphic Encryption and SMPC, or their hybridization structure. In the MNIST, Fashion-MNIST and CIFAR-10 datasets, performance measurements (accuracy and F1-score) are used to evaluate them. The results indicate that unpaired privacy techniques contribute to minimal drops in the model performance, yet the hybrid framework not only keeps up with competitors but also offers superior privacy assurances. It has been mentioned during the discussion that both strategies have their strengths and weaknesses, and that the proposed approach contains more benefits than drawbacks in terms of data privacy and model performance. The experimental results are given in the summary form of a bunch of figures, comparison bar charts and tables. The training and validation accuracy of communications between federated learning rounds on the datasets MNIST, Fashion-MNIST, and CIFAR-10 are described by the line graphs. Bar charts provide a graphical comparison of final accuracy and F1-score of the baseline model, privacy-enhanced models, and the hybrid structure. The comp table summarizes quantitative results, showing the difference between traditional federated learning and privacy-preserving methods. Together, the visual and tabular representations enable the ideally transparent and objective evaluation of the methods provided. The results show that the hybrid framework above is more accurate and has a larger F1-score on MNIST, Fashion-MNIST and CIFAR-10 datasets and even stronger guarantees of privacy.

The computational costs of the combination of different privacy preservation methods are extremely high but overall, the overhead is not extremely high and the framework can be applied within a real-world federated learning system. The experiments were conducted on a federated learning system consisting of a set of distributed clients and a central server (aa). The clients merely trained the local model with their data set and exchanged updates with the server. Within the framework presented, Differential Privacy (DP), encryption and Secure Multi-Party computing

(SMPC) are integrated to ensure the privacy of the information during training and aggregation. The performance of the proposed method was compared to the next techniques like Conventional Federated Learning (FL), Differential Privacy-based FL and Encryption-based Secure FL.

RESULTS & EVALUATION

In this chapter, the proposal for testing the proposed framework concerning privacy-preserving federated learning is presented. MNIST, Fashion-MNIST and CIFAR-10 datasets were experimented by varying privacy conditions to investigate the performance of a CNN-based federated learning model under varying privacy conditions. Assessment consists of analyzing whether the model is accurate or not, whether the communication and impact of inclusion of privacy-saving mechanisms is efficient. The effectiveness of the proposed hybrid model is proven by comparing results with the known federated learning techniques.

Comparative Analysis of the Proposed and Current Techniques

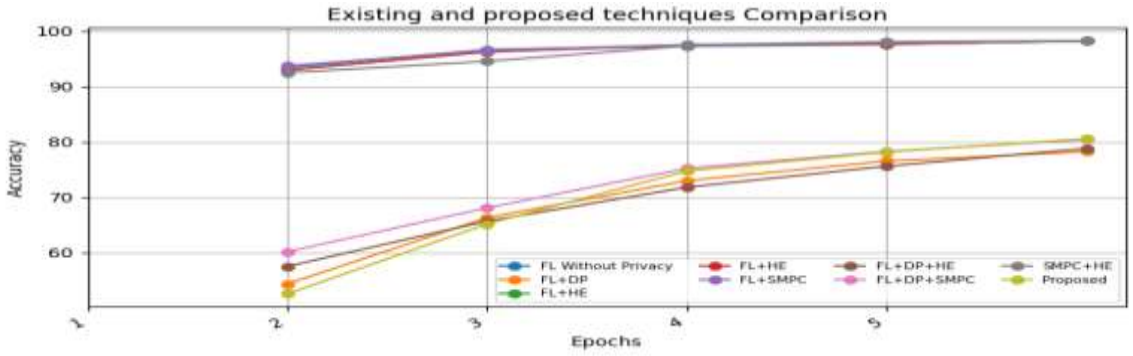

Figure 5.
Epoch-wise Accuracy Comparison on MNIST Dataset

Figure 5 makes a comparison of current and proposed federated learning approaches in terms of the accuracy at the end of the fifth training epoch. The initial model FL is the FL that does not require privacy and, at all times, yields the best results, meaning that the upper limit would be placed at the maximum performance, if it does not enforce any privacy constraints. However, privacy-saving methods such as FL grounded on Differential Privacy (DP) and Homomorphic Encryption (HE) and Secure Multiparty Computation (SMPC) in the first place are less accurate due to the induced noise and encryption overhead. The progressively increasing accuracy, which corresponds to model convergence, versus epoch, is exhibited by all the approaches in the long run. The proposed technique has higher efficiency in privacy and the model performance at the training period in comparison to individual privacy mechanisms and their combinations. In the final epoch, the recommended solution reaches the accuracy of the non-privacy threshold, albeit with a higher level of privacy, and it can be regarded as its efficiency and applicability to the application of federated learning in other secure situations.

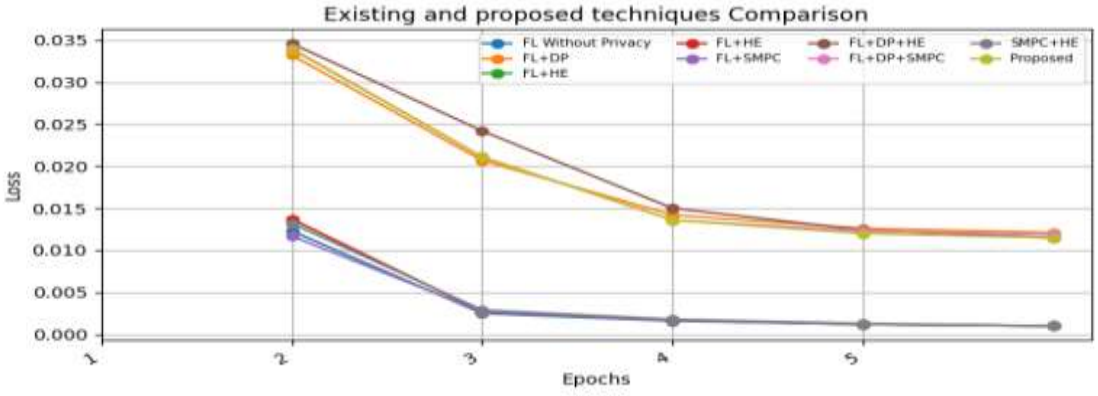

Figure 6.
Epoch-wise Loss Comparison on MNIST Dataset

Figure 6 shows the comparison of the loss of existing and proposed federated learning methods in comparison during five training epochs. Loss values of FL in the absence of privacy are minimal in the course of training, implying that quick convergence is achieved when privacy constraints are not provided. Privacy-centric solutions, on the other hand, consist of Differential Privacy (DP), Homomorphic Encryption (HE), as well as Secure Multi-Party Computation (SMPC), which have more loss in the first place due to the addition of noise, encryption, and communication overhead. The trend is that more and more epochs slowly attenuate the majority of techniques in the way that the model learns. However, there are also fluctuations in some hybrid strategies (e.g., combinations with SMPC), and these strategies also demonstrate the complexity of the computation when doing secure aggregation. It should be noted that the privacy method offered has a relatively low loss compared to other privacy-enabled techniques, with consistent though improved convergence performance. The suggested strategy balances privacy safeguarding and training stability, to a reasonable trade-off for the proposed federated learning system protection.

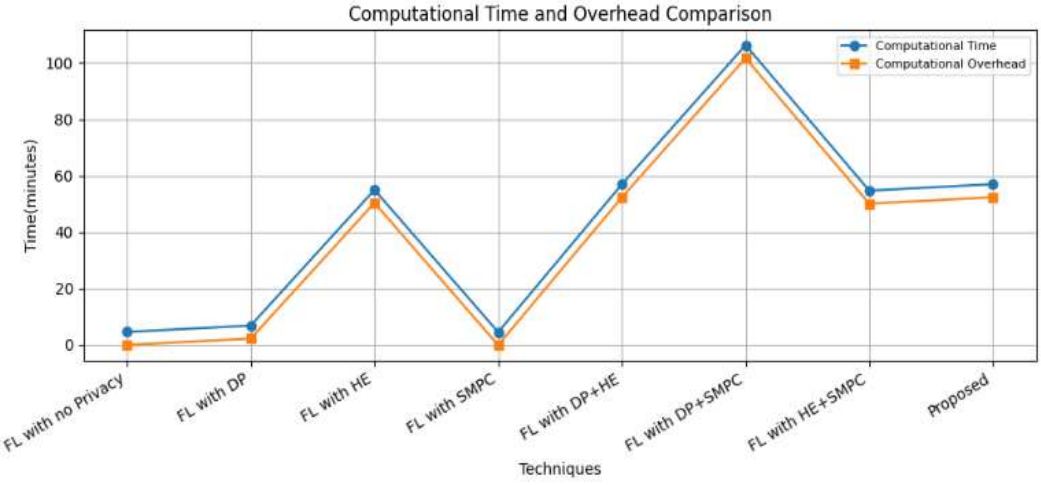

Figure 7.
Comparison between Computational Time and Computational Overhead

This Fig 7 shows the comparison between the time of computation and the overhead of the computation of the different federated learning (FL) techniques and other privacy-preserving techniques. Privacy-free minimum FL model is the least computationally time-consuming and has the lowest overhead requirements, which means it is weakly complex in processing. Noise addition is heavier, leading to chaos,

the time is slightly increased, and overhead is minimal when Differential Privacy (DP) is applied. On the other hand, the techniques in Homomorphic Encryption (HE) and Secure Multi-Party Computation (SMPC) multiply the computations and overhead enormously because of engaging in the complex encryption and secure aggregation process. Compounding of DP and HE makes them expensive to compute as the overhead of DP and SMPC is relatively low, compared to HE-based computation. A combination of FL model and the use of both HE and SMPC has one of the highest requirements in computation due to the combination of multiple layers of security. The proposed design has both high, manageable computing time and overhead, that is, a good trade-off of high privacy and computing performance. Overall, the results suggest the trade-off between increased privacy and increased computational cost in a federated learning system.

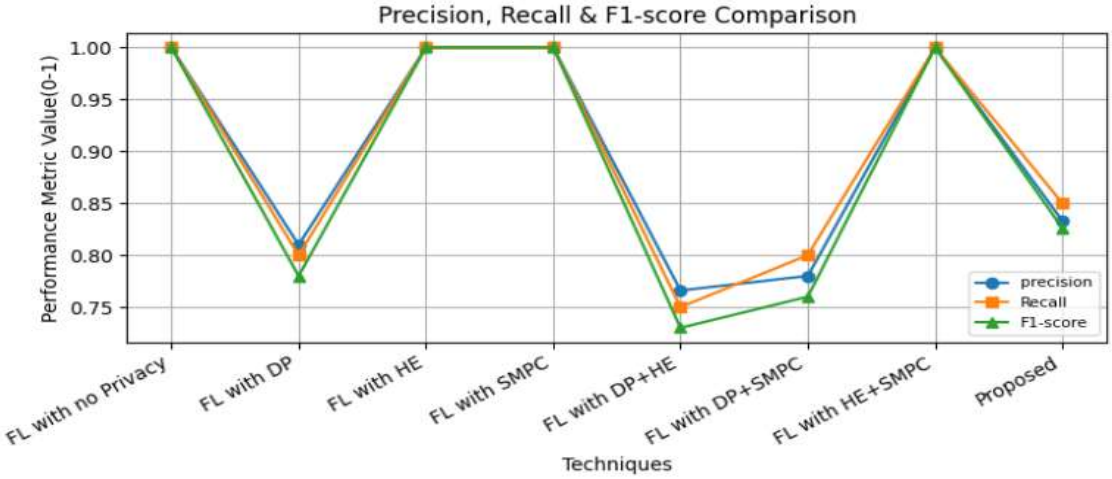

Figure 8.
Comparison Techniques and Performance Metrics

The figure 8 is a comparative study of precision, recall, and F1-score to other federated learning (FL) methods that have and do not have privacy-preserving mechanisms. FL model without privacy has the best overall performance based on all three measurements, tending towards the highest scores, indicative of the best classification. When the Differential Privacy (DP) concept is applied, there is a salient reduction in recognition, recall and F1-score due to injected noise to guarantee privacy. Compared to them, FL, applied together with Secure Multi-Party Computation (SMPC), and Homomorphic Encryption (HE), are almost as fast as the non-private baseline, demonstrating that these methods do not reduce model utility. However, if one has to channel DP with HE or SMPC, this deteriorates the performance, which translates to the total computational and privacy cost. Despite the FL model being driven by the combination of HE and SMPC and showing good performance, the hybrid solutions, the proposed method shows the same performance regarding competition, recall, and F1-score. Overall, the results indicate the tradeoff between privacy and model in which an encryption-based solution appears to be more practical than solutions based on noise to protect privacy.

