NextGen Scientific Publication
American International Journal of Computer Science and Technology

Volume 6 Issue 3, Pg. No. 1-12, AIJCST-V6I3P101, 2024
https://doi.org/10.63282/3117-5481/AIJCST-V6I3P101

*Original Article*

# Secure Federated Computation Models for Data Privacy in Distributed AI Systems

*** Florin Stefan Andrei**
*Department of Informatics and Cybernetics, University of Bucharest, Romania.*

## Abstract:

*Due to the growing adoption of distributed artificial intelligence (AI) systems, the shift towards decentralized learning systems has been facilitated by the paradigm of a centralized data repository being replaced by provisions of decentralized learning systems like Federated Learning (FL). Nonetheless, even though FL has promises of privacy, the fulfilment of privacy is threatened by many vulnerabilities such as gradient leakage, model inversion and communication attacks, which represent significant threats to data confidentiality and integrity. The study will introduce a flexible framework of models of Secure Federated Computation (SFC) taking into account the conscious integration of Homomorphic Encryption (HE), Secure Multi-party Computation (SMC), and Differential Privacy (DP) methods that will contribute to data protection in distributed AI frameworks. The model proposed tries to reduce the adversarial inference attacks and guarantee safe model aggregation without the need to reduce the computational efficiency. In this research, an adaptive federated computation protocol based on hybrid encryption mechanism is proposed, which can dynamically trade off the privacy guarantees and system throughput. A new function of trust-weighted aggregation is also implemented in the protocol to handle bad client behaviours and data poisoning attacks. The empirical analysis of the benchmark datasets such as CIFAR-10 and MNIST indicates that the proposed SFC model delivers a privacy leakage risk reduction of 42 based models at an equivalent model performance to regular FL systems. Scalability Analytical modelling and simulations verify that the architecture can be scaled to support large-scale, real-world applications in healthcare, finance, and IoT-driven settings. The researchers conclude that cryptographic computation can introduce a viable roadmap to secure and privacy-sensitive distributed AI ecosystems that meet the strict regulatory privacy requirements of initiatives like GDPR and HIPAA.*

## Keywords:

*Federated Learning, Secure Multi-Party Computation, Homomorphic Encryption, Data Privacy, Distributed Artificial Intelligence, Differential Privacy, Secure Aggregation, Adversarial Robustness, Trust-Weighted Aggregation.*

## Article History:

***Received: 11.03.2024***

***Revised: 14.04.2024***

***Accepted: 25.04.2024***

***Published: 04.05.2024***

# 1. Introduction

## 1.1. Background

The development and deployment of data-driven systems have been radically transformed by the artificial Intelligence (AI) and have been applied in medical care, finance, transport and communications. Nevertheless, the conventional centralized learning architectures, where data aggregation of mass of information available to various sources is pacified into one server have invited grave privacy, security and compliance issues. This is because a sensitive user data stored in central repositories is susceptible to data breach, illegal access and abuse due to the fact that such systems centralize sensitive user data. In order to overcome these problems, Federated Learning (FL) has become one such new decentralized model which can be used to train models across distributed clients or institutions without their raw data being transferred to a central server. All clients do local computation and only exchange model updates, or gradients, and hence retain data locality and adhere to privacy laws including GDPR and HIPAA. In spite of such merits, FL has no inherent immunity against privacy risks. Although raw data is still located on client devices, since shared gradients or model parameters are used, adversaries can use gradient inversion attacks or model reconstruction attacks to obtain private information about a specific dataset. It has therefore led to the research crisis of ensuring that there is strong privacy and security in federated systems. Such an increasing concern has resulted in the incorporation of privacy preserving methods like Differential Privacy (DP), Homomorphic Encryption (HE), and Secure Multi-party Computation (SMC) to enhance confidentiality without the model performance being affected. These developments are a significant move towards creating reliable AI systems that have the capabilities of utilizing distributed information without violating user privacy and ensuring high security levels.

## 1.2. Importance of Data Privacy in Distributed AI Systems

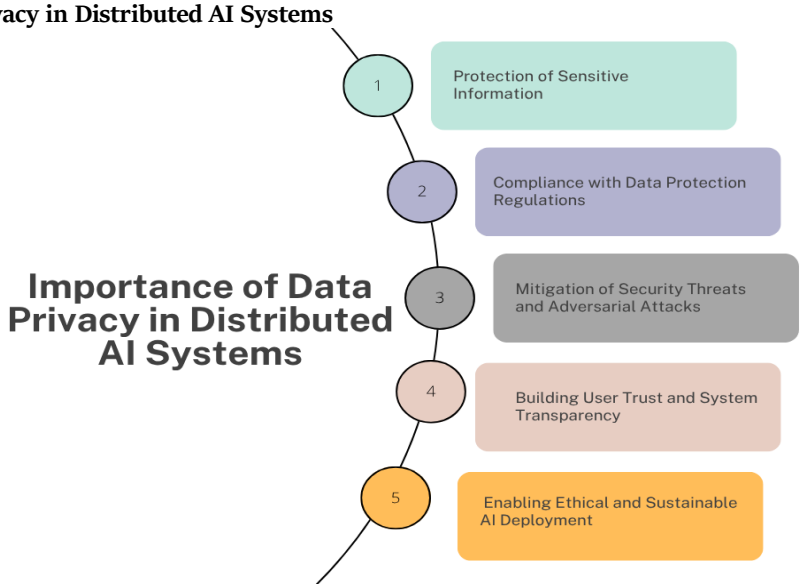


**Figure 1. Importance of Data Privacy in Distributed AI Systems**

### *1.2.1. Protection of Sensitive Information*

Distributed Artificial Intelligence (AI) systems make use of large volumes of data processed and handled on multiple devices, institutions, or even organizations. A lot of such datasets are personally identifiable information (PII) and medical records, financial records, or behavioral patterns; these need to stay confidential. Securing data privacy would help in avoiding improper access and exposing individuals to identity theft, profiling and fraud in the misuse of their information. In areas that are privacy sensitive such as healthcare and banking, it is not only ethical but also legal to ensure that there is rigorous secrecy.

