

Original Article

# Privacy-Preserving Homomorphic Encryption Schemes for Machine Learning in the Cloud

Ranadeep Pale<sup>1</sup>, Dr. A. Punitha<sup>2</sup>

<sup>1</sup>Independent Researcher, Austin, Texas, USA.

<sup>2</sup>Professor, Department Electronics Communication Engineering, MAM School of Engineering, Tamilnadu, India

Received Date: 17 October 2021

Revised Date: 01 November 2021

Accepted Date: 15 November 2021

**Abstract:** This examination investigates the joining of protection safeguarding homomorphic encryption plans in cloud-based AI to address blossoming concerns regarding information security and protection. This proposed method is based on recent contributions and focuses on tailoring homomorphic encryption algorithms like Paillier and Fully Homomorphic Encryption (FHE) to specific machine learning tasks. To strike a balance between data utility and privacy, seamless compatibility with preprocessing pipelines is prioritized. Secure model preparation strategies, consolidating cryptographic conventions and secure conglomeration techniques, are crucial in saving the secrecy of delicate data. The improvement of encoded model assessment measurements guarantees a hearty evaluation of model execution without compromising protection. Our technique stretches out to strengthening the general security act through exhaustive examination and countermeasure execution, tending to likely weaknesses in homomorphic encryption. Coordination inside the cloud foundation is a focal subject, with an emphasis on versatility, similarity, and true relevance. Challenges connected with dormancy, asset utilization, and versatility to fluctuating jobs are addressed to exhibit the down-to-earth practicality of security safeguarding AI. Looking forward, future work ought to envelop headways in encryption calculations, client-driven contemplations, cooperation with industry partners, and novel applications in united learning and IoT situations.

**Keywords:** Privacy-Preserving Machine Learning, Homomorphic Encryption, Security, Scalability, Cloud Computing,

## I. INTRODUCTION

The protection of sensitive data is still the most important concern in an era dominated by the ubiquitous integration of cloud computing and the insatiable demand for advanced machine learning capabilities. The juncture of these objectives moves the exploration outskirts into the domain of "Security Saving Homomorphic Encryption Plans for AI in the Cloud." This expanding field looks to blend the unmatched capability of homomorphic encryption with the groundbreaking utilizations of AI, all inside the powerful setting of distributed computing conditions. Homomorphic encryption, a cryptographic wonder, engages calculation on encoded data without the necessity for interpreting [1]. This quality is particularly imperative within the world of machine learning, where it is inconceivable to compromise on the security of delicate information. The request of conveying AI models within the cloud, with its flexibility and resource flexibility, meets with the essential to fortify security securing components [2]. This examination endeavors to investigate the eccentric exchange between homomorphic encryption and AI within the cloud, burrowing into the streamlining of execution, post against likely shortcomings, and the reliable coordination into certifiable applications over grouped spaces. As the caretakers of tremendous datasets continuously share their information with cloud-based AI systems, the premise to construct an impervious protect around this data gets to be principal [3]. This examination into security shielding homomorphic encryption traces unused skylines in cryptographic investigation as well as delineates a pathway toward pleasing the clearly disparate spaces of data security, AI advancement, and conveyed computing practicality.

### A. Aims and Objectives

#### a) Aims:

This investigation aims to propel the reconciliation of security-saving homomorphic encryption plans interior cloud-based AI structures.

#### b) Objectives

- To overhaul and upgrade existing homomorphic encryption plans, with an accentuation on their congruity to gigantic scope AI obligations in cloud conditions.
- To survey the sensibility and comfort of assurance defending homomorphic encryption interior the setting of diverse AI applications, spreading over zones like restorative care, back, and the Web of Things (IoT).
- To maintain the security position of homomorphic encryption plans by coordinating an intensive examination of likely weaknesses and contriving capable countermeasures to ensure against unapproved get to and data breaks.



- To energize interoperability and normalization of security defending homomorphic encryption traditions, ensuring reliable consolidation over diverse cloud stages and AI frameworks, in like manner working with more broad gathering and course of action.