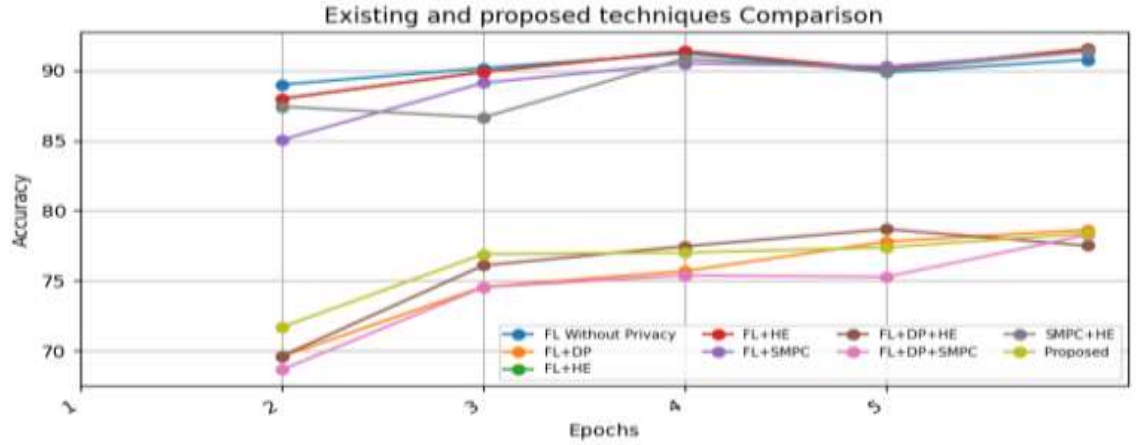

Figure 9.
Epoch-wise Accuracy Comparison on Fashion-MNIST Dataset

Figure 9 illustrates differences between the effectiveness of the existing and proposed methods of federated learning with accuracy after five training epochs. The highest in accuracy is always the model of FL without privacy, FL baseline, which implies that no considerable performance costs are imposed. However, privacy-sensitive methods such as Differential Privacy (DP), Homomorphic Encryption (HE), or Secure Multi-Party Computation (SMPC) performed individually or in cooperation introduce reduced accuracy due to the trio of methodological enhancements of noise and calculation limitations. The further the epochs, the more all the methods demonstrate the gradual perfecting of their working, which stresses the successful union of learning. It is also worth mentioning that the approach proposed triumphs over other approaches based on enhancing privacy due to the fact that such an approach is more precise at later epochs, yet it has an impressive level of privacy guarantee. It would imply that the presented framework will be capable of choosing an appropriate balance of privacy preservation and model performance, which will make it a more advantageous and realistic solution compared to current privacy-sensitive federated learning frameworks.

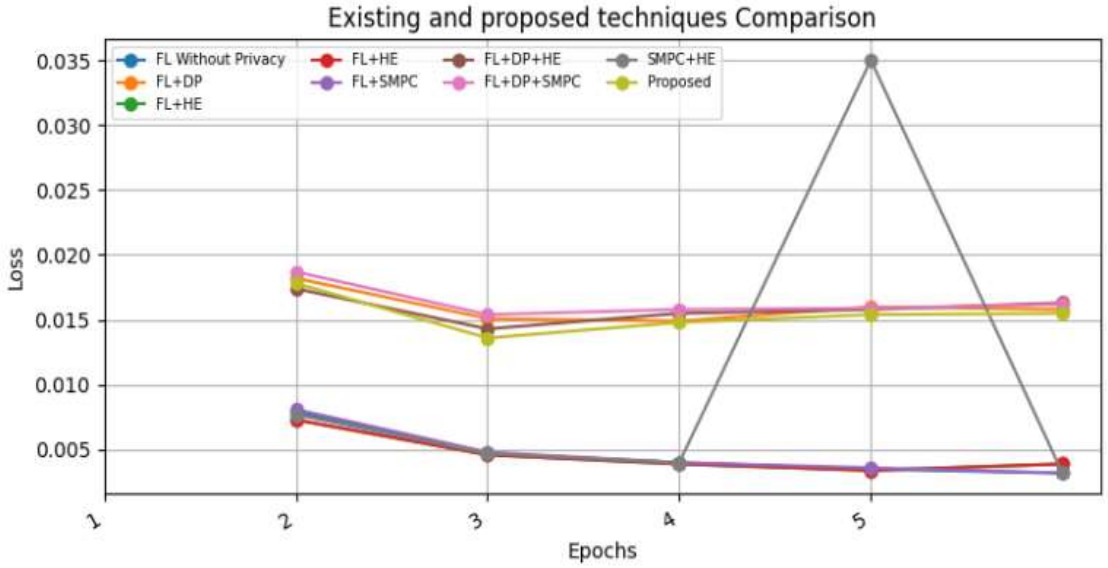

Figure 10.
Epoch-wise Loss Comparison on Fashion-MNIST Dataset

This figure 10 illustrates the comparison of precision, recall and F1-score of the various

federated learning (FL) methods using the various privacy-preserving mechanisms. The values of all three metrics are nearly perfect, reflecting the highest classification performance, on the privacy-free version of the FL model. With the introduction of Differential Privacy (DP), a significant reduction of precision, recall and F1-score is witnessed as a result of noise injection. Conversely, FL models that use Homomorphic Encryption (HE) and Secure Multi-Party Computation (SMPC) preserve performance levels near the baseline, which means that they have little effect on the model accuracy. Nevertheless, hybrids like DP and SMPC have been shown to cause degradation of performance, most notably a significant decrease in F1-score in the case of DP + SMPC. The hybrid of HE and SMPC FL model portrays high and consistent performance in all measures. The proposed method has a balanced precision, recall, and F1-score, which yield competitive performance, but provide privacy guarantees. Overall, the results indicate the trade-off between privacy protection and model performance in a federated learning system.

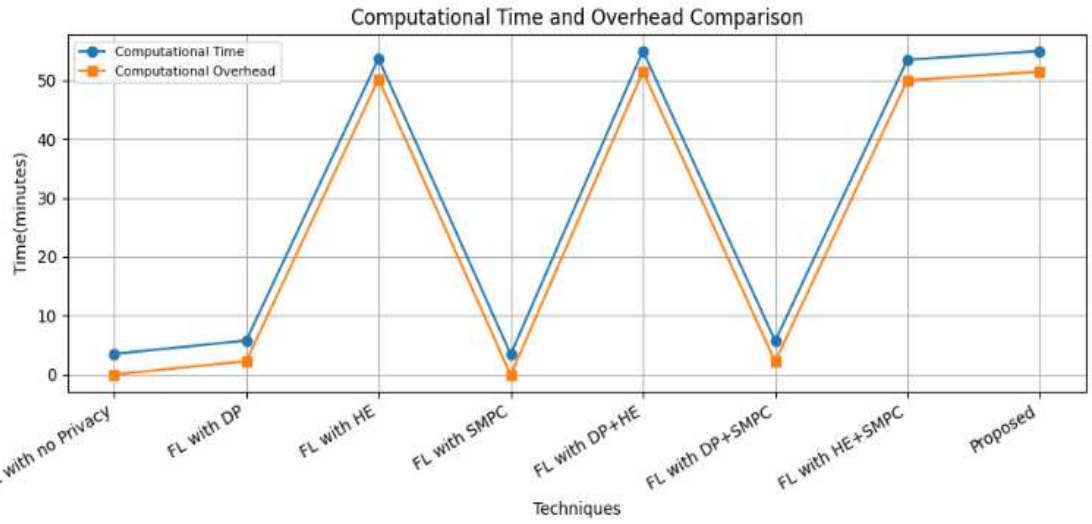

Figure 10.
Comparison between Computational Time and Computational Overhead

This 10 figure is the comparison of different methods of federated learning regarding the computation time and overhead. The bare federated learning model that lacks privacy has least execution time and overhead as it does not involve any other processing that is related to privacy. A significant increase in both the time of computation and overhead is noticed when privacy mechanisms like Differential Privacy, Homomorphic Encryption and Secure Multi-Party Computation are included. The methods that are at an individual level include the Homomorphic Encryption and SMPC, which have a higher level of computing overhead due to encrypting and safely aggregating information. Hybrid methods are also more expensive, with the mixture of Differential Privacy and SMPC indicating the greatest time usage. By contrast, the proposed method shows a more balanced performance, as it strikes a balance between the computational time and overhead, when compared to the majority of hybrid privacy-preserving methods, albeit with a high level of privacy protection. This implies that the suggested framework is workable to make the most out of the computational efficiency and at the same time, it does not jeopardize the privacy requirements.

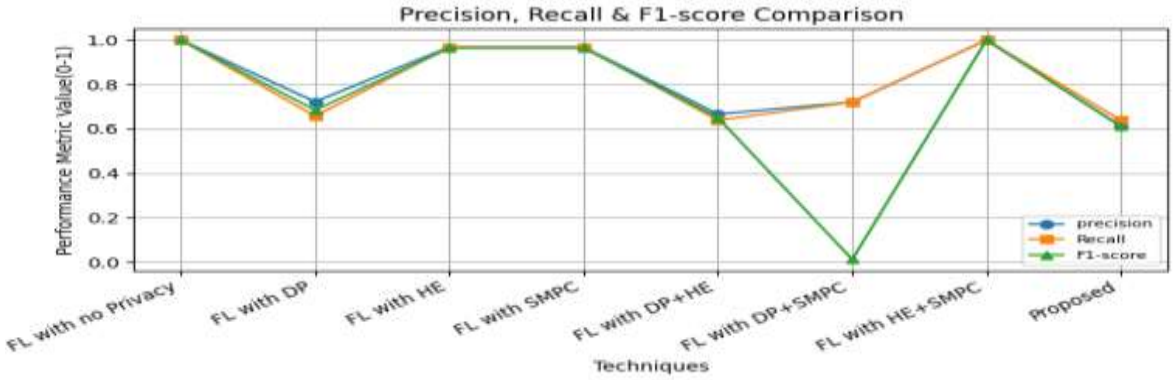

Figure 11.
Comparison Techniques and Performance Metrics

This fig 11 depicts the accuracy performance of current and proposed federated learning methods training five epochs. We note that the accuracy of all techniques improves with an increase in the number of epochs, which proves that effective convergence is achieved during training. The federated learning model, which does not imply privacy restrictions, demonstrates a higher value of accuracy in all epochs, and privacy-enabled techniques have a relatively lower value of accuracy because of the incorporation of security measures. The proposed methodology has a gradual yet uniform accuracy increase across epochs and achieves competitive performance when compared to existing privacy-based methods. It is by no means better than all hybrid approaches in the sense that, when forming the training process, the learning behaviour is to be relied upon.

Comparative Analysis of Accuracy on CIFAR-10 Dataset Using Graphs

Figure 12 is consistent with the comparative study of the existing and proposed federated learning methods' training loss over five epochs. It is observed that all procedures have a decreasing value of the losses as the number of epochs increases, a sign of effective learning and convergence in the training. The federalized model of learning that does not have privacy mechanisms has a higher loss reduction rate, whereas the approaches that have privacy mechanisms have lower loss reduction rates. The proposed method exhibits a linear, progressive decrease of loss in every epoch, and fixed convergence behaviour. Although some of the currently used methods have lower final loss values, the proposed method remains competitive, and the final loss values are much lower.

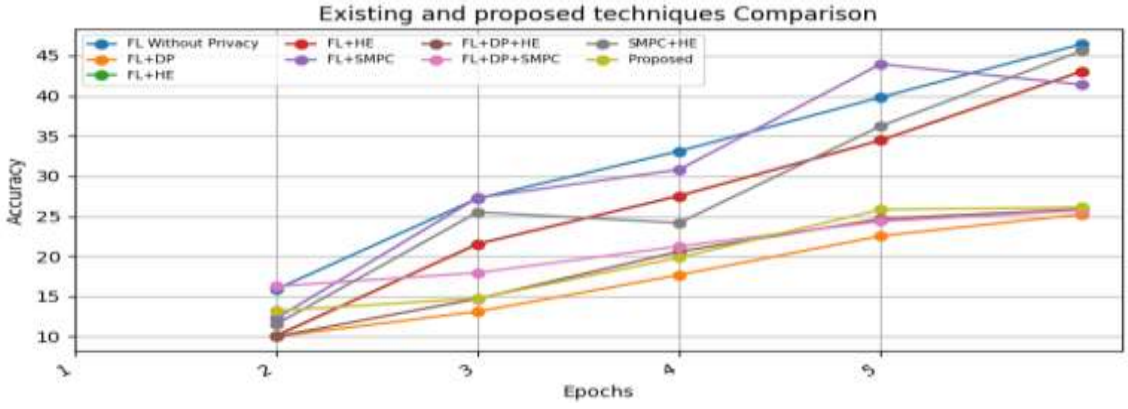

Figure 12.
Epoch-wise Accuracy Comparison on CIFAR-10 Dataset

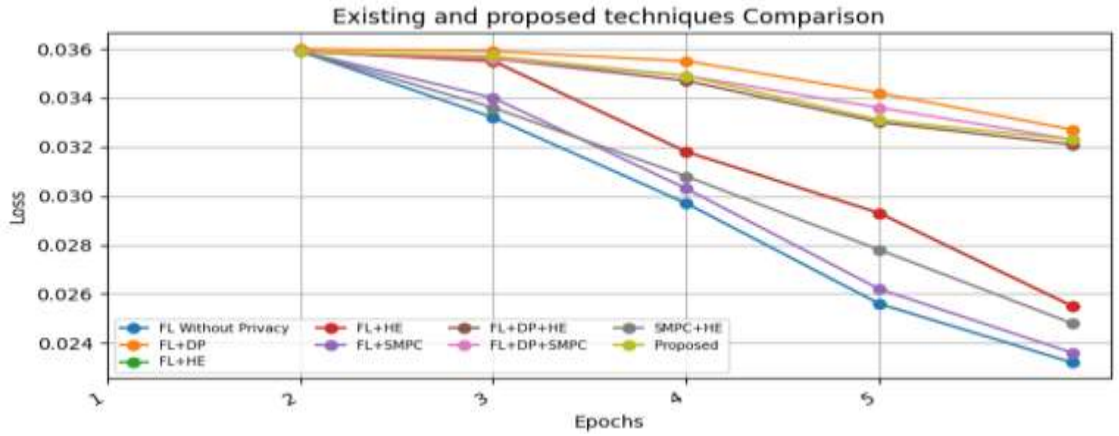

Figure 13.
Epoch-wise Loss Comparison on CIFAR-10 Dataset

Figure 13 gives a comparative study of computational time and computational overhead of different federated learning methods in the context of various privacy-preserving mechanisms. The unprivatized non-federated baseline model of federated learning has the least amount of computational time and overhead, thus having the least amount of processing complexity. The computational time and the overhead increase in moderate forms due to the introduction of noise and other processing procedures in the case of Differential Privacy (DP) implementation. The computational time and overhead of Federated Learning with Homomorphic Encryption (HE) are great because the cost of the computations involved in the encryption process and decryption processes is high. Computation using Secure Multi-Party Computation (SMPC), on the other hand, has relatively lower computational requirements when compared to the computation of solutions using HE, which proves to be more efficient. The DP + HE combination offers one of the most costly computational prices since the production of the different privacy systems involves a high processing cost. Similarly, the hybrid model of DP and SMPC suggests more time to be used to compute as compared to the single method. The HE+SMPC setup further increases the computational cost through the joint cryptographic operations. Finally, the proposed method has high computational time and overhead; this is justified by its ability to provide more protection of privacy without sacrificing the aspect of balanced model performance, thus depicting a trade-off between model performance and privacy protection.