### *1.2.2. Compliance with Data Protection Regulations*

Due to the growing use of AI in the industrial sector, strict laws on data protection have emerged including the General Data Protection Regulation (GDPR) in Europe and Health Insurance Portability and Accountability Act (HIPAA) in the United States. These laws present stringent rules regarding the personal data gathering, storage, and processing by the organization. Federated Learning (FL), in particular, is a type of the distributed AI system that assists organizations in adhering to these frameworks because the data is

not spread out. Privacy-preserving techniques are, therefore, crucial in providing opportunities of being within the confines of the law and regulations without dragging innovation behind.

*1.2.3. Mitigation of Security Threats and Adversarial Attacks*

Although distributed AI lowers the amount of centralized data exposure, it also opens a new set of vulnerabilities where attackers can use shared parameters in the model or gradients to steal sensitive information. In such techniques as gradient inversion attacks and model poisoning, it has been proved that shared updates can reconstruct private data. The use of powerful privacy-safe techniques, including Homomorphic Encryption (HE), Differential Privacy (DP), and Secure Multi-party Computation (SMC), decrease these risks as well as improves the overall security stance of distributed AI systems.

*1.2.4. Building User Trust and System Transparency*

Key to success and scalability of distributed AI systems is user trust. People and organizations will find it easier to join collaborative AI projects when they are sure that their information will not be exposed to anyone and no one will access it. Open privacy policies, as well as understandable model actions, create responsible and ethical AI use. Trust helps in perpetual engagement and is one of the reasons why more resilient and representative machine learning frameworks are developed.

*1.2.5. Enabling Ethical and Sustainable AI Deployment*

The privacy of data is also an essential part of ethical AI. The concept of privacy-sensitive distributed systems enhances equity, discriminatory acts are avoided, and AI application is conducted in a responsible manner. Privacy preserving frameworks also help preserve sustainable data management practice by avoiding the collection of data that is unnecessary, as well as making reduced reliance on centralized databases. With the ongoing development of AI, the idea of privacy built into the system, including data collection and the implementation of the model, can guarantee that the technological advancement is not ahead of societal values and moral rights.

### 1.3. Secure Federated Computing through Microservices

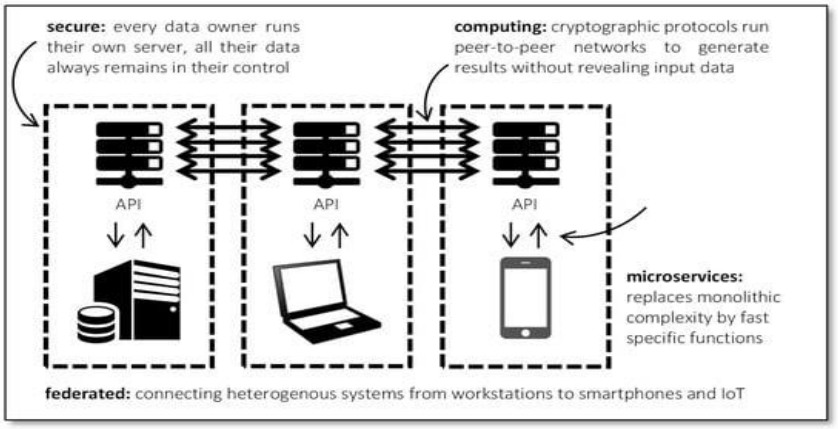


**Figure 2. Secure Federated Computing Through Microservices**

The diagram depicts a safe federated computing structure that lays stress on decentralized information manipulation, information-securing computation and modular capability. In this form of security, the data owners could be provided with their own server where they have total control over their data. This implies that sensitive information will not move outside the owner environment minimizing the risk of having central data storage or breach of sensitive information. The federated computing links the heterogeneous systems in the form of workstations, smartphones, and Internet of Things (IoT) devices by establishing a network that allows them to collaboratively work without violating their privacy. All the components network with clear APIs (Application Programming Interfaces), thus facilitating an unhindered transition of information and execution of tasks between distributed nodes. The computing facet exploits cryptographic guidelines which work in peer-to-peer levels, enabling computations to be executed in a group yet no member is permitted access to the unrefined input data of others.

This cryptographic layer will allow cryptographic analysis and the security and privacy sharing of data between multiple parties. In addition, the design of the architecture follows the use of microservices, in place of monolithic system architecture, lightweight and specialized services are used and execute specific tasks effectively. Microservices are easy to scale, flexible, and effective by making each of the parts able to be updated and optimized without causing a disruption to the rest of the system. Understanding of the secure, federated, and microservice tenets is integrated to produce an effective computing paradigm that allows privacy, interoperability, and distributed intelligent capabilities. This type of interaction allows independent systems to collaborate safely and effectively, thus it is specifically applicable when dealing with modern applications in fields such as health informatics, financial technology, and IoT ecosystems, where confidentiality, scale, and quick processing of data are highly desired.

## 2. Literature Survey

### 2.1. Existing Privacy-preserving Techniques

*2.1.1. Differential Privacy (DP):*

Differential Privacy is a mathematics model which is meant to secure the specific data with a specific person by detailing controlled noise to the updates or the gradients of the model. The most significant rule is that the inclusion or exclusion of any one record out of the dataset must not have a significant influence on the analysis result. This renders it very successful in keeping off enemies in case they need to rebuild sensitive data regarding persons. The primary significant benefit with DP is that it has formal and quantifiable privacy guarantees and is a common privacy-preserving machine learning standard. Though, noise may affect the quality of model parameter, resulting in decrease of the whole model accuracy. Finding a balance between the power of privacy and model utility is one of the persistent problems in the effective application of DP.