## II. NOTEWORTHY CONTRIBUTIONS IN THE FIELD

The field of privacy-preserving machine learning has seen huge progressions, as clear in ongoing examinations [15] [16] [17] [18] [19]. Sarkar et al. [15] add to the area by applying homomorphic encryption to disease type expectation, guaranteeing the secrecy of delicate clinical information during the forecast interaction. Sirisha and Boleem [16] present a spearheading approach, coordinating homomorphic encryption into picture based AI models for mishap seriousness order. This work shows an outstanding step in defending delicate visual data. Yang and others [17] give a thorough survey of homomorphic encryption applications in the biometrics space, revealing insight into the qualities and difficulties in safeguarding biometric information. Security safeguarding cooperative learning without a believed outsider facilitator is tended to by Yu, Tang, and Zhao [18], who influence homomorphic encryption to guarantee information protection in cloud-edge conditions. Zhao et al. [19] add to the field by proposing an effective and protection-saving AI system in view of haze figuring, improving both productivity and security in the handling of delicate information. In a medical care setting, Zhao et al. [20] spotlight on down-to-earth utilizations of protection-saving strategies, involving homomorphic encryption for a secure rethinking of multiclass SVM-based sickness analysis. The blend of unified learning and homomorphic encryption is investigated by Angulo, Márquez, and Villanueva-Polanco [21] for the preparation of characterization models, introducing an inventive way to deal with security-protecting cooperative model preparation. Duy Tung et al. [22] present HeFUN, a novel homomorphic encryption approach for secure brain network surmising in unconstrained situations. Protection worries in k-nearest Neighbor (k-NN) arrangement over rethought cloud conditions are tended to by Guo et al. [23], who utilize homomorphic encryption to guarantee information privacy. Lee, Duong, and Lee [24] add to the field configurable encryption and decoding models for CKKS-based homomorphic encryption, improving the versatility of homomorphic encryption executions. Mangala, Eswara Reddy, and Venugopal [25] present a light-weight Roundabout Blunder Learning Calculation (CELA) for secure information correspondence conventions in IoT-Cloud frameworks, utilizing homomorphic encryption to address security challenges in IoT-Cloud correspondence. Munjal and Bhatia [26] contribute a deliberate survey that orchestrates existing writing on homomorphic encryption in the medical care industry, giving important bits of knowledge to scientists and experts in space. Aggregately, these examinations feature the adaptability of homomorphic encryption across assorted applications, tending to security concerns and guaranteeing the privacy of delicate information in different spaces. The combination of homomorphic encryption procedures in these works shows a pledge to propelling the field of protection safeguarding AI and upgrading the security of information handling in cloud and edge registering conditions.

## III. PROPOSED METHODOLOGY

In light of the rising worries encompassing information protection in the period of cloud-based AI, the mix of cutting-edge cryptographic procedures has arisen as a basic exploration try. Homomorphic encryption stands out as a promising way to reconcile the requirements of data privacy with the transformative potential of machine learning because it can perform computations on encrypted data without the need for decryption. This proposed strategy frames a far-reaching and smoothed-out way to deal with flawlessly coordinated protection-saving homomorphic encryption plans inside cloud-based AI structures.

### A. Homomorphic Encryption Determination and Tailoring:

The most vital phase in the proposed strategy includes the cautious choice of a homomorphic encryption plot customized to the particular necessities of the AI jobs needing to be done. This determination cycle considers factors, for example, computational proficiency, the degree of homomorphism required (somewhat or completely homomorphic), and the idea of the information to be handled [4]. Fitting the encryption plan to the particular necessities of the AI application guarantees that the protection-saving instrument adjusts flawlessly with the computational requests and security contemplations.

### B. Data Preprocessing and Homomorphic Compatibility:

Once the homomorphic encryption plot is picked, the following stage includes the execution of an information preprocessing pipeline. This pipeline tends to the crude information before encryption, applying methods like standardization, tokenization, or dimensionality decrease [5]. It is basic to guarantee that the preprocessing steps are viable with homomorphic encryption, finding some kind of harmony between saving information protection and keeping up with the utility of the information for ensuing AI undertakings. The subsequent processes of encryption and model training are laid out in this step.

### C. Encrypted Preparing Data Transformation:

With preprocessed information close by, the picked homomorphic encryption conspire is applied to change the preparation information into an encoded design reasonable for calculation. This change is vital in protecting the security of delicate data during the AI model's preparation stage [6]. Because it has a direct impact on the subsequent model training

process, evaluating the effects of encryption on the distribution of the training data becomes crucial. This step incorporates a significant effect on the effectiveness of the privacy-preserving framework as an entire by adjusting information security and show utility.

#### ***D. Secure Model Training Techniques:***

The center of the framework lies within the headway of secure show planning strategies fit for working on encoded data. Altering machine learning calculations to work in a protection-saving environment incorporates the examination of strategies like secure collection and cryptographic traditions [7]. Secure demonstrate planning is particularly important in multi-party circumstances, where agreeable learning happens without compromising the security of person datasets. This step ensures that the AI demonstrate picks up from encoded depictions of the data, keeping up with the security confirmations all through the arrangement interaction.