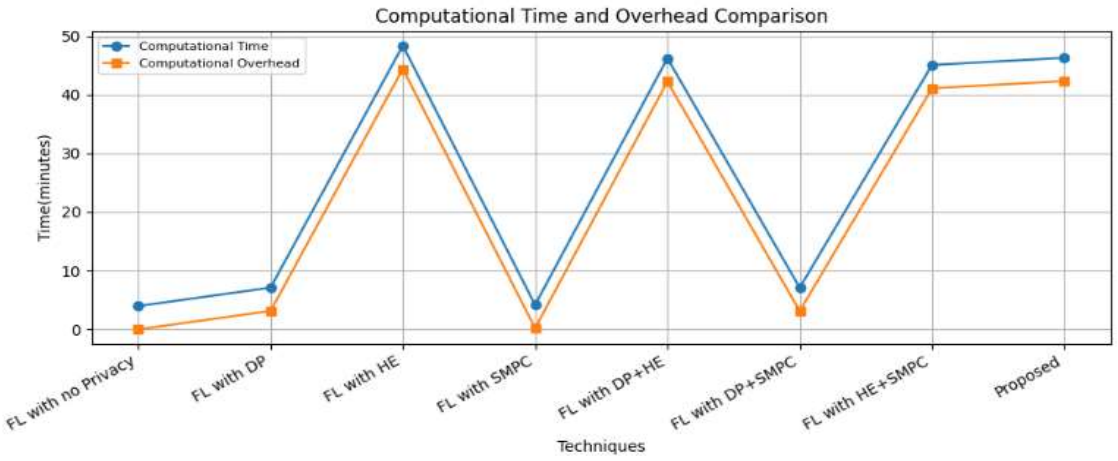

Figure 14.
Comparison between Computational Time and Computational Overhead

Fig 14 reflects a comparative analysis of precision, recall, and F1-score under different federated learning-based configurations under different privacy-preserving mechanisms. Relative performance in all three measures indicates relatively balanced performance of the initial federated learning model with no privacy restrictions. However, when the Differential Privacy (DP) is applied individually, a considerable drop in the accuracy, recall and F1-score is observed, which reflects the impact of adding noise on the model performance. On the other hand, the highest accuracy can be obtained in case of pure usage of Homomorphic Encryption (HE), however, the values of recall and F1-scores are rather moderate. The performance of Federated Learning using Secure Multi-Party Computation (SMPC) is moderately stable and moderate, and has a recommendable balance between accuracy and recall. The overall best performance is a combination of the overheads of different privacy mechanisms, and is achieved by the joint action of DP and HE. Using the DP and SMPC, it is possible to observe a slight improvement in the performances; however, the values remain lower than in the case of single-privacy solutions. The HE+SMPC configuration has improved performance compared to other combined methods, and demonstrates higher consistency of metrics. Finally, the proposed approach offers a relatively stable and balanced accuracy, recall, and F1-score values, which implies its capability to diminish the degradation of performance caused by privacy and ensure consistent classification performance.

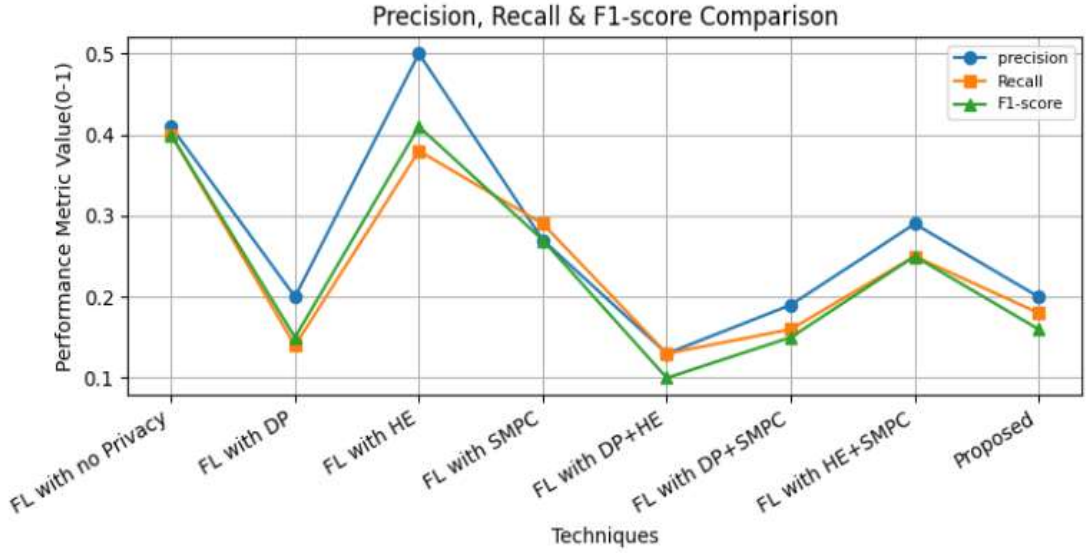

Figure 15.
Comparison Techniques and Performance Metrics

Fig 15 gives a comparison of how the existing and the proposed methods are accurate, per epoch by epoch, on the Fashion-MNIST dataset. The more epochs, 1, 2, 3, 4, the better all the models perform in terms of gradually improving their accuracy with increases in the number of epochs. Privacy-preserving techniques that are already in existence have moderate accuracy, but not as high as they would have been without their extra computational and privacy overhead. Conversely, the proposed technique always achieves higher accuracy in all epochs, showing faster convergence and better learning stability. These results reveal that the proposed strategy can be useful to increase the accuracy of classifications and maintain privacy in federated learning.

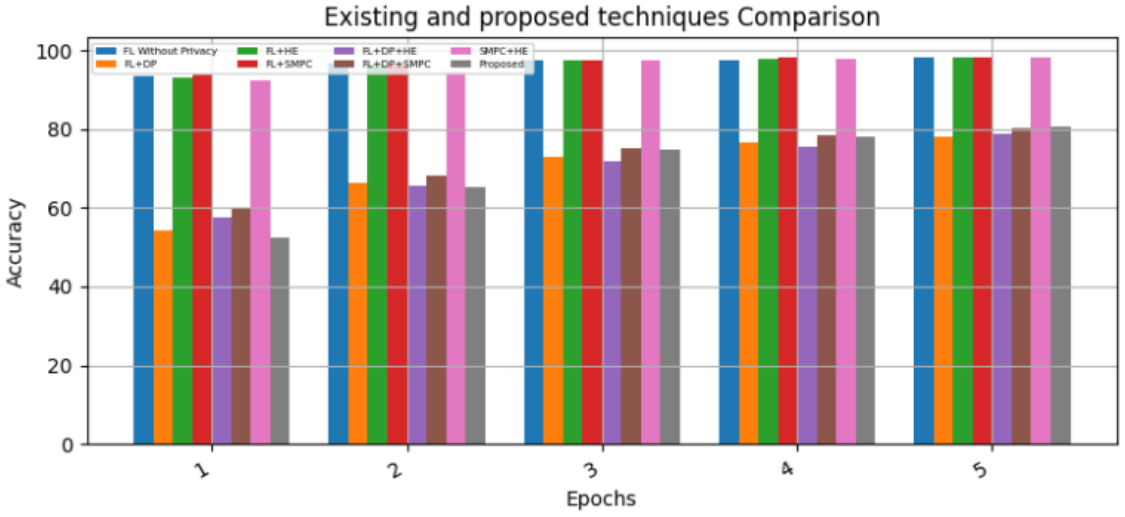

Figure 16.
Epoch-wise Accuracy Comparison on MNIST Dataset

Figure 16 is an epoch-by-epoch comparison of training loss on the MNIST data of existing and proposed techniques. The loss values tend to decrease with an increase in the number of epochs i.e., as the number of epochs increases by 1 to 5 epochs, the loss values tend to decrease. Existing privacy-preserving techniques originally incurred a greater loss due to the additional noise and computation overheads. However, the proposed approach shows a more rapid reduction of loss through the epochs and the loss values of the proposed technique are lower than those of the existing methods. This proves to be more stable and efficient in learning compared to the proposed approach and yet meets privacy restrictions, and thus proves to be more effective in federated learning on the MNIST dataset.

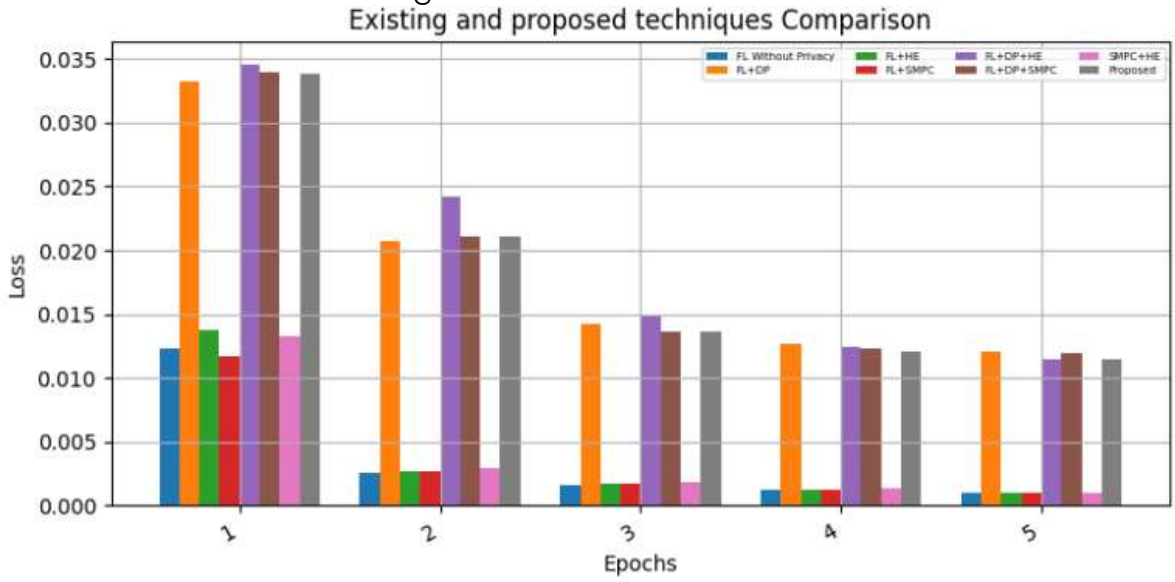

Figure 17.
Epoch-wise loss Comparison on the MNIST Dataset

Figure 17 shows a comparison between the computational time and overhead of different machine learning and privacy-preserving techniques on the MNIST dataset. These results show that traditional models are linked to the least amount of computational resources, and privacy-preserving techniques are associated with the added time and overhead linked with security-related operations. The proposed methodology has a reasonable computation cost compared to all-secure

mechanisms and demonstrates an effective tradeoff between protecting privacy and computational efficiency. This means that the proposed framework is appropriate to be applied in a real-world scenario where both performance and data privacy are paramount.

Below figure 18 presents the comparison of precision, recall, and F1-score of different learning and privacy-preserving methods. The findings indicate that the performance of initial models is relatively good, yet there is a slight drop in the performance in the case that, in the event of additional limitations, privacy mechanisms are implemented. However, the proposed technique is always more accurate and recalls more and the F1-score is higher compared to other safe techniques. This shows that the proposed framework is good at preserving classification performance and incorporating privacy protection, thus making it more reliable than the current privacy-preserving methods.