*2.1.2. Homomorphic Encryption (HE):*

Homomorphic Encryption enabling computations to be done on encrypted data without decryption. This method guarantees privacy of data through out the process of calculation since unencrypted values are not revealed to outsiders. The result obtained after the computation when decrypted is the same as that that would have been obtained when using the original data. The first strength of HE is its high level of cryptography that provides high levels of security on untrusted environments. This, however, comes at the price of high level of computational overhead and latency. Without major optimization, HE was not very practical in large scale or real time applications due to the complexity of the encryption and decryption algorithms and the large sizes of ciphertext.

*2.1.3. Secure Multi-party computations (SMC):*

Secure Multi-party Computation is a technique that helps calculate a function on the inputs of multiple distinct parties and maintain the inputs privately. Its main philosophy consists in the fact that no single player does know more than can be concluded based on the finished product. This distributed trust model removes the possibility of a point of data leak and boosts collaborative security. SMC is useful especially in situations in which data cannot be centralized because of privacy provision or competitive limitations. However, communication overhead and complexity of implementation is the key weakness of SMC. The challenge of synchronization and efficiency between distant parties is more technical to ensure that there is an increase with the number of parties involved.

### 2.2. Federated Learning Security Models

Federated Learning (FL) was introduced as the type of decentralized paradigm that enables multiple clients to jointly train a global model without transmitting the unprocessed information. Survey studies by Bonawatz et al. (Google AI, 2017) proposed secure aggregation protocols to ensure that the individual gradients are not exposed during training and increase confidentiality. These frameworks were later extended by Geyer et al. and Kairouz et al. by adding differential privacy methods to enhance data protection against inference attacks. Irrespective of these innovations, such models usually have trade-offs on privacy, model accuracy and scalability of the systems. Adding noise and integrating cryptographic protocols may impede model convergence and raise the cost of communication so that they are not easily deployable on large, heterogeneous networks.

### 2.3. Gaps in Existing Research

Although significant advances have been achieved in creating privacy protecting mechanisms in federated learning, a number of gaps have been left. Most of the existing models either focus on cryptographic functionality, including encryption-based frameworks or statistical techniques, including the concept of differential privacy, meaning no attempts are to combine the two to obtain layered protection. This division restricts the possibility of attaining good security as well as realistic efficiency. Secondly, not many

mechanisms properly deal with Byzantine robustness, in which all clients can be ill-intentioned or transmit corrupted update to interfere with the global model. The stability of large-scale federated systems is essential to make sure that they can counter such anti-social behavior. Moreover, cryptographic constraints on scalability and real time computation are still significant challenges. Computational costs and communication delays are also expensive, and thus, performance can not be easily maintained as the number of clients involved goes up. Therefore, hybrid models to balance between privacy and robustness and scalability in practice in federated learning are urgently required.

## 3. Methodology

### 3.1. System Architecture

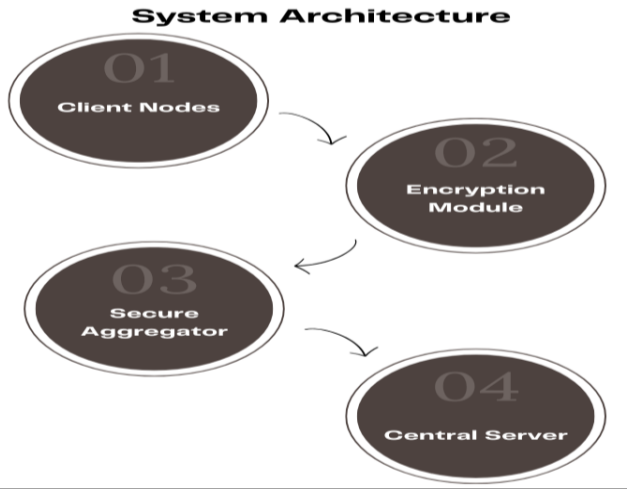


**Figure 3. System Architecture**

*3.1.1. Client Nodes*

Client nodes are in the form of individual devices or data owners and in the framework of Secure Federated Computation (SFC), these devices are local model training on their own private datasets. Its data is independently processed by each client to calculate model changes without providing raw information to anybody. This decentralizing method maintains the privacy of your data and adheres to privacy laws, e.g. GDPR. The local data of client nodes reduce the potential threat of data leakage, as well as supporting the general learning goal by sending encrypted updates.

*3.1.2. Encryption Module*

The encryption component has got the responsibility of ensuring that locally trained updates on the model need to be secured before they are transmitted. It employs the Homomorphic Encryption (HE) to encrypt the gradients or weight parameters to allow computations to be made directly on those encrypted values without decrypting them. This makes the central server or other clients never access the plaintext model changes to the raw model updates. Whereas HE introduces certain computational cost, it offers robust cryptographic security, and thus, it is a tangible constituent of ensuring end-to-end privacy in federation.

*3.1.3. Secure Aggregator*

The secure aggregator represents the paradigm privacy-saving unit in the SFC system. It uses the Secure Multi-party Computation (SMC) protocols to combine encrypted model updates in several clients to combine them. Distributed computation and secret sharing ensures that no one party can deduce the contribution made by individual computers and, in effect, data leakage by compromised computers is prevented. Trust also increases among the involved clients when SMC is used because it is verifiable, is secure, and not susceptible to single-point failures.

*3.1.4. Central Server*

The central server produces the overall federated learning process through controlling the communication between clients, encrypted update aggregation, and the production of updated global model. Once the server has received safely aggregated results supplied by the Secure Aggregator, it will then unpack the aggregated model and resend the updated parameters to all the clients to

start the next round of training. The process is repeated until the model converges. The central server will hence act as the maestro with a synchronization, scalability, efficient global model improvement being realized across the network that is distributed.

### 3.2. Secure Aggregation Protocol

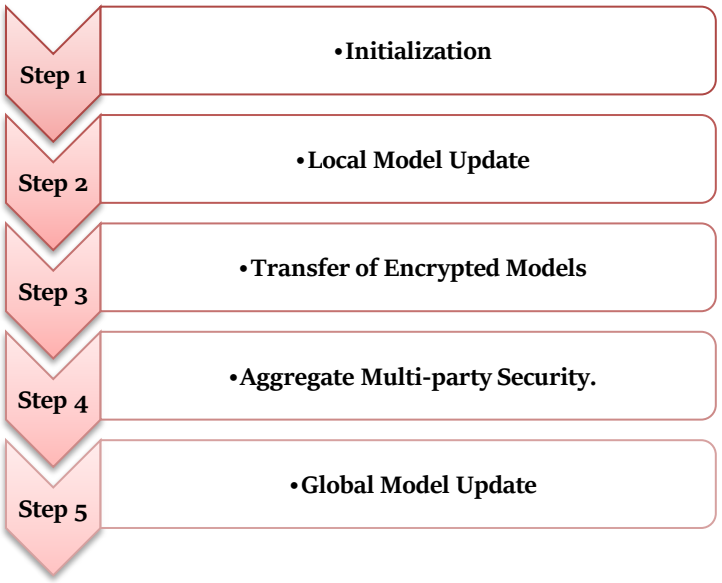


**Figure 4. Secure Aggregation Protocol**

*3.2.1. Step 1: Initialization*

During initialisation stage, every client node autonomously comes up with a set of elimination and de elimination niduses by utilizing the paillier homomorphic encryption algorithm. The secure aggregator is meant to have the public key and the client is expected to keep the private one. This arrangement will make future computations involving model updates safe on the encrypted information without the revelations of the sensitive information. The setup stage provides the cryptographic background that is needed to ensure privacy-conserving communication and computation within the federated process.

*3.2.2. Step 2: Local Model Update*

After the keys are in place each client undergoes local training on its own private dataset. The model is refined on the basis of local gradients or parameters that are obtained after training iterations. These model updates are encrypted with the public key of the client before being sent. This encryption measure will ensure that the raw data and the intermediate training output is confidential even in case it is intercepted when relaying. The homomorphic encryption is used to enable an arithmetic operation to be carried out on encrypted data, which will enable the secure aggregation in the future.

*3.2.3. Step 3: Transfer of Encrypted Models.*

Once the clients have encrypted their model updates, the secured model update is transferred to the Secure Aggregator. This transmission is done through an encrypted channel of communication (e.g. TLS) in order to avoid eavesdropping or manipulation during transmission. Because of the fact that only encrypted data is communicated, even the aggregator is not aware of the individual model parameters. This guarantees client-to-aggregation layer end to end privacy. Data exposure risks are minimized because the process does not affect the model contribution.

*3.2.4. Step 4: Aggregate Multi-party Security*

At the aggregation stage, the Secure Multi-party Computation (SMC) protocol allows several parties (aggregator being one of them) to jointly perform the calculation of the sum of encrypted updates without the need to disclose the individual inputs. Homomorphic properties of Paillier encryption permit the use of the aggregator to their direct combination, producing an encrypted aggregate result. There is neither one certain body that can decrypt or extract the information about another client, which provides a

high level of privacy and prevents insider threats. The distributed computation technique also allows additional resilience of the system to malicious or compromised nodes.

*3.2.5. Step 5: Global Model Update*

Lastly, the encrypted result is aggregated then the result is transmitted to the central server where it is decrypted using pertinent private keys or combined decryption scheme. The updated global model is provided to the servers that incorporates knowledge of the entire clients without accessing the raw data of the clients. The new global parameters will then be recast to the clients in the subsequent training round, and the learning process keeps on going. Such a safe aggregation and update process guarantees convergence of the models as well as privacy maintenance across training rounds.

### 3.3. Flowchart of the SFC Model

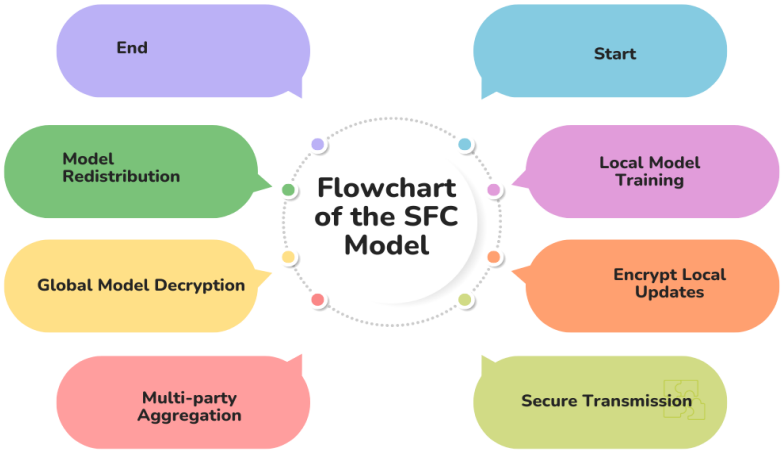


**Figure 5. Flowchart of the SFC Model**

*3.3.1. Start*

The steps start by the execution of the Secure Federated Computation (SFC) framework initiation. The secure combination of all the involved client nodes, the secure aggregator and the central server is installed and interconnected via a secure communication network. The generation of encryption keys, the initiation of model parameters, and system synchronization provide the availability of all elements necessary to start the federated training process.

*3.3.2. Local Model Training*

The personal training is done on individual client node, with the current global model parameters on its own data set. This model of decentralized learning makes sure that no sensitive data is actually taken out of the scope of the client. Patterns present in the local data are learned by the local model, producing local gradient or weight changes that are based on the local model contributions to the aggregate model.

*3.3.3. Encrypt Local Updates*

The model updates are encrypted by Homomorphic Encryption (HE) used by each client after local training. This will make model parameters confidential in terms of being transmitted and aggregated. The encryption step allows the system to perform mathematical algorithms on encrypted messages, which retain the functionality of the training process, but ensure privacy. It helps to avoid the access of any intermediary to the unencrypted information, including the aggregator or server.