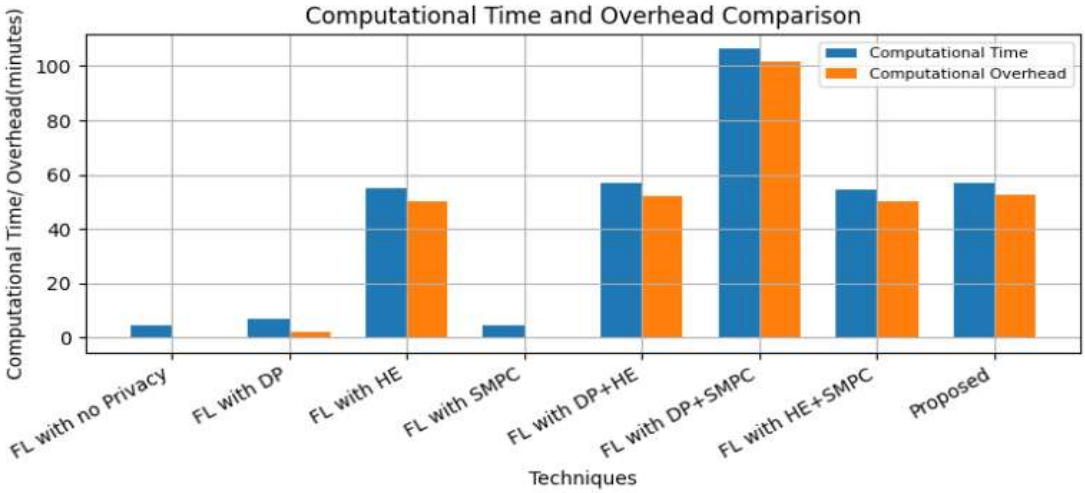

Figure 18.
Comparison between Computational Time and Computational Overhead

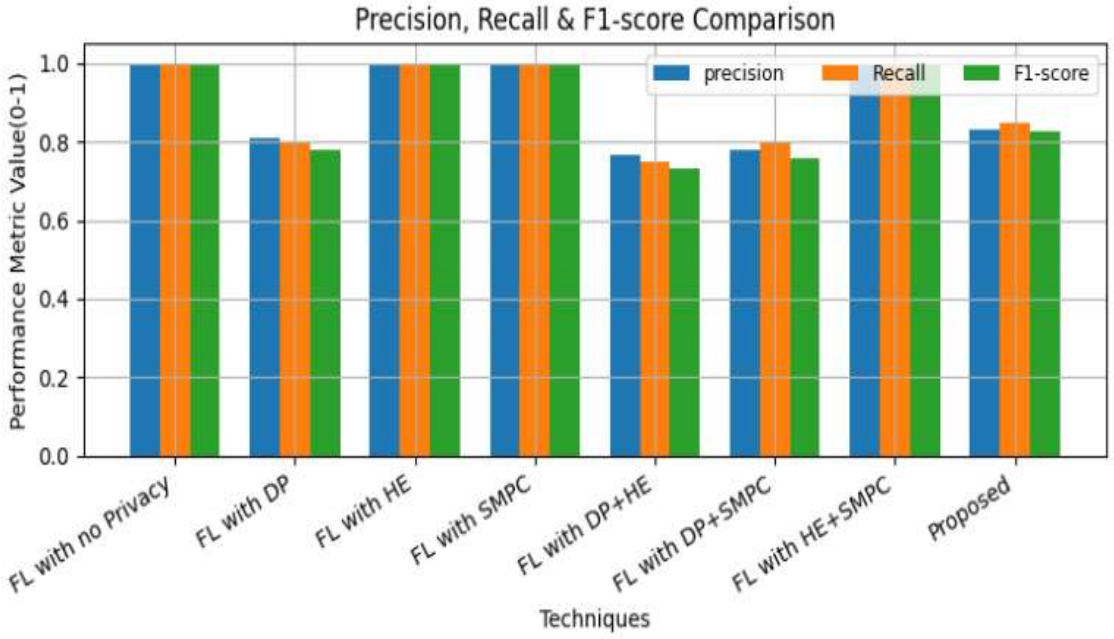

Figure 19.
Comparison Techniques and Performance Metrics

Figure 19 gives a comparative study of existing and proposed privacy-preserving methods in a federated learning setup over five training epochs. The number of epochs is the x-axis and the accuracy of the model is the y-axis. The proposed technique is contrasted with such methods as FL without privacy, FL with DP, FL with HE, and hybrid techniques (DP+HE, DP+SMPC, HE+SMPC, and hybrid techniques). The results indicate that all the approaches are likely to improve their accuracy as the number of epochs increases. However, privacy-aware techniques have a marginally reduced accuracy than FL without privacy due to the security constraints. The proposed method is the only method that achieves a better accuracy of all epochs, with a more balanced data privacy and model performance.

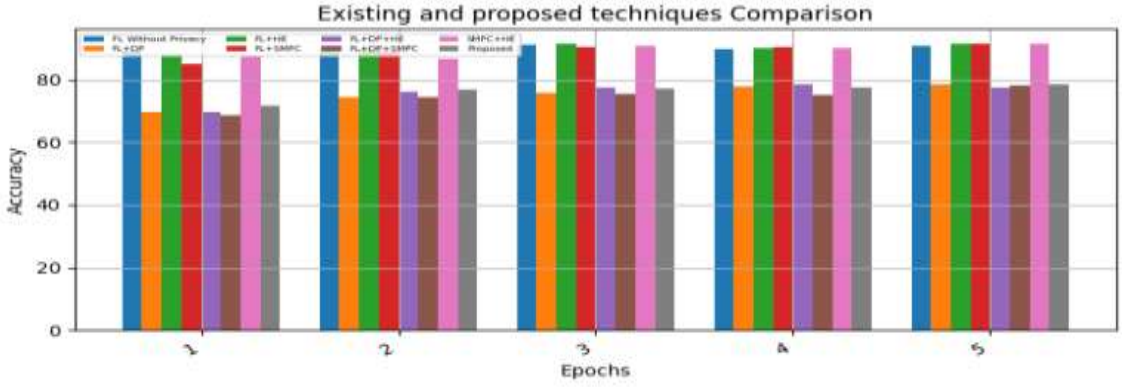

Figure 20.
Epoch-wise Accuracy Comparison on Fashion-MNIST Dataset

Figure 20 shows a comparative analysis of the training loss of different existing and proposed federated learning methods using five epochs. The results indicate that the values of losses successively decrease with the growth of the number of epochs, which confirms the effective learning behavior. A standard federated learning that lacks privacy may incur low loss, but approaches that protect privacy may incur relatively high loss due to encryption and the overhead of secure computation. However, the proposed method incurs less loss over time compared to the current methods and this factor shows that the proposed method can enhance convergence and has a high level of privacy preservation.