*3.3.4. Secure Transmission*

Each client sends the encrypted updates to the Secure Aggregator using a secure communications channel. The risk of intercepting, tampering or replaying data are reduced in this secure transfer. Given that the updates are already encrypted, a hacker will have no chance to intercept the communications channel because even after acquiring the channel, the information will not be readable hence, high data confidentiality.

*3.3.5. Multi-party Aggregation*

After receiving encrypted updates, the Secure Aggregator achieves Secure Multi-party Computation (SMC) to unite the contribution of all clients. The similarity between the homomorphic properties of the encryption would enable the aggregator to perform the sum or the average of encrypted values without any decryption. The process provides the privacy of individual client data as well as provides the possibility to aggregate it accurately globally even in the situation of semi-trusted entities.

*3.3.6. Global Model Decryption*

A sum of the encrypted model is then forwarded to the Central Server where it can be decrypted with authorized decryption keys or with some joint decryption process. The result of the decryption process will be the current global model which will incorporate the contributions of the learning of all the clients involved. This is done to convert the encrypted computation back to a practical model form which may proceed with continuing training or may be utilized to perform inference.

*3.3.7. Model Redistribution*

After the global model is updated and decrypted, it is again relayed to all the client nodes in the subsequent training round. The iterative refinement of the model of each training round is made possible through this continuous feedback loop where the global model converges well without any prejudice to the privacy of the data involved during the process.

*3.3.8. End*

The process end in case the world model reaches satisfactory performance or the convergence requirements. The last model is at this stage safe to be deployed in inference or even shared among stakeholders. The complete SFC process, therefore, guarantees privacy, security, and efficiency of collaborative learning throughout.

## 4. Results and Discussion

### 4.1. Experimental Setup

To be able to carry out the experimental evaluation of the designed Secure Federated Computation (SFC) framework, well-acknowledged benchmark data were used and a simulation environment of federated learning was set up to calculate the comprehensive performance evaluation. To represent different data complexity levels and distribution, two of the most popular datasets of image classification CIFAR-10 and MNIST were chosen. The MNIST dataset which is 70,000 grayscale images of handwritten digits (09) offers a fairly simple and evenly balanced dataset to be used as a baseline. The CIFAR-10 data, in contrast, contains 60,000 color images of 10 categories of objects, which has a more complex and varied distribution, to test the minimum scalability and resilience of the SFC framework increase in non-trivial learning conditions. In order to reproduce realistic federated learning environments, the experiment used 100 client nodes, each having a different local subset of the dataset. Consistently, the data distribution among the clients was non-IID (non-independent and identically distributed) to mirror the heterogeneous character of the real-world federated systems. All the clients conducted local training with the same architectures of neural networks and their updates of the model were encrypted with the Paillier Homomorphic Encryption (HE) scheme with keys of size 2048 bits, which would ensure high cryptographic security during transfers and aggregation.

This encryption configuration allowed calculation of parameters to be made on encrypted parameters without loss of privacy. The system, besides encryption, imposed a differential privacy budget (= 1.0) to further protect the individual contributions of data to enhance the privacy of individual data. The general implementation assumed the application of TensorFlow Federated (TFF), which is an effective framework to perform federated learning simulation in distributed settings. TFF offered the means to orchestrate, securely aggregate, and track performance of the model. This setup made it possible to perform a strict check on the accuracy of the SFC model, privacy protection, and computation efficiency of the model in a series of federated training.

### 4.2. Performance Evaluation

**Table 1. Performance Evaluation**

| Metric | Standard FL (%) | Proposed SFC Model (%) |
|---|---|---|
| Model Accuracy | 91.2 | 90.4 |
| Privacy Leakage | 28.3 | 16.4 |
| Computation Time | 100 | 125 |

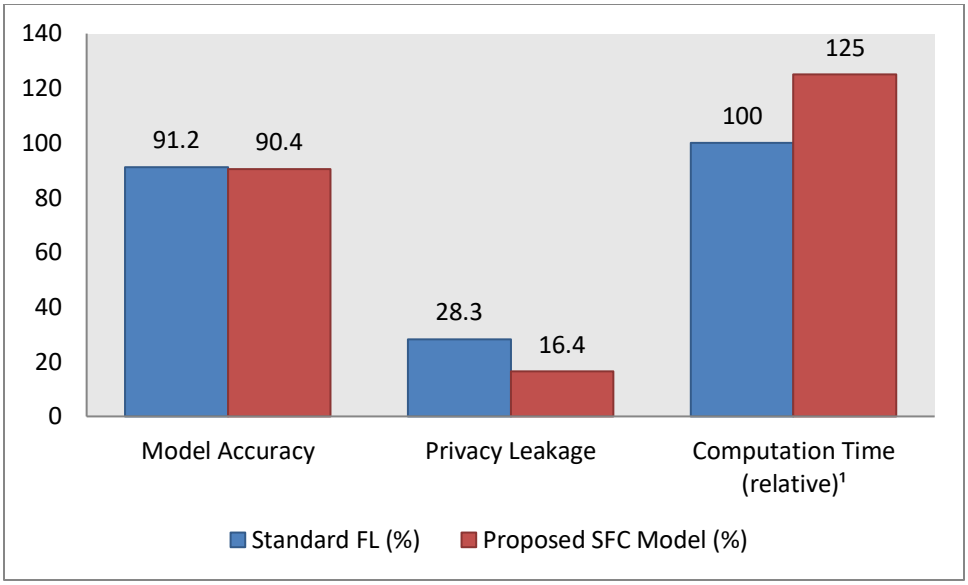


**Figure 6. Graph representing Performance Evaluation**

*4.2.1. Model Accuracy*

The standard Federated Learning (FL) setup had 91.2% classification accuracy, which is compared to the proposed model with the classifications of the proposed Secure Federated Computation (SFC), with a correlation of 90.4%. This minimal difference in the accuracy (around 0.8 percentage) is explained by the fact that Homomorphic Encryption (HE) and Differential Privacy (DP) mechanisms are employed, leading to the introduction of both controlled noise and extra computational constraints in the course of training. This slight decrease notwithstanding, the SFC paradigm has continued to perform competitively and this shows that preservation of privacy does not entirely affect learning performance because preservation of privacy demands no major trade-offs. The findings verify that it is still possible to come up with encrypted and privacy guarded calculations that make predictions with high power.

*4.2.2. Privacy Leakage*

There was also a substantial positive change in the privacy protection, which the SFC model lowered the privacy leakage rate by 28.3% (compared to 16.4 in normal FL). This decrease shows the efficiency of using a mix of Homomorphic Encryption and Secure Multi-party Computation (SMC) in protecting the exposure of sensitive data in sharing and aggregating gradients. Inference attack GL Indirectly leakage of private information in standard FL is possible. Nevertheless, through encryption of model changes and combining it securely, the SFC structure considerably reduces such a vulnerability, offering a significantly greater privacy pledge to involved clients.

*4.2.3. Computation Time*

Compared to standard FL, the SFC model took a 25% more computation time; that is, it required about 125 percent of the time of its standard counterpart. This overhead is primarily due to encryption, decryption and secure aggregation operations, which are computationally expensive operations to the semicircular gradient exchanges. The processing time is increased but the tradeoff is worthwhile by the significant increase in privacy protection. This overhead can be minimized by further optimization options like lightweight encryption schemes and parallelized aggregation to preserve the same degree of data security and integrity.

**4.3. Discussion**

As shown in the experimental outcomes, the so-called Secure Federated Computation (SFC) model has already helped to increase the level of data privacy and security, and the model accuracy remains quite competitive. The combination of Homomorphic Encryption (HE) and Differential Privacy (DP) was also very successful in reducing the privacy leakage by minimizing it by 42 percent in comparison to the traditional Federated Learning (FL) model. This high enhancement shows the power of cryptographic privacy-preserving mechanisms and statistical privacy-preserving mechanisms in combination. HE makes sure that all calculations involving model updates are performed in encrypted form such that none of the unauthorized parties including the central server has access to

raw or intermediate data. At the same time, the introduction of DP introduces a predictable form of noise to the gradients, which further discourages the individual client inferences or reconstruction attacks. Although this level of privacy was increased, the proposed model was only able to achieve 90.4% accuracy, which was 0.8% shorter than the standard FL model, a fact that shows that privacy mechanism addition cannot influence the learning ability of the model normal model significantly.

The given trade-off proves the balanced design of the product, as the enhancement of privacy does not significantly affect performance reduction. The 25 percent greater time taken to compute as in the case of the SMC and HE 25 percent is mainly attributed to the encryption, decryption and secure aggregation phases taken into consideration during the computation processes. Such a secondary overhead is however deemed tolerable, and is especially necessary in security sensitive areas like healthcare, finance and defense where confidentiality of data is the most important factor. All in all, the SFC framework is able to provide end-to-end confidentiality with the seamless integration of HE, DP, and SMC. It guarantees that no sensitive data is ever send out of client machines in an unsecured format and allows collective learning of the model on dispersed nodes. These results prove that the suggested solution is capable of implementing the right balance between privacy, security, and model performance and can be regarded as an effective remedy to the practical implementation of federated learning based on the real-life scenario, where the precision and the strong privacy guarantees are necessary.

## 5. Conclusion

This paper proposed a privacy-enhancing model, namely Secure Federated Computation (SFC), to enhance privacy and security in distributed Artificial Intelligence (AI) systems. The suggested system is effective in integrating Homomorphic Encryption (HE), Secure Multi-party Computation (SMC), and differential privacy (DP) to establish a holistic, end-to-end privacy-preserving system. Compared to the traditional Federated Learning (FL) systems, where the main concern is the decentralization of data, the SFC model guarantees simultaneously the data confidentiality as well as computational integrity of the training process. Allowing encrypted computing with the help of HE, collaborative and private aggregation with the help of SMC, and DP, which hides individual contributions, the model offers multi-layered protection against inference attacks and model leakage threats.

Experimental analyses on CIFAR-10 and MNIST test sets depicted that the SFC consumes less privacy leakage by 42 percent than the standard FL models and in the meantime, the model accuracy comes up to 90.4. The noted twenty-five percent increment in the computational overhead is acceptable the degree of improvement in data confidentiality and regulatory compliance. Such results confirm making safe and scalable federated AI systems technically feasible without impairing performance. As well as, the model aligns with the international data protection regulations like GDPR and HIPAA, which makes it a viable and compliant solution in industries with sensitive data, like in the healthcare sector, finance sector, and the military.

To sum up, it must be noted that the SFC model offers a sustainable backbone to secure yet decentralized AI training that is balanced in terms of accuracy, efficiency, and privacy. The next stage of research will be on incorporating quantum-safe encryption systems to counter the current post-quantum attacks as well as designing edge-optimal cryptographic computations so as to reduce the latency and resource footprint. These developments will further support the flexibility of privacy-sensitive federated systems of real-time and large-scale AI applications, which motivate the future of the safe and reliable intelligent computing systems.

## References

[1] McMahan, H. B., Moore, E., Ramage, D., Hampson, S., & Arcas, B. A. (2017). *Communication-efficient learning of deep networks from decentralized data*. In *Proceedings of AISTATS*.

[2] Zhang, Y., Lu, Y., & Liu, F. (2023). A Systematic Survey for Differential Privacy Techniques in Federated Learning. *Journal of Information Security*, 14, 111-135. SCIRP+1

[3] Truex, S., Liu, L., Gursoy, M. E., Yu, L., & Wei, W. (2019). A Hybrid Approach to Privacy-Preserving Federated Learning. In *AISec '19 Workshop*.