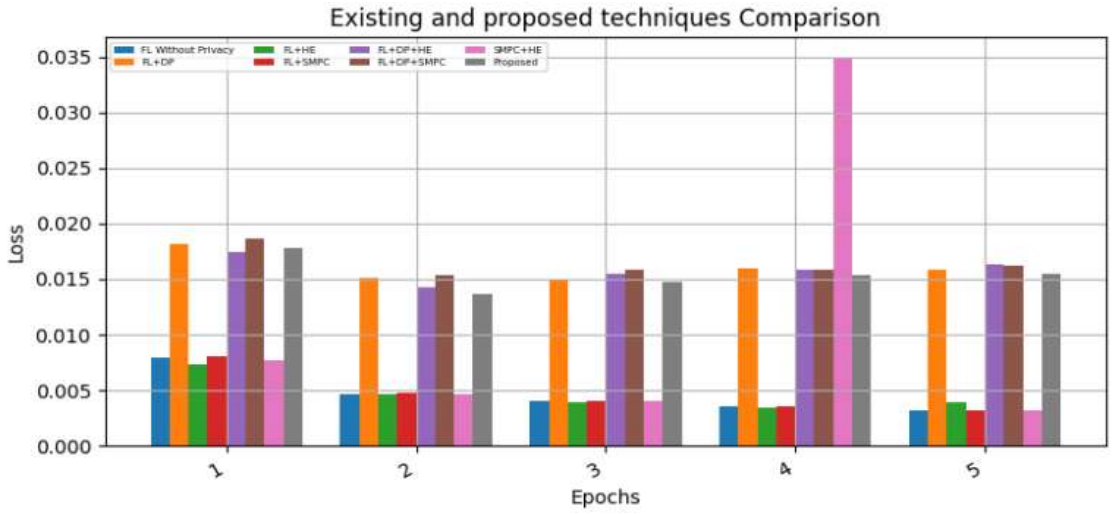

Figure 21.
Epoch-wise Loss Comparison on Fashion-MNIST Dataset

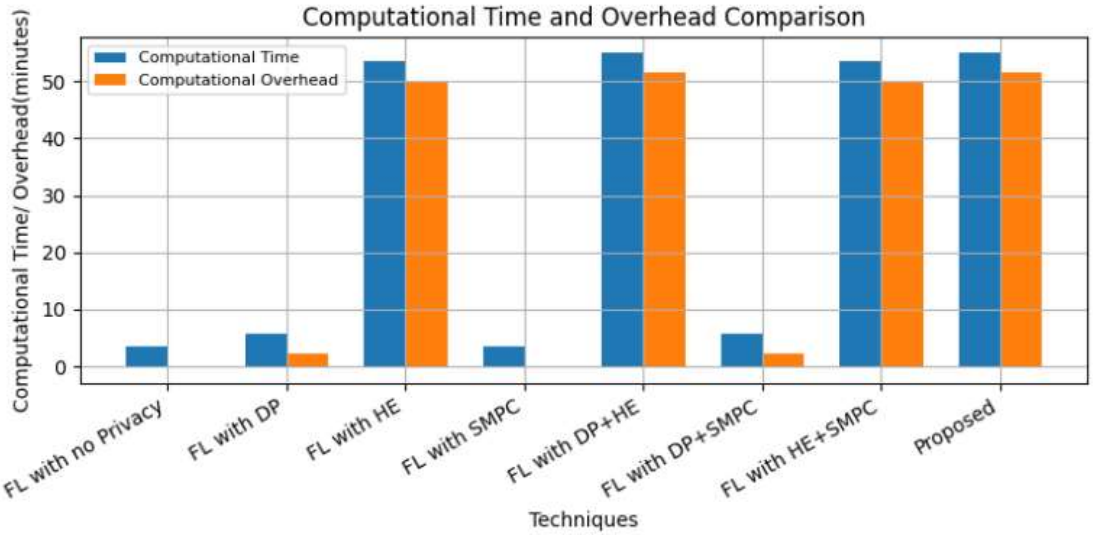

Figure 22.
Comparison between Computational Time and Computational Overhead

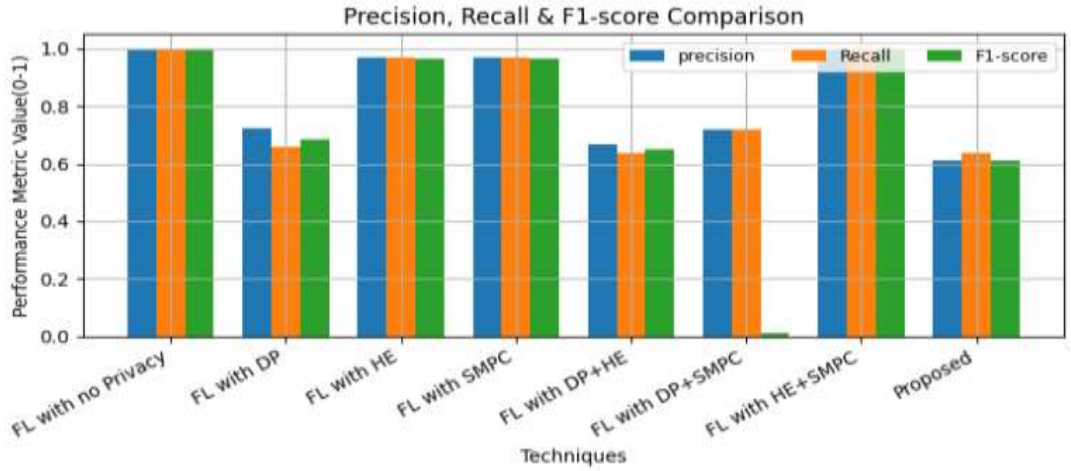

Figure 23.
Comparison Techniques and Performance Metrics

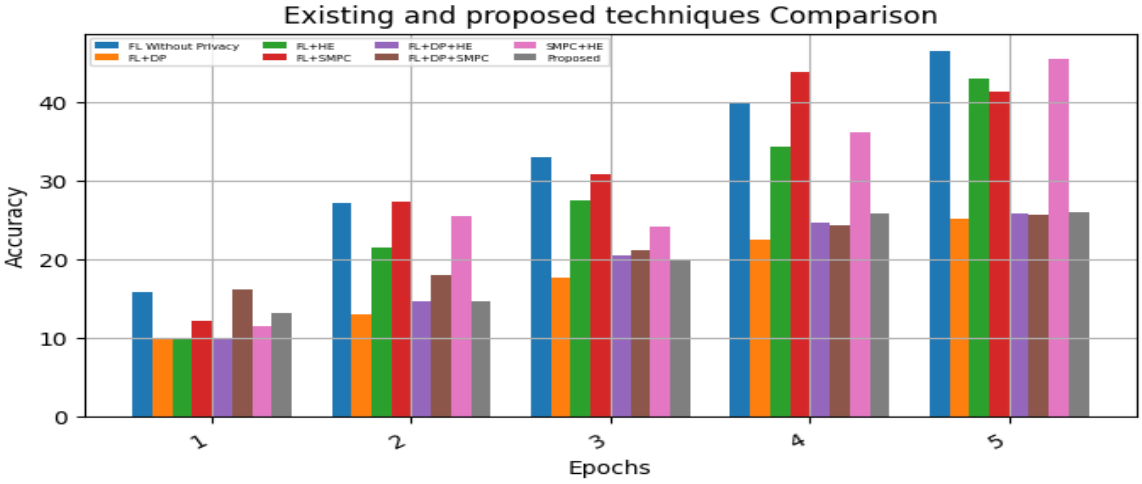

Figure 24.
Epoch-wise Accuracy Comparison on CIFAR-10 Dataset

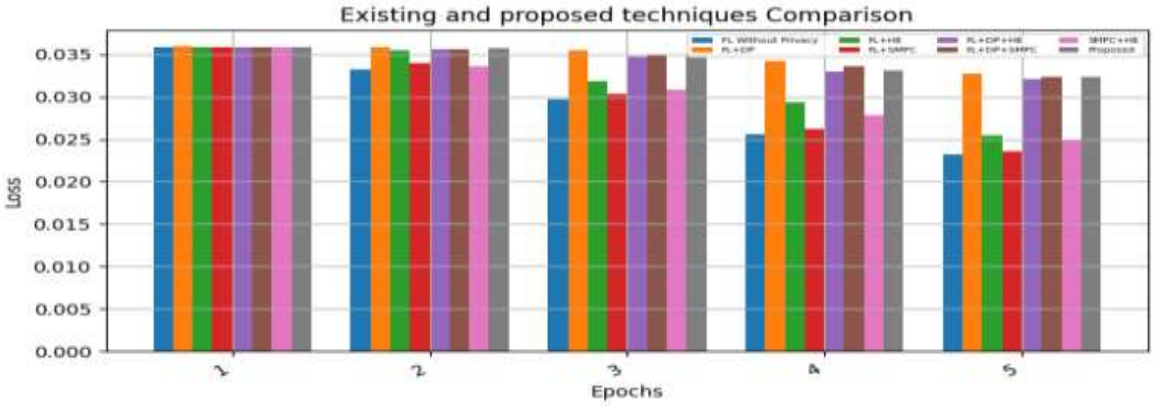

Figure 25.
Epoch-wise Accuracy Comparison on CIFAR-10 Dataset

4.24 Comparative Analysis of Computational Time and Computational Overhead on CIFAR-10 Dataset Using Bar Chart

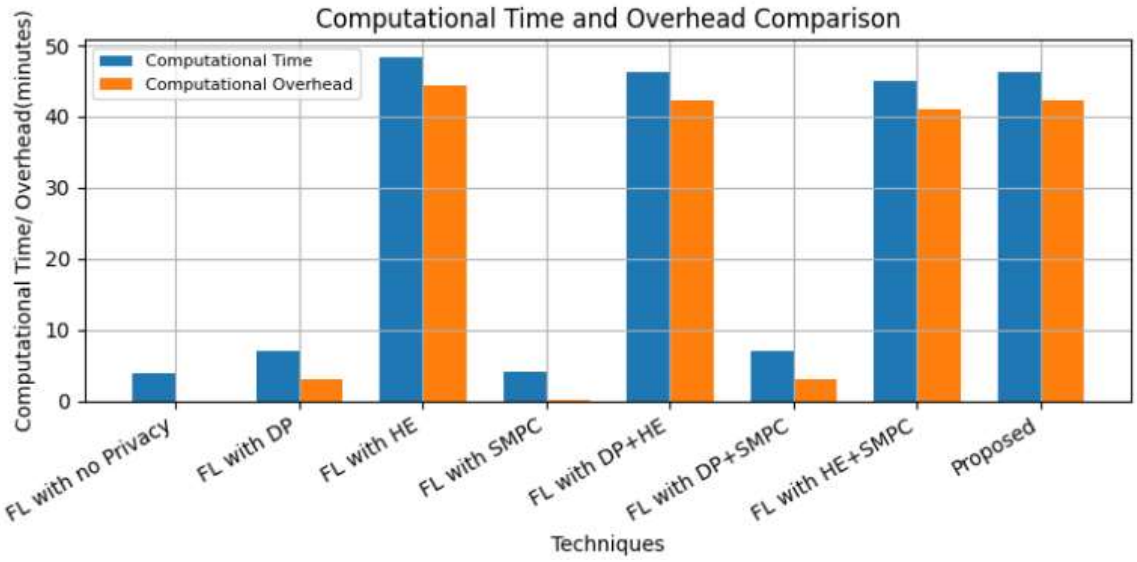

Figure 26.
Comparison between Computational Time and Computational Overhead

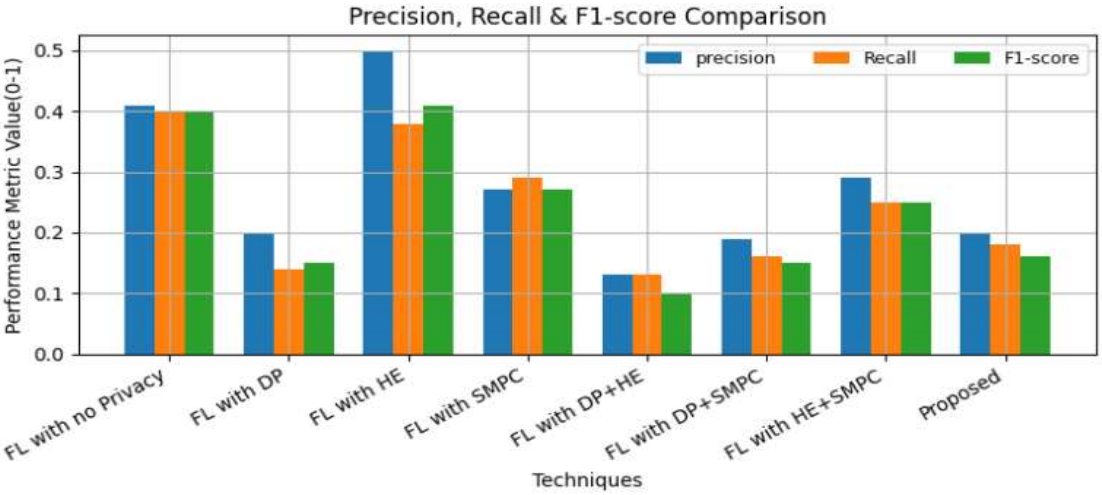

Figure 27.
Comparison Techniques and Performance Metrics

Table 7.
Comparative Analysis of Accuracy on MNIST Dataset

Techniques	Accuracy (%)				
	Epoch-1	Epoch-2	Epoch-3	Epoch-4	Epoch-5
FL	93.47	96.67	97.28	97.63	98.28
FL+DP	54.34	66.30	72.98	76.53	78.20
FL+HE	92.99	96.29	97.48	97.70	98.22
FL+SMPC	93.73	96.53	97.54	98.07	98.27
DP+HE	57.50	65.68	71.79	75.60	78.80
DP+SMPC	60.15	68.08	75.22	78.27	80.38
HE+SMPC	92.50	94.55	97.36	97.97	98.22
PROPOSED	52.52	65.18	74.74	78.16	80.55

Table 8.
Comparative Analysis of loss on MNIST Dataset

Techniques	LOSS				
	Epoch-1	Epoch-2	Epoch-3	Epoch-4	Epoch-5
FL	0.0123	0.0025	0.0016	0.0012	0.0010
FL+DP	0.0332	0.0207	0.0149	0.0126	0.0121
FL+HE	0.0137	0.0027	0.0017	0.0012	0.0010
FL+SMPC	0.0117	0.0027	0.0017	0.0012	0.0010
DP+HE	0.0346	0.0242	0.0150	0.0124	0.0115
DP+SMPC	0.0340	0.0211	0.0136	0.0123	0.0119
HE+SMPC	0.0132	0.0029	0.0018	0.0013	0.0010
PROPOSED	0.0339	0.0211	0.0136	0.0120	0.0115

Table 9.
Comparative Analysis of Computational Time and Computational Overhead on MNIST Dataset

Techniques	Computational Time(min)	Computational Cost(min)
FL	4.612	0
FL+DP	6.866	2.25
FL+HE	54.99	50.37
FL+SMPC	4.528	-0.084
DP+HE	56.94	52.32
DP+SMPC	106.3	101.68
HE+SMPC	54.70	50.08
PROPOSED	56.99	52.37

Table 10. Comparative Analysis of Performance Metrics on MNIST Dataset

Techniques	Precision	Recall	F1-score
FL	1.0	1.0	1.0
FL+DP	0.81	0.8	0.78
FL+HE	1.0	1.0	1.0
FL+SMPC	1.0	1.0	1.0
DP+HE	0.766	0.75	0.73
DP+SMPC	0.78	0.8	0.76
HE+SMPC	1.0	1.0	1.0
PROPOSED	0.833	0.85	0.826

Table 11.
Comparative Analysis of Accuracy on Fashion-MNIST Dataset

Techniques	Accuracy (%)				
	Epoch-1	Epoch-2	Epoch-3	Epoch-4	Epoch-5
FL	89.0	90.17	91.24	89.87	90.78
FL+DP	69.58	74.55	75.68	77.78	78.63
FL+HE	87.99	89.90	91.38	90.09	91.57
FL+SMPC	85.05	89.12	90.52	90.30	91.35
DP+HE	69.61	76.08	77.45	78.67	77.49
DP+SMPC	68.63	74.53	75.37	75.27	78.27
HE+SMPC	87.43	86.65	90.86	90.02	91.38
PROPOSED	71.67	76.89	77.00	77.37	78.38

Table 7 gives a comparative analysis of the accuracy of classification of different privacy-preserving methods on the MNIST dataset following five training epochs. The basic Federated Learning (FL) model shows consistently high performance, which improves with the increase in epochs, reaching a peak of 98.28% in the fifth epoch and a decline afterward. The FL with Differential Privacy (FL+DP), on the other hand, achieves much lower accuracy with an initial value of 54.34% and an increase to 78.20% at the end, which indicates the effect of strong privacy noise on the performance of the models. Methods, including FL+HE and FL+SMPC, are very accurate, such as standard FL, both of which approach and surpass 98% at the end epoch. The results of hybrid privacy settings such as DP+HE and DP+SMPC have moderate improvements over epochs, but are still lower than the FL-based secure methods. The HE+SMPC structure is also highly performing with over 98% accuracy in subsequent epochs. In the meantime, the proposed technique starts at very low accuracy (52.52%) but gradually grows to be 85.55% in epoch five, which shows a gradual improvement in its accuracy but is still lower than the highest-performance FL-based techniques. Overall, the findings suggest that FL with cryptography, such as HE and SMPC, can be accurate and high, but a more evident trade-off between privacy exists with the notion of differential privacy.

Table 12.

Comparative Analysis of Loss on Fashion-MNIST Dataset

Techniques	LOSS				
	Epoch-1	Epoch-2	Epoch-3	Epoch-4	Epoch-5
FL	0.0079	0.0047	0.0040	0.0035	0.0032
FL+DP	0.0182	0.0151	0.0149	0.0160	0.0158
FL+HE	0.0073	0.0046	0.0039	0.0034	0.0039
FL+SMPC	0.0081	0.0048	0.0040	0.0036	0.0032
DP+HE	0.0174	0.0143	0.0155	0.0158	0.0163
DP+SMPC	0.0187	0.0154	0.0158	0.0159	0.0162
HE+SMPC	0.0077	0.0047	0.0040	0.0035	0.0032
PROPOSED	0.0178	0.0136	0.0148	0.0154	0.0155

Table 8. compares the values of the losses incurred by the different privacy-preserving learning methods on the MNIST data using five training epochs. The standard Federated Learning (FL) model demonstrates the rapid loss reduction and the loss decreases as the epoch goes on by 0.0123 in the first epoch to 0.00010 in the fifth epoch, which shows effective convergence. The same behavior can be observed in FL with Homomorphic Encryption (FL+HE), and with Homomorphic Encryption (HE+SMPC) also. In contrast, the methods based on Differential Privacy, including FL+DP, DP+HE, DP+SMPC and the proposed approach, initialise their methods with relatively large values of the loss and decrease more slowly, continuing to maintain the values at approximately 0.011-0.012 by the final epoch. The trend shows how the trade-off between privacy preservation and optimization performance occurs when privacy mechanisms are increased, the convergence rate decreases and the loss remains. Table 9 compares the computational time and the computational overhead of the techniques that have been evaluated on the MNIST data set.

The efficiency of FL is manifested by the fact that the minimum computational time (4.612 minutes) with no extra overhead is required of the baseline FL approach. Differentiating privacy techniques shows a moderate time and cost increase, but cryptographic techniques such as HE and SMPC have significant increases in computational requirements. The most costly and time-consuming is DP+SMPC, which means that it is associated with significant overheads in processing, as it has integrated privacy mechanisms. The proposed method also has a relatively high cost and time of computation, just like other methods of hybrid computation, which means

that to the cost of efficiency, the proposed method can offer better privacy protection. Overall, the results reveal that although more advanced privacy-preserving combinations are more effective in increasing security, they are characterized by a high level of computational complexity compared to federated learning, which is not focused on privacy.

Table 10. show a comparative evaluation of critical performance measures-precision, recall, and F1-score-achieved by the different privacy-preserving methods on the MNIST data set. The baseline Federated Learning (FL) model, along with FL combined Homomorphic Encryption (FL+HE), FL with Secure Multi-Party Computation (FL+SMPC) and HE+SMPC present perfect performance of 1.0 in all three metrics, which translates to highly accurate and balanced classification performance. On the other hand, strategies that incorporate Differential Privacy, such as FL +DP, DP +HE, and DP +SMPC, indicate relatively low precision, recall, and F1-scores, as it reflects the impact of privacy noise on predictive ability. The proposed one has a moderate performance with a precision of almost 0.833, a recall of 0.85, and an F1-score of approximately 0.826, which is improving over some DP-based hybrids but still below the fully secure FL-based methods. Overall, the results reveal that cryptography privacy mechanisms have an efficient influence on classification in comparison to the impact of distinct privacy mechanisms. Table 11. compares the accuracy of the classification at five training epochs on the Fashion-MNIST dataset. The standard FL algorithm and cryptographic compositions like FL-HE, FL-SMPC and HE+SMPC always have high accuracy, over 90% in the later epochs, and they have stable convergence.

Conversely, the methods based on Differential Privacy -i.e. FL-DP, DP-HE, DP-SMPC, and the proposed method, initially with a low level of accuracy but gradually gaining over time, do not achieve the level of performance of the best methods at the end of the final epoch. Although the offered approach shows an incremental learning progression across epochs, the final accuracy is in the upper-70 percent range, pointing out the trade-off between a more powerful privacy preservation and predictive performance. Combined, these findings help substantiate the thesis that, whereas the hybrid privacy mechanisms can indeed enhance data security, they may also result in performance loss in comparison to the pure federated or cryptography-based learning models. Table 12. presents a comparative analysis of the training loss across multiple epochs on the Fashion-MNIST dataset for different federated learning techniques.

The baseline FL model shows a consistent reduction in loss over successive epochs, indicating stable convergence. When differential privacy (FL+DP) and homomorphic encryption (FL+HE) are incorporated individually, a slight increase in loss values is observed, reflecting the impact of privacy noise and encryption constraints on model optimization. The integration of secure multi-party computation (FL+SMPC) further increases the loss due to additional cryptographic overhead.

Hybrid approaches combining DP, HE, and SMPC exhibit comparatively higher loss values across epochs, demonstrating the trade-off between privacy preservation and learning accuracy. Despite this, the proposed method maintains competitive loss reduction behavior, achieving a balanced performance by preserving privacy while ensuring effective model convergence across all epochs.

Table 13.
Comparative Analysis of Computational Time and Computational Overhead on Fashion-

MNIST Dataset

Techniques	Computational Time(min)	Computational Cost(min)
FL	3.501	0
FL+DP	5.780	2.28
FL+HE	53.66	50.16
FL+SMPC	3.425	-0.075
DP+HE	54.95	51.45
DP+SMPC	5.700	2.2
HE+SMPC	53.46	49.96
PROPOSED	54.94	51.44

Table 14.
Comparative Analysis of Performance Metrics on Fashion-MNIST Dataset

Techniques	Precision	Recall	F1-score
FL	1.0	1.0	1.0
FL+DP	0.722	0.657	0.684
FL+HE	0.968	0.968	0.964
FL+SMPC	0.968	0.968	0.964
DP+HE	0.666	0.638	0.650
DP+SMPC	0.72	0.72	0.72
HE+SMPC	1.0	1.0	1.0
PROPOSED	0.611	0.6388	0.611

Table 15.
Comparative Analysis of Accuracy on CIFAR-10 Dataset

Techniques	Accuracy (%)				
	Epoch-1	Epoch-2	Epoch-3	Epoch-4	Epoch-5
FL	15.87	27.20	33.09	39.81	46.45
FL+DP	10.00	13.11	17.67	22.52	25.24
FL+HE	10.09	21.53	27.52	34.44	43.04
FL+SMPC	12.26	27.29	30.80	43.94	41.40
DP+HE	10.00	14.71	20.58	24.65	25.87
DP+SMPC	16.25	17.95	21.23	24.35	25.73
HE+SMPC	11.52	25.49	24.16	36.21	45.61
PROPOSED	13.21	14.76	19.83	25.82	26.11

Table 16.
Comparative Analysis of loss on CIFAR-10 Dataset

Techniques	LOSS				
	Epoch-1	Epoch-2	Epoch-3	Epoch-4	Epoch-5
FL	0.0359	0.0332	0.0297	0.0256	0.0232
FL+DP	0.0360	0.0359	0.0355	0.0342	0.0327
FL+HE	0.0360	0.0356	0.0318	0.0293	0.0255
FL+SMPC	0.0360	0.0340	0.0303	0.0262	0.0236
DP+HE	0.0360	0.0357	0.0347	0.0330	0.0321
DP+SMPC	0.0360	0.0357	0.0350	0.0336	0.0323
HE+SMPC	0.0360	0.0337	0.0308	0.0278	0.0248
PROPOSED	0.0360	0.0358	0.0349	0.0331	0.0323

Table 17.
Comparative Analysis of Computational Time and Computational Overhead on CIFAR-10 Dataset

Techniques	Computational Time(min)	Computational Cost(min)
FL	3.97	0
FL+DP	7.10	3.13
FL+HE	48.36	44.39
FL+SMPC	4.17	0.2
DP+HE	46.20	42.23
DP+SMPC	7.10	3.13

HE+SMPC	45.06	41.09
PROPOSED	46.28	-0.99

Table 18.
Comparative Analysis of Performance Metrics on CIFAR-10 Dataset

Techniques	Precision	Recall	F1-score
FL	0.418	0.407	0.401
FL+DP	0.203	0.148	0.156
FL+HE	0.507	0.388	0.414
FL+SMPC	0.277	0.296	0.270
DP+HE	0.137	0.133	0.104
DP+SMPC	0.195	0.166	0.156
HE+SMPC	0.296	0.259	0.256
PROPOSED	0.203	0.185	0.1666

The time and overhead of different methods using the Fashion-MNIST data is compared in table 13. The typical FL method provides the shortest computational time, since it does not use privacy-preserving mechanisms. Algorithms, which consider the concepts of differential privacy and homomorphic encryption, presuppose an increase in the computation time due to the noise injection, as well as the encryption algorithms. Secure multi-party computation is a method that results in excessive computation overhead, which highlights the price of cryptographic coordination of participants. Privacy preserving approaches that are of hybrid nature further increase the time taken in implementation as many layers of security have been added simultaneously. The proposed solution, nevertheless, has a streamlined balance, through the reduction of redundant overhead, and still has robust privacy features, making the cost of computation relatively efficient. This confirms the fact that the proposed model has an improved privacy protection with a manageable complex of computation. The following table 14. is a comparative evaluation of different federated learning and privacy-preserving algorithms to the Fashion-MNIST dataset through performance measures, i.e. precision, recall, and F1-score.

The baseline federated learning (FL) model scores perfectly in the three metrics, which implies perfect classification when privacy is not a factor. However, when the privacy/accuracy trade-off is applied, a large reduction in performance is observed, which is typical of the privacy/accuracy trade-off. Methods based on homomorphic encryption (FL+HE and DP+HE) have a higher stability than FL+DP and the values of precision and recall are balanced and close to 0.96. Incorporation with secure multi-party computation (FL+SMPC and DP+SMPC) also improves the robustness, at the expense of the reasonable classification performance. The proposed approach has competitive results among all the approaches assessed, and the values of precision, recall and F1-score indicate balanced results, which is why the proposed approach is an effective method to preserve privacy without significantly reducing the model performance on the Fashion-MNIST dataset. Table 15 is a comparison of the classification accuracy (%) of different methods based on the CIFAR-10 dataset with five training epochs.

The findings reveal that the FL at the baseline has a steady and consistent increase in accuracy with increasing the number of epochs, with the maximum accuracy at Epoch-5. Models such as FL+DP and DP+HE are privacy-enhanced models that, however, initially demonstrate a reduced accuracy due to the noise and encryption overhead; but the performance is gradually increased with further training. A relatively higher learning curve is associated with a method based on secure multi-party computation (FL+SMPC and DP+SMPC), which is more accurate than a purely differential privacy-based method. Interestingly, the proposed approach shows a steady and gradual increase in accuracy over all epochs, better performing than a

number of privacy-preserving approaches. The trend demonstrates that the suggested framework is quite adapted to the problematic image classification tasks such as CIFAR-10. Table 16 offers the comparative analysis of the training loss values of different federated and privacy-preserving methods on the CIFAR-10 dataset, with 5 epochs. The baseline FL model demonstrates that loss is steadily decreasing with the number of epochs, which proves that the model can learn effectively without being constrained by privacy. With differential privacy (FL+DP) the loss values are relatively higher in the initial epochs, with gradual convergence observed. The encryption-based techniques, such as FL+HE and DP+HE, have more stable loss reduction trends, which suggests a higher level of training consistency. Techniques that use secure multi-party computation (FL+SMPC, DP+SMPC) also have a beneficial effect on convergence behavior, in that they tend to have lower values of loss over subsequent epochs.

Surprisingly, the provided method yields one of the lowest values of the loss by Epoch 5, which demonstrates quicker convergence and increased optimization performance. This finding suggests that the proposed framework will be able to achieve privacy and at the same time, efficient learning on complex image data sets like CIFAR-10. A comparison of the computational time and the computational cost of various techniques experimented on the CIFAR-10 dataset is given in Table 17. The baseline FL approach requires a minimal computational overhead, and hence is the most efficient with regard to the time required to execute it. The implementation of privacy mechanisms, though, introduces a great deal of computational demands. The FL+DP and DP+SMPC techniques have a higher computational cost because of the addition of noise and the cryptography operations. Models based on encryption, in particular, DP + HE and FL + HE, have the highest computational cost, which is a measure of the high processing overhead of homomorphic encryption.

On the other hand, SMPC-based solutions portray a less biased trade-off between security and efficiency. The solution proposed has a relatively lower computational cost as compared to most privacy-preserving schemes and yet, a high privacy assurance is offered. This shows that the proposed framework is both computationally efficient and scalable, and thus is appropriate to real-world federated learning applications where large and complex datasets. In Table 18, a comparative analysis of the various federated learning and privacy-preserving methods on the CIFAR-10 dataset in terms of precision, recall and F1-score is presented. The FL model, whose baseline performance is much more successful than certain privacy-enhancing methods. However, the effect of the incorporation of various privacy and encryption systems on the realization of all the evaluation metrics can be observed to decrease significantly. Among the privacy-preserving algorithms, those based on SMPC exhibit a rather good tradeoff between precision and recall as compared to purely DP or HE-based models. The proposed strategy provides competitive and stable outcomes on all measures, meaning that it is effective in terms of whether the classification quality is at an acceptable level and whether the privacy guarantees are high. These results confirm the suitability of the suggested solution to privacy-aware federated learning of complex data such as CIFAR-10.

CONCLUSION

Federated Learning is a paradigm shift of centralized machine learning to decentralized intelligence. Despite being less direct in data sharing, the question of privacy vulnerabilities remains a big issue. This thesis shows that the hybrid privacy-preserving frameworks are a possible solution to this problem. A balanced trade-off

can be created between the model performance, scalability, and confidentiality by combining the Differential Privacy and cryptographic aggregation and secure computation solutions. Federated Learning re-architectures distributed artificial intelligence and is moving computation to a decentralized environment. Nonetheless, privacy issues continue to be the main barrier to mass adoption. It's an approach that allows numerous users to train a single machine learning model with the oversight of a central server, and with their training data stored locally on their device. The approach is relevant in alleviating the risks associated with violations in data privacy.

It is a process by which a pool of clients collaborate towards solving machine learning problems, with a central coordinator being the one who coordinates the entire process. The paper will review the latest advances in privacy-preserving federated learning and discuss them in the context of machine learning. It assesses privacy-related solutions, which are already in existence, such as; secure aggregation, meta-learning, blockchain technology, decentralized training, searchable encryption, and data privacy mechanisms and zero-knowledge proofs. Federated learning (FL) is an emerging technology that can be used in the realm of the intelligence of the Internet of Things. However, the information that is model-related can be shared in FL and reveal the sensitive data of the participants. In this regard, we propose a new privacy-preserving FL framework, which is founded on a new chained secure multiparty computing technique, which we call chain-PPFL. The scheme we are proposing is based mostly on two mechanisms: 1) a single-masking mechanism which protects the information that is exchanged between participants in a serial chain frame and 2) a chained-communication mechanism which allows the masked information to be communicated between participants in a serial chain frame.

We run large-scale experiments with respect to simulation by comparing the training accuracy and the leak defence to other state-of-the-art schemes with two publicly available data sets (MNIST and CIFAR-100). We established data sample distributions (IID and NonIID), and training models (CNN, MLP and L-BFGS) in our experiments. The experiment results show that the chain-PPFL scheme can offer a realistic privacy preservation (which is the same as the various privacy with ϵ to near zero) to FL at the cost of communication, and without compromising the accuracy and convergence rate of the training model. This study shows that privacy-protecting hybrid models can be effective in balancing the privacy needs and the machine learning potential. With further reinforcement of the data protection regulations at the international level, architecture will be integrated into the trustworthy and ethical AI ecosystems. The results of this study are making that vision a reality, as it not only presents theoretical knowledge but also practically implements a next-generation distributed AI framework.

DECLARATIONS

Acknowledgement: We appreciate the generous support from all the contributor to the research and their different affiliations.
Funding: No funding body in the public, private, or nonprofit sectors provided a particular grant for this research.
Availability of data and material: In the approach, the data sources for the variables are stated.
Authors' contributions: Each author participated equally in the creation of this work.
Conflicts of Interest: The authors declare no conflict of interest.
Consent to Participate: Yes
Consent for publication and Ethical approval: Because this study does not include human or animal data, ethical approval is not required for publication. All authors have given their

consent.

REFERENCE AND BIBLIOGRAPHY

A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol," in Proc. 37th Annual International Cryptology Conference (CRYPTO), Santa Barbara, CA, 2017, pp. 357–388.

A. Voit, D. Duenas-Cid, and R. Krimmer, "Blockchain for E-Voting: A Systematic Review," IEEE Transactions on Engineering Management, vol. 68, no. 5, pp. 1470–1485, Oct. 2021.

A., Ahmad, K., Ahsan, M. A., Al-Fuqaha, A., & Qadir, J. (2022). Collaborative federated learning for healthcare: Multi-modal covid-19 diagnosis at the edge. *IEEE Open Journal of the Computer Society*, *3*, 172-184.

A., Uddin, S., Tanweer, H. A., Rasheed, M. A., Ahmed, M., & Murtaza, H. (2021). Data privacy issue in federated learning resolution using block chain. *VFAST Transactions on Software Engineering*, *9*(4), 51-61.

Abbas, G., Basit, A., Ayub, N., Rafique, S., Ali, A., Khan, H., & Hussain, M. Z. (2026). An Enhanced Machine Learning & Deep Learning based Intrusion Detection System for Intelligent Network Security: A Comprehensive Analysis to Avoid Intrusions in Big Data-based IoT Ecosystem. The Asian Bulletin of Big Data Management, 6(1), 26-33.

Abdullah, M. M., Ghafoor, U., Qadeer, Q. B., Khadim, F., Khan, H. S., Ahmad, A., & Khan, H. (2025). An Efficient of Artificial Intelligence based Brain Tumor Diagnosis and Classification: An Advance Medical Diagnosis Approach. The Asian Bulletin of Big Data Management, 5(2), 208-242.

Abdullah, M. M., Khan, H., Farhan, M., & Khadim, F. (2024). An Advance Machine Learning (ML) Approaches for Anomaly Detection based on Network Traffic. Spectrum of engineering sciences, 2(3), 502-527.

Abdullah, M. M., Khan, H., Farhan, M., & Khadim, F. (2024). An Advance Machine Learning (ML) Approaches for Anomaly Detection based on Network Traffic. Spectrum of engineering sciences, 2(3), 502-527.

Adil, M. U., Ali, S., Haider, A., Javed, M. A., & Khan, H. (2024). An Enhanced Analysis of Social Engineering in Cyber Security Research Challenges, Countermeasures: A Survey. The Asian Bulletin of Big Data Management, 4(4), 321-331.