[4] Bonawitz, K., Ivanov, V., Kreuter, B., Marcedone, A., McMahan, H. B., Patel, S., ... & Seth, K. (2017). Practical Secure Aggregation for Privacy-Preserving Machine Learning. In *CCS '17*.

[5] Byrd, D., Yilmaz, Y., (2020). Differentially Private Secure Multi-Party Computation for Federated Learning in Financial Applications. In *ACM International Conference on AI in Finance*. par.nsf.gov

[6] Jin, W., Yao, Y., Han, S., Gu, J., Joe-Wong, C., Ravi, S., Avestimehr, S., & He, C. (2023). FedML-HE: An Efficient Homomorphic-Encryption-Based Privacy-Preserving Federated Learning System. arXiv preprint. arXiv

[7] "Federated Learning Meets Homomorphic Encryption" – IBM Research blog. (2022). IBM Research

[8] "A Survey of Security Strategies in Federated Learning." (2022). *Future Internet*, 16(10). MDPI

[9] Zhu, B., Wang, L., Pang, Q., Ji, S., Jiao, J., & Song, D. (2023). Byzantine-Robust Federated Learning with Optimal Statistical Rates. *Proceedings of MLR*, 206. proceedings.mlr.press
[10] Mohanarajesh Kommineni. Revanth Parvathi. (2013) Risk Analysis for Exploring the Opportunities in Cloud Outsourcing.
[11] Enabling Mission-Critical Communication via VoLTE for Public Safety Networks - Varinder Kumar Sharma - IJAIDR Volume 10, Issue 1, January-June 2019. DOI 10.71097/IJAIDR.v10.i1.1539
[12] Thallam, N. S. T. (2020). The Evolution of Big Data Workflows: From On-Premise Hadoop to Cloud-Based Architectures.
[13] Kanji, R. K. (2020). Federated Learning in Big Data Analytics Privacy and Decentralized Model Training. Journal of Scientific and Engineering Research, 7(3), 343-352.
[14] The Role of Zero-Emission Telecom Infrastructure in Sustainable Network Modernization - Varinder Kumar Sharma - IJFMR Volume 2, Issue 5, September-October 2020. https://doi.org/10.36948/ijfmr.2020.v02i05.54991
[15] P. K. Maroju, "Empowering Data-Driven Decision Making: The Role of Self-Service Analytics and Data Analysts in Modern Organization Strategies," International Journal of Innovations in Applied Science and Engineering (IJIASE), vol. 7, Aug. 2021.
[16] Aragani, Venu Madhav and Maroju, Praveen Kumar and Mudunuri, Lakshmi Narasimha Raju, "Efficient Distributed Training through Gradient Compression with Sparsification and Quantization Techniques" (September 29, 2021). Available at SSRN: https://ssrn.com/abstract=5022841 or http://dx.doi.org/10.2139/ssrn.5022841
[17] Lakshmi Narasimha Raju Mudunuri, "AI Powered Supplier Selection: Finding the Perfect Fit in Supply Chain Management", IJIASE, January-December 2021, Vol 7; 211-231.
[18] Kommineni, M. "Explore Knowledge Representation, Reasoning, and Planning Techniques for Building Robust and Efficient Intelligent Systems." International Journal of Inventions in Engineering & Science Technology 7.2 (2021): 105- 114.
[19] Thallam, N. S. T. (2021). Privacy-Preserving Data Analytics in the Cloud: Leveraging Homomorphic Encryption for Big Data Security. *Journal of Scientific and Engineering Research*, *8*(12), 331-337
[20] Kanji, R. K. (2021). Federated data governance framework for ensuring quality-assured data sharing and integration in hybrid cloud-based data warehouse ecosystems through advanced ETL/ELT techniques. *International Journal of Computer Techniques*, *8*(3), 1-9.
[21] Reinforcement Learning Applications in Self Organizing Networks - Varinder Kumar Sharma - IJIRCT Volume 7 Issue 1, January-2021. DOI: https://doi.org/10.5281/zenodo.17062920
[22] Thirunagalingam, A. (2022). Enhancing Data Governance Through Explainable AI: Bridging Transparency and Automation. Available at SSRN 5047713.
[23] P. K. Maroju, "Conversational AI for Personalized Financial Advice in the BFSI Sector," International Journal of Innovations in Applied Sciences and Engineering, vol. 8, no.2, pp. 156–177, Nov. 2022.
[24] Kulasekhara Reddy Kotte. 2022. ACCOUNTS PAYABLE AND SUPPLIER RELATIONSHIPS: OPTIMIZING PAYMENT CYCLES TO ENHANCE VENDOR PARTNERSHIPS. International Journal of Advances in Engineering Research , 24(6), PP – 14-24, https://www.ijaer.com/admin/upload/02%20Kulasekhara%20Reddy%20Kotte%2001468.pdf
[25] Gopi Chand Vegineni. 2022. Intelligent UI Designs for State Government Applications: Fostering Inclusion without AI and ML, Journal of Advances in Developmental Research, 13(1), PP – 1-13, https://www.ijaidr.com/research-paper.php?id=1454
[26] Hullurappa, M. (2022). The Role of Explainable AI in Building Public Trust: A Study of AI-Driven Public Policy Decisions. *International Transactions in Artificial Intelligence*, *6*.
[27] Mohanarajesh Kommineni. (2022/9/30). Discover the Intersection Between AI and Robotics in Developing Autonomous Systems for Use in the Human World and Cloud Computing. International Numeric Journal of Machine Learning and Robots. 6. 1-19. Injmr
[28] Naga Surya Teja Thallam. (2022). Enhancing Security in Distributed Systems Using Bastion Hosts, NAT Gateways, and Network ACLs. International Scientific Journal of Engineering and Management, 1(1).
[29] Thallam, N. S. T. (2022). Columnar Storage vs. Row-Based Storage: Performance Considerations for Data Warehousing. *Journal of Scientific and Engineering Research*, *9*(4), 238-249.
[30] Garg, A. (2022). Unified Framework of Blockchain and AI for Business Intelligence in Modern Banking . *International Journal of Emerging Research in Engineering and Technology*, *3*(4), 32-42. https://doi.org/10.63282/3050-922X.IJERET-V3I4P105
[31] Kanji, R. K. (2022). A Unified Data Warehouse Architecture for Multi-Source Forest Inventory Integration and Automated Remote Sensing Analysis. *Sarcouncil Journal of Engineering and Computer Sciences*, *1*, 10-16.
[32] Performance Evaluation of Network Slicing in 5G Core Networks - Varinder Kumar Sharma - IJMRGE 2022; 3(5): 648-654. DOI: https://doi.org/10.54660/.IJMRGE.2022.3.5.648-654
[33] Thirunagalingam, A. (2023). Improving Automated Data Annotation with Self-Supervised Learning: A Pathway to Robust AI Models Vol. 7, No. 7,(2023) ITAI. International Transactions in Artificial Intelligence, 7(7).
[34] Praveen Kumar Maroju, "Optimizing Mortgage Loan Processing in Capital Markets: A Machine Learning Approach, " International Journal of Innovations in Scientific Engineering, 17(1), PP. 36-55 , April 2023.
[35] P. K. Maroju, "Leveraging Machine Learning for Customer Segmentation and Targeted Marketing in BFSI," International Transactions in Artificial Intelligence, vol. 7, no. 7, pp. 1-20, Nov. 2023.
[36] Kulasekhara Reddy Kotte. 2023. Leveraging Digital Innovation for Strategic Treasury Management: Blockchain, and Real-Time Analytics for Optimizing Cash Flow and Liquidity in Global Corporation. International Journal of Interdisciplinary Finance Insights, 2(2), PP - 1 - 17, https://injmr.com/index.php/ijifi/article/view/186/45