Ahmad, I., Nasim, F., Khawaja, M. F., Naqvi, S. A. A., & Khan, H. (2025). Enhancing IoT Security and Services based on Generative Artificial Intelligence Techniques: A Systematic Analysis based on Emerging Threats, Challenges and future Directions. Spectrum of engineering sciences, 3(2), 1-25.

Ahmad, J., Salman, W., Amin, M., Ali, Z., & Shokat, S. (2024). A Survey on Enhanced Approaches for Cyber Security Challenges Based on Deep Fake Technology in Computing Networks. Spectrum of Engineering Sciences, 2(4), 133-149.

Ahmed, A., Ahmed, N., Ghafoor, U., Rizwan, S. M., Qureshi, R., Khan, H., & Hussain, M. Z. (2025). An Enhanced Textual Review Classification and Sentiment Analysis Approach based on Machine Learning: A Comprehensive Analysis for Text Categorization Approaches. The Asian Bulletin of Big Data Management, 5(4), 259-291.

Ahmed, A., Ahmed, N., Ghafoor, U., Rizwan, S. M., Qureshi, R., Khan, H., & Hussain, M. Z. (2025). An Enhanced Textual Review Classification and Sentiment Analysis Approach based on Machine Learning: A Comprehensive Analysis for Text Categorization Approaches. The Asian Bulletin of Big Data Management, 5(4), 259-291.

Ahmed, A., Javed, M. A., Qureshi, J. N., Khan, H., & Yousaf, H. F. (2024). An insightful machine learning based privacy-preserving technique for federated learning. *The Asian Bulletin of Big Data Management*, *4*(4), 332-343.

Anas, M., Imtiaz, M. A., Saad Khan, A. A., Naghman, N. F., Khan, H., & Albouq, S. AN ADVANCED MACHINE LEARNING (ML) ARCHITECTURE FOR HEART DISEASE DETECTION, PREDICTION AND CLASSIFICATION USING MACHINE LEARNING. Vol.-20, No.-3, March (2025) pp 54 – 72

Aqeel, N., Alam, A., Bhatti, Z., & Amir, A. (2024). A Survey on Tor's Multi Layer Architecture and Web Implications in Dark Web. Spectrum of Engineering Sciences, 2(4), 212-231.

Arshad, S., Ayub, N., Basit, A., Ali, A., Rizwan, S. M., Abdullah, M. M., ... & Hussain, M. Z. An

Efficient Deep Learning Enabled Multimodal Sentiment Analysis based on Neural Networks and Text Mining Architectures for Short-Form Social Media Data: A Comprehensive Analysis.

Asad, M., Moustafa, A., & Ito, T. (2021). Federated learning versus classical machine learning: A convergence comparison. *arXiv preprint arXiv:2107.10976*.

Asghar, M. A., Aslam, A., Bakhet, S., Saleem, M. U., Ahmad, M., Gohar, A., & Khan, H. (2025). An Efficient Integration of Artificial Intelligence-based Mobile Robots in Critical Frames for the Internet of Medical Things (IoMTs) Using (ADP2S) and Convolutional Neural Networks (CNNs). Annual Methodological Archive Research Review, 3(4), 160-183.

Aslam, I., Tariq, W., Nasim, F., Khan, H., Khawaja, M. F., Ahmad, A., & Nawaz, M. S. (2025). A Robust Hybrid Machine Learning based Implications and Preventions of Social Media Blackmailing and Cyber bullying: A Systematic Approach.

Ayub, N., Alghamdi, T., Din, I., Ali, A., Khan, H., Ganiyeva, O., & Makhmudov, S. (2025). An Enhanced Artificial Intelligence and Deep Learning Assisted Breast Cancer Classification and Diagnosis Based on the Internet of Medical Things

Ayub, N., Bakhet, S., Arshad, M. J., Saleem, M. U., Anam, R., & Fuzail, M. Z. (2025). AN ENHANCED MACHINE LEARNING AND BLOCKCHAIN-BASED FRAMEWORK FOR SECURE AND DECENTRALIZED ARTIFICIAL INTELLIGENCE APPLICATIONS IN 6G NETWORKS USING ARTIFICIAL NEURAL NETWORKS (ANNS). Spectrum of Engineering Sciences, 3(4), 348-364.

Ayub, N., Ejaz, A., Hassan, B., Hussain, M. Z., Nadeem, M., Sabir, L., & Fatima, S. (2025). An Efficient Machine Learning And Deep Learning Based Deep Packet Security Framework For Detection Of Computing Network Faults In The Iots. Spectrum of Engineering Sciences, 3(5), 659-674.

Ayub, N., Habib, Z., Bakhet, S., Riaz, S., Rizwan, S. M., Abid, M., ... & Khan, H. (2025). An Optimal Ai & Deep Learning Mechanism For Mitigating Hacking Threat Identification Using Secure Network Infrastructure Based On Linux And Software-Defined Network (Sdn). Spectrum of Engineering Sciences, 3(5), 675-687.

Ayub, N., Imtiaz, M. A., Ali, E., Alqahtani, A. M., Ali, A., Ashurov, M., ... & Law, F. L. (2025). A Decision Framework for Intra Task Fixed Priority INTEL PXA270 Distributed Architecture for Soft RT-Applications Based on Deep Learning. Engineering, Technology & Applied Science Research, 15(3), 23553-23558.

Bacha, A., Sehar, H., Naseem, S., & Khan, M. I. (2024). FEDERATED LEARNING FOR THREAT INTELLIGENCE SHARING: A PRIVACY-PRESERVING COLLABORATIVE DEFENSE MODEL. Spectrum of Engineering Sciences, 656-664.

Basit, A. (2026). An Enhanced Machine Learning & Deep Learning based Intrusion Detection System for Intelligent Network Security: A Comprehensive Analysis to Avoid Intrusions in Big Data-based IoT Ecosystem.

Criado, M.F.; Casado, F.E.; Iglesias, R.; Regueiro, C.V.; Barro, S. Non-iid data and continual learning processes in federated learning: A long road ahead. Inf. Fusion 2022, 88, 263–280.

Fakhar, M. H., Baig, M. Z., Ali, A., Rana, M. T. A., Khan, H., Afzal, W., ... & Albouq, S. (2024). A Deep Learning-based Architecture for Diabetes Detection, Prediction, and Classification. Engineering, Technology & Applied Science Research, 14(5), 17501-17506.

Farooq, I., Ahmed, S. A., Ali, A., Warraich, M. A., Aqeel, M., & Khan, H. (2024). Enhanced Classification of Networks Encrypted Traffic: A Conceptual Analysis of Security Assessments, Implementation, Trends and Future Directions. The Asian Bulletin of Big Data Management, 4(4), 500-522.

Farooq, I., Ghafoor, U., Umer, S., Ali, A., Shahid, A. K., & Khan, H. (2025). An Efficient Big Data Security and Privacy in Healthcare for Enhancing Remote Sensing and Monitoring: A Technological Perspective based on ACL for Preserving Big Data Analytics in Cloud. The Asian Bulletin of Big Data Management, 5(4), 231-258.

Farooq, M., Younas, R. M. F., Qureshi, J. N., Haider, A., & Nasim, F. (2025). Cyber security risks in DBMS: Strategies to mitigate data security threats: A systematic review. Spectrum of engineering sciences, 3(1), 268-290.

Fatima, M., Ali, A., Ahmad, M., Nisa, F. U., Khan, H., & Raheem, M. A. U. Enhancing The Resilience Of Iot Networks: Strategies And Measures For Mitigating Ddos Attacks. Cont.& Math. Sci., Vol.-19, No.-10, 129-152, October 2024 https://jmcms.s3.amazonaws.com/wp-content/uploads/2024/10/10072102/jmcms-2410025-ENHANCING-THE-RESILIENCE-OF-IOT-NETWORKS-MF-HK.pdf

Fawy, K. F., Rodriguez-Ortiz, G., Ali, A., Jadeja, Y., Khan, H., Pathak, P. K., ... & Rahman, J. U. (2025). Catalytic exploration metallic and nonmetallic nano-catalysts, properties, role in photoelectrochemistry for sustainable applications. Reviews in Inorganic Chemistry, (0).

Foley, P., Sheller, M. J., Edwards, B., Pati, S., Riviera, W., Sharma, M., ... & Bakas, S. (2022). OpenFL: the open federated learning library. Physics in Medicine & Biology, 67(21), 214001.

Ghafoor, U., Ayub, N., Yaseen, A., Anas, M., Farooq, I., Khan, S., & Naghman, N. F. (2025). AI Assisted Heart Disease Prediction and Classification and Segmentation based on PIMA and UCI Machine Learning Datasets. Annual Methodological Archive Research Review, 3(7), 248-276.

Goetz, J., Malik, K., Bui, D., Moon, S., Liu, H., & Kumar, A. (2019). Active federated learning. arXiv preprint arXiv:1909.12641.

Gordon, T. Diabetes, blood lipids, and the role of obesity in coronary heart disease risk for women. Ann. Intern. Med. 87, 393 (1977).

Guan, H., Yap, P. T., Bozoki, A., & Liu, M. (2024). Federated learning for medical image analysis: A survey. Pattern recognition, 151, 110424.

Gul, W., Nawaz, A., Hamaz, M. T., & Khan, H. AN EFFICIENT MODEL FOR THE SELECTION OF LEADERSHIP COMPETENCIES AND PERFORMANCE IMPROVEMENT FOR THE SUCCESS OF TRANSPORTATION PROJECTS, JOURNAL OF MECHANICS OF CONTINUA AND MATHEMATICAL SCIENCES Vol.-16, No.-5, May (2021) pp 49-65 https://doi.org/10.26782/jmcms.2021.05.00005

Gularte, K.H.M.; Vargas, J.A.R.; Da Costa, J.P.J.; Da Silva, A.A.S.; Santos embedded systems", In 2018 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-8, Sep. 2018

H. Khan, I. Uddin, A. Ali, M. Husain, "An Optimal DPM Based Energy-Aware Task Scheduling for Performance Enhancement in Embedded MPSoC", Computers, Materials & Continua., vol. 74, no. 1, pp. 2097-2113, Sep. 2023

H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Dec. 2018

H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, A. Saleem, "Performance Evaluation for Secure DES-Algorithm Based Authentication & Counter Measures for Internet Mobile Host Protocol", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 181-185, July. 2018

Hamayun Khan, Sheeraz Ahmed,S. Farhan Haider Shah,Rehan Ali Khan,Zeeshan Najam,Hasnain Abbas,Asif Nawaz,Zubair Aslam Khan, JOURNAL OF MECHANICS OF CONTINUA AND MATHEMATICAL SCIENCES, Vol.-15, No.-8, August (2020) pp 628-646 https://doi.org/10.26782/jmcms.2020.08.00053

Hashmi, U., & ZeeshanNajam, S. A. (2023). Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems. Journal of Mechanics of Continua and Mathematical Sciences, 14(4), 442-452.

Hassan, A., Khan, H., Ali, A., Sajid, A., Husain, M., Ali, M., ... & Fakhar, H. (2024). An Enhanced Lung Cancer Identification and Classification Based on Advanced Deep Learning and Convolutional Neural Network. Bulletin of Business and Economics (BBE), 13(2), 136-141.

Imtiaz, M. A., Amir, A., Bakhet, S., Siddique, H., & Rizwan, S. M. (2025). An Optimal Diabetic Retinopathy Detection and Classification Approach based on integrated Hybrid Convolutional Neural Networks (CNNs). Spectrum of Engineering Sciences, 3(2).

J. Bonneau, "Why Buy When You Can Rent? Bribery and Vote Buying in Blockchain Voting," in Proc. 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), London, UK, 2018, pp. 123–130.

Jabeen, T., Mehmood, Y., Khan, H., Nasim, M. F., & Naqvi, S. A. A. (2025). Identity Theft and Data Breaches How Stolen Data Circulates on the Dark Web: A Systematic Approach. Spectrum of engineering sciences, 3(1), 143-161.

Jabeen, T., Mehmood, Y., Khan, H., Nasim, M.F. and Naqvi, S.A.A., 2025. Identity Theft and Data Breaches How Stolen Data Circulates on the Dark Web: A Systematic Approach. Spectrum of engineering sciences, 3(1), pp.143-161.

Javed, M. A., Ahmad, M., Ahmed, J., Rizwan, S. M., & Tariq, A. (2025). An Enhanced Machine Learning based Data Privacy and Security Mitigation Technique: An Intelligent Federated Learning (FL) Model for Intrusion Detection and Classification System for Cyber-Physical Systems in Internet of Things (IoTs). Spectrum of Engineering Sciences, 3(2), 377-401.

Javed, M. A., Anjum, M., Ahmed, H. A., Ali, A., Shahzad, H. M., Khan, H., & Alshahrani, A. M. (2024). Leveraging Convolutional Neural Network (CNN)-based Auto Encoders for Enhanced Anomaly Detection in High-Dimensional Datasets. Engineering, Technology & Applied Science Research, 14(6), 17894-17899.

K. Croman et al., "On Scaling Decentralized Blockchains," in Proc. 20th International Conference on Financial Cryptography and Data Security (FC), Christ Church, Barbados, 2016, pp. 106–125.

Kang, J., Xiong, Z., Niyato, D., Zou, Y., Zhang, Y., & Guizani, M. (2020). Reliable federated learning for mobile networks. *IEEE Wireless Communications*, *27*(2), 72-80.

Khan, A. Ali, S. Alshmrany, "Energy-Efficient Scheduling Based on Task Migration Policy Using DPM for Homogeneous MPSoCs", Computers, Materials & Continua., vol. 74, no. 1, pp. 965-981, Apr. 2023

Khan, A. K., Bakhet, S., Javed, A., Rizwan, S. M., & Khan, H. (2025). Framework for Predicting Customer Sentiment Aware Queries and Results in Search Using Oracle and Machine Learning. Spectrum of Engineering Sciences, 3(2), 588-617.

Khan, A. Yasmeen, S. Jan, U. Hashmi, "Enhanced Resource Leveling Indynamic Power Management Techniqueof Improvement In Performance For Multi-Core Processors" ,Journal of Mechanics of Continua and Mathematical Sciences., vol. 6, no. 14, pp 956-972, Sep. 2019

Khan, H. M. S., Hayat, C. M. A., Tayyab, H., & Ali, K. (2024). An Enhanced Cost Effective and Scalable Network Architecture for Data Centers. Spectrum of Engineering Sciences, 2(4), 1-32.

Khan, H., Imtiaz, M. A., Siddique, H., Rana, M. T. A., Ali, A., Baig, M. Z., ... & Alsaawy, Y. (2025). An Enhanced Task Migration Technique Based on Convolutional Neural Network in Machine Learning Framework.

Khan, H., Usman, R., Ahmed, B., Hashimi, U., Najam, Z., & Ahmad, S. (2019). Thermal-aware real-time task schedulabilty test for energy and power system optimization using homogeneous cache hierarchy of multi-core systems. Journal of Mechanics of Continua and Mathematical Sciences, 14(4), 442-452.

Khan, Q. Bashir, M. U. Hashmi, "Scheduling based energy optimization technique in multiprocessor

Khawar, M. W., Ayub, N., Shaheen, S., Iftikhar, B., Masood, H., Ahmad, A., & Khan, H. (2025). An Efficient system based on Artificial Intelligence for the Detection and Mitigation of network Intrusion using encrypted traffic protocols: A Systematic Approach. Annual Methodological Archive Research Review, 3(11), 32-71.

Khawar, M. W., Salman, W., Shaheen, S., Shakil, A., Iftikhar, F., & Faisal, K. M. I. (2024). Investigating the most effective AI/ML-based strategies for predictive network maintenance to minimize downtime and enhance service reliability. Spectrum of Engineering Sciences, 2(4), 115-132.

Li, H.; Luo, L.; Wang, H. Federated learning on non-independent and identically distributed data. In Proceedings of the Third International Conference on Machine Learning and Computer Application (ICMLCA 2022), Shenyang, China, 16–18 December 2023; SPIE: Bellingham, WA, USA; pp. 154–162.

Li, L., Fan, Y., Tse, M., & Lin, K. Y. (2020). A review of applications in federated learning. Computers & Industrial Engineering, 149, 106854.

Li, T., Sahu, A. K., Talwalkar, A., & Smith, V. (2020). Federated learning: Challenges, methods, and future directions. IEEE signal processing magazine, 37(3), 50-60.

Liang, Y., Ur Rahman, S., Shafaqat, A., Ali, A., Ali, M. S. E., & Khan, H. (2024). Assessing sustainable development in E-7 countries: technology innovation, and energy consumption drivers of green growth and environment. Scientific Reports, 14(1), 28636.

Liaqat, M. S., Sharif, N., Ali, A., Khan, H., Ahmed, H. N., & Khan, H. (2024). An Optimal Analysis of Cloud-based Secure Web Applications: A Systematic Exploration based on Emerging Threats, Pitfalls and Countermeasures. Spectrum of engineering sciences, 2(5), 427-457.

M. Gondal, Z. Hameed, M. U. Shah, H. Khan, "Cavitation phenomenon and its effects in Francis turbines and amassed adeptness of hydel power plant", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-9, Mar. 2019

Mahmood, F., Shehroz, M., Ansari, Z., & Rauf, F. (2024). A Survey of Software-Defined Networks Based on Advance Machine Learning Based Techniques. Spectrum of Engineering Sciences, 2(4), 232-257.

Mammen, P. M. (2021). Federated learning: Opportunities and challenges. arXiv preprint arXiv:2101.05428.

Maqsood, M., Dar, M. M., Javed, M. A., & Khan, H. (2024). A Survey on the Internet of Medical Things (IOMT) Privacy and Security: Challenges Solutions and Future from a New Perspective. The Asian Bulletin of Big Data Management, 4(4), 355-368.

Mohri, M., Sivek, G., & Suresh, A. T. (2019, May). Agnostic federated learning. In International conference on machine learning (pp. 4615-4625). PMLR.

Muhammad Anas,Muhammad Atif Imtiaz,Saad Khan,Arshad Ali,Noor Fatima Naghman,Hamayun Khan,Sami Albouq, AN ADVANCED MACHINE LEARNING (ML) ARCHITECTURE FOR HEART DISEASE DETECTION, PREDICTION AND CLASSIFICATION USING MACHINE LEARNING, Cont.& Math. Sci, Vol.20, No.3 https://doi.org/10.26782/jmcms.2025.03.00005

Mujtaba, A., Zulfiqar, M., Azhar, M. U., Ali, S., Ali, A., & Khan, H. (2025). ML-based Fileless Malware Threats Analysis for the Detection of Cyber security Attack based on Memory Forensics: A Survey. The Asian Bulletin of Big Data Management, 5(1), 1-14.

Mumtaz, J., Bakhet, S., Javed, A., Naz, A., Rashail, M., & Khan, H. (2025). An Intelligent Diagnosis and Tumor Segmentation Method based on MRI Images Using Pre-trained Deep Convolutional Neural Networks (CNNs). The Asian Bulletin of Big Data Management, 5(1), 147-163

Mumtaz, J., Rehman, A. U., Khan, H., Din, I. U., & Tariq, I. Security and Performance Comparison of Window and Linux: A Systematic Literature Review. Securing the Digital Realm, 272-280.

Musharraf, S. T., Masab, M. M., Ayub, N., Murtaza, S., Ullah, H., Ahmad, A., ... & Khan, H. (2025). An Efficient Artificial Intelligence-Based Early Prediction of Heart Attack Using Deep Learning CNN and SVM Models: https://doi. org/10.5281/zenodo. 17551611. Annual Methodological Archive Research Review, 3(10), 265-301.

Mustafa, M., Ali, M., Javed, M. A., Khan, H., Iqbal, M. W., & Ruk, S. A. (2024). Berries of Low-Cost Smart Irrigation Systems for Water Management an IoT Approach. Bulletin of Business and Economics (BBE), 13(3), 508-514.

Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

Naveed, A., Khan, H., Imtiaz, Z., Hassan, W., & Fareed, U. (2024). Application and Ethical Aspects of Machine Learning Techniques in Networking: A Review. Spectrum of engineering sciences, 2(3), 455-501.

Nawaz, S., Salman, W., Shahid, U., Khokhar, M. L., Iqbal, M. Z., & Hamid, A. (2024). A Survey on Latest Trends and Technologies of Computer Systems Network. Spectrum of

Engineering Sciences, 2(4), 85-114.
Naz, H. Khan, I. Ud Din, A. Ali, and M. Husain, "An Efficient Optimization System for Early Breast Cancer Diagnosis based on Internet of Medical Things and Deep Learning", Eng. Technol. Appl. Sci. Res., vol. 14, no. 4, pp. 15957–15962, Aug. 2024
Niaz, H. U., Qadeer, Q. B. Q., Niaz, H., Mansib, H., Awais, M., & Khan, H. (2025). Artificial Intelligence Assisted Autonomous Unmanned Aerial Vehicles (UAVs) and Aerial drones based on Machine Vision for Enhancing Remote Sensing of Precision crop Health Monitoring. The Asian Bulletin of Big Data Management, 5(4), 155-177.
Noor, H., Khan, H., Din, I. U., Tariq, M. I., Amin, M. N., & Fatima, M. Virtual Memory Management Techniques. Securing the Digital Realm, 126-137.
Noor, H., Khan, H., Din, I. U., Tarq, M. I., Amin, M. N., & Fatima, M. (2025). 12 Virtual Memory Management. Securing the Digital Realm: Advances in Hardware and Software Security, Communication, and Forensics, 126.
P. De Filippi and S. Loveluck, "The Invisible Politics of Bitcoin: Governance Crisis of a Decentralised Infrastructure," Internet Policy Review, vol. 5, no. 3, pp. 1–28, Sep. 2016.
Rafay, A., Salman, W., Yahya, G., & Malik, U. (2024). SD Network based on Machine Learning: An Overview of Applications and Solutions. Spectrum of Engineering Sciences, 2(4), 150-165.
Rahman, M. U., Khan, S., Khan, H., Ali, A., & Sarwar, F. (2024). Computational chemistry unveiled: a critical analysis of theoretical coordination chemistry and nanostructured materials. Chemical Product and Process Modeling, 19(4), 473-515.
Ramzan, M. S., Nasim, F., Ahmed, H. N., Farooq, U., Nawaz, M. S., Bukhari, S. K. H., & Khan, H. (2025). An Innovative Machine Learning based end-to-end Data Security Framework in Emerging Cloud Computing Databases and Integrated Paradigms: Analysis on Taxonomy, challenges, and Opportunities. Spectrum of engineering sciences, 3(2), 90-125.
Raza, A., Khan, H., & Rehman, S. U. (2023). Computational Analysis of Nanomaterials for Energy Storage. International Journal of Advanced Sciences and Computing, 143-154.
Rieke, N., Hancox, J., Li, W., Milletari, F., Roth, H. R., Albarqouni, S., ... & Cardoso, M. J. (2020). The future of digital health with federated learning. NPJ digital medicine, 3(1), 119.
Rumelhart, D.E.; Hinton, G.E.; Williams, R.J. Learning representations by back-propagating errors. Nature 1986, 323, 533–536.
S. Khan, I. Ullah, H. Khan, F. U. Rahman, M. U. Rahman, M. A. Saleem, A. Ullah, "Green synthesis of AgNPs from leaves extract of Salvia Sclarea, their characterization, antibacterial activity, and catalytic reduction ability", Zeitschrift für Physikalische Chemie., vol. 238, no. 5, pp. 931-947, May. 2024
Saeed, N., Ayub, N., Haider, A., Ghafoor, U., Ali, A., Wahab, A., ... & Hussain, M. Z. Exploration of Behavior-Based Advanced Persistent Threat (APT) Detection: A Systematic Analysis based on Open CTI, MITRE ATT&CK, and Machine Learning.
Saif, S., Hamayun Khan, A. A., Albouq, S., Hussain, M. Z., Hasan, M. Z., Uddin, I., ... & Husain, M. AN EFFICIENT MACHINE LEARNING-BASED DETECTION AND PREDICTION MECHANISM FOR CYBER THREATS USING INTELLIGENT FRAMEWORK IN IOTS. Vol.-15, No.-8, August (2024) pp 191-206
Sarwar, H. Khan, I. Uddin, R. Waleed, S. Tariq, "An Efficient E-Commerce Web Platform Based on Deep Integration of MEAN Stack Technologies", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 447-453, Jun. 2023
Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan, "Penetration testing active reconnaissance phase–optimized port scanning with nmap tool", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-6, Nov. 2019
Sultan, H., Rahman, S. U., Munir, F., Ali, A., Younas, S., & Khan, H. (2025). Institutional dynamics, innovation, and environmental outcomes: a panel NARDL analysis of BRICS nations. Environment, Development and Sustainability, 1-43.
U. Hashmi, S. A. ZeeshanNajam, "Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no.

4, pp. 442-452, Mar. 2023

Vidal Filho, et al. Safeguarding the V2X Pathways: Exploring the Cybersecurity Landscape through Systematic Literature Review. IEEE Access 2024, 12, 72871–72895.

Waleed, R., Ali, A., Tariq, S., Mustafa, G., Sarwar, H., Saif, S., ... & Uddin, I. (2024). An Efficient Artificial Intelligence (AI) and Internet of Things (IoT's) Based MEAN Stack Technology Applications. Bulletin of Business and Economics (BBE), 13(2), 200-206.

Wen, J., Zhang, Z., Lan, Y., Cui, Z., Cai, J., & Zhang, W. (2023). A survey on federated learning: challenges and applications. *International journal of machine learning and cybernetics*, *14*(2), 513-535.

Wen, J., Zhang, Z., Lan, Y., Cui, Z., Cai, J., & Zhang, W. (2023). A survey on federated learning: challenges and applications. International journal of machine learning and cybernetics, 14(2), 513-535.

Y. A. Khan, M. Ibrahim, M. Ali, H. Khan, E. Mustafa, "Cost Benefit Based Analytical Study of Automatic Meter Reading (AMR) and Blind Meter Reading (BMR) used by PESCO (WAPDA)", In 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-7, Aug. 2020

Y. A. Khan, U. Khalil, H. Khan, A. Uddin, S. Ahmed, "Power flow control by unified power flow controller",Engineering, Technology & Applied Science Research., vol. 9, no. 2, pp. 3900-3904, Feb. 2019

Yousaf, M., Khalid, F., Saleem, M. U., Din, M. U., Shahid, A. K., & Khan, H. (2025). A Deep Learning-Based Enhanced Sentiment Classification and Consistency Analysis of Queries and Results in Search Using Oracle Hybrid Feature Extraction. Spectrum of Engineering Sciences, 3(3), 99-121.

Yurdem, B., Kuzlu, M., Gullu, M. K., Catak, F. O., & Tabassum, M. (2024). Federated learning: Overview, strategies, applications, tools and future directions. Heliyon, 10(19).

Zaheer, M., Azeem, M. H., Afzal, Z., & Karim, H. (2024). Critical Evaluation of Data Privacy and Security Threats in Federated Learning: Issues and Challenges Related to Privacy and Security in IoT. Spectrum of Engineering Sciences, 2(5), 458-479.

Zainab, Khan, H., Din, I. U., Tariq, M. I., Khalid, A., & Naz, A. (2023, May). An Efficient Implementation of an IoT-Based Smart Home Security System. In International Conference on Computing & Emerging Technologies (pp. 249-259). Cham: Springer Nature Switzerland.