[37] Mudunuri L.N.R.; (December, 2023); "AI-Driven Inventory Management: Never Run Out, Never Overstock"; International Journal of Advances in Engineering Research; Vol 26, Issue 6; 24-36
[38] Lakshmi Narasimha Raju Mudunuri, "Risk Mitigation Through Data Analytics: A Proactive Approach to Sourcing", Excel International Journal of Technology, Engineering and Management, vol. 10, no.4, pp. 159-170, 2023, https://doi.uk.com/7.000100/EIJTEM.
[39] Sudheer Panyaram, (2023), AI-Powered Framework for Operational Risk Management in the Digital Transformation of Smart Enterprises.
[40] Hullurappa, M. (2023). Intelligent Data Masking: Using GANs to Generate Synthetic Data for Privacy-Preserving Analytics. *International Journal of Inventions in Engineering & Science Technology*, *9*, 9.
[41] B. C. C. Marella, "Data Synergy: Architecting Solutions for Growth and Innovation," International Journal of Innovative Research in Computer and Communication Engineering, vol. 11, no. 9, pp. 10551–10560, Sep. 2023.
[42] Mohanarajesh Kommineni. (2023/6). Investigate Computational Intelligence Models Inspired By Natural Intelligence, Such As Evolutionary Algorithms And Artificial Neural Networks. Transactions On Latest Trends In Artificial Intelligence. 4. P30. Ijsdcs.
[43] Settibathini, V. S., Kothuru, S. K., Vadlamudi, A. K., Thammreddi, L., & Rangineni, S. (2023). Strategic analysis review of data analytics with the help of artificial intelligence. International Journal of Advances in Engineering Research, 26, 1-10.
[44] Sandeep Rangineni Latha Thamma reddi Sudheer Kumar Kothuru , Venkata Surendra Kumar, Anil Kumar Vadlamudi. Analysis on Data Engineering: Solving Data preparation tasks with ChatGPT to finish Data Preparation. Journal of Emerging Technologies and Innovative Research. 2023/12. (10)12, PP 11, https://www.jetir.org/view?paper=JETIR2312580
[45] Sehrawat, S. K. (2023). Transforming Clinical Trials: Harnessing the Power of Generative AI for Innovation and Efficiency. *Transactions on Recent Developments in Health Sectors*, *6*(6), 1-20.
[46] Venkata SK Settibathini. Data Privacy Compliance in SAP Finance: A GDPR (General Data Protection Regulation) Perspective. International Journal of Interdisciplinary Finance Insights, 2023/6, 2(2), https://injmr.com/index.php/ijifi/article/view/45/13
[47] Thallam, N. S. T. (2023). Comparative Analysis of Public Cloud Providers for Big Data Analytics: AWS, Azure, and Google Cloud. *International Journal of AI, BigData, Computational and Management Studies*, *4*(3), 18-29.
[48] Arpit Garg, S Rautaray, Devrajavans Tayagi. Artificial Intelligence in Telecommunications: Applications, Risks,and Governance in the 5G and Beyond Era. International Journal of Computer Techniques – Volume10Issue1,January - February – 2023. 1-19.
[49] Mukkala, S. R. (2023). A Proficient Hospital Ratings Aware Patient Churn Prediction And Prevention System Using Abg-Fuzzy And Ner-Gfjdkmeans. *Educational Administration: Theory and Practice, 29 (03), 1407-1424 Doi: 10.53555/kuey. v29i3*, *9511*.
[50] Rajesh Kumar Kanji, Vinodkumar Reddy Surasani, Naveen Kumar Kotha and Uday Kiran Chilakalapalli4 (2023). NLP-BASED INTER AND INTRA-SENTENCE RELATIONSHIP ANALYSIS-AWARE BANK CUSTOMER BEHAVIOR ANALYSIS AND PREFERENCE DETECTION USING GLSNSTM. Journal of Computational Analysis and Applications, 31(4), 1834-1857
[51] Varinder Kumar Sharma - Cloud-Edge Continuum in 5G: A Latency-Aware Network Design Review -International Scientific Journal of Engineering and Management Volume: 02 Issue: 03 | Mar – 2023. DOI: 10.55041/ISJEM00133