#### ***E. Encrypted Model Assessment Measurements:***

The proposed approach dives into the execution of strategies for assessing the machine learning model's execution on scrambled information taking after the preparing stage. This incorporates the advancement of estimations that can be figured on mixed desires without revealing sensitive information [8]. Assessing the compromises between show exactness and the computational complexity displayed by homomorphic encryption gets to be critical in checking the common amplexness of the security-protecting system. The decision-making forms with respect to the model's sending in real-world applications are backed by this step, which gives bits of knowledge into the models utility.

#### ***F. Security Examination and Countermeasure Execution:***

A comprehensive security investigation is carried out so that the privacy-preserving framework can be fortified. This incorporates recognizing conceivable shortcomings within the homomorphic encryption execution and examining streets for unapproved get to. Overwhelming countermeasures are at that point executed, wrapping secure key organization and additional cryptographic traditions. The objective is to overhaul the common security position of the system, ensuring that the mixed data remains invulnerable to conceivable perils or ambushes [9].

#### ***G. Cloud Integration and Real-world Application Testing:***

The homomorphic encryption scheme's integration into cloud-based machine learning framework gets to be the essential center as the strategy creates. Scalability, resource utilization, and compatibility with popular cloud platforms are all aspects of this [31]. Certifiable application testing turns into a vital stage, where the security-protecting AI framework is sent in different applications, traversing areas like medical care, finance, and the Internet of Things (IoT) [10]. Challenges connected with idleness, asset utilization, and versatility to shifting responsibilities are addressed to find out the common sense and viability of the proposed philosophy in true situations.

With regard to information, the proposed procedure focuses on the protection of delicate data through the encryption of preparing information. During the training phase, this ensures that the machine learning model learns from hidden data representations, preventing the exposure of individual data points [11]. The cautious plan of preprocessing steps looks to work out some kind of harmony between security conservation and the support of information utility for ensuing AI undertakings. Hearty encryption key administration rehearses are basic to forestall unapproved access and keep up with the secrecy of the scrambled information. The coordination inside a cloud foundation presents extra contemplations, including secure information stockpiling, moving, and handling. This thorough and smoothed-out approach plans to work with the arrangement of protection safeguarding AI models in cloud conditions while guaranteeing security, adaptability, and certifiable materialness.

#### ***H. Paillier Encryption***

Pascal Paillier came up with the idea for the Paillier cryptosystem in 1999. This partially homomorphic encryption method is well-known for its simplicity and effectiveness. It upholds homomorphic expansion, making it reasonable for security-saving applications where the attention is on calculations including expansion tasks.

#### ***I. Fully Homomorphic Encryption (FHE)***

Not at all like somewhat homomorphic encryption, completely homomorphic encryption permits both expansion and augmentation procedures on scrambled information. One of the striking FHE plans is the Brakerski-Vaikuntanathan FHE conspire, which uses cross-section-based cryptography.

- Key Generation:
  - Choose two large prime numbers,  $p$  and  $q$ .
  - Compute  $n = pq$  and  $n^2$ .
  - Select a random number  $g$  such that  $g^n \bmod n^2 = 1$ .
  - Public key:  $(n, g)$
  - Private key:  $(p, q)$
- Encryption:
  - Given a plaintext  $m$ , where  $0 \leq m < n$ .
  - Choose a random  $r$  such that  $0 \leq r < n$ .
  - Compute the ciphertext  $c$  using  $c = g^m \cdot r^n \bmod n^2$ .
- Decryption:
  - Given a ciphertext  $c$ .
  - Compute  $L(c^\lambda \bmod n^2) / L(g^\lambda \bmod n^2) \bmod n$ , where  $L(x) = \frac{x-1}{n}$ .
  - The result is the original plaintext  $m$ .

```
function KeyGeneration():
    p, q = generateLargePrimes()
    n = p * q
    n_squared = n^2
    g = randomElement(n_squared)
    public_key = (n, g)
    private_key = (p, q)
    return public_key, private_key

function Encryption(public_key, plaintext):
    n, g = public_key
    r = randomElement(n)
    ciphertext = (powmod(g, plaintext, n_squared) * powmod(r, n, n_squared)) % n_squared
    return ciphertext

function Decryption(private_key, public_key, ciphertext):
    p, q = private_key
    n, g = public_key
    lambda_val = (p-1)*(q-1)
    mu = modinv(L(powmod(g, lambda_val, n_squared)), n)
    plaintext = (L(powmod(ciphertext, lambda_val, n_squared)) * mu) % n
    return plaintext
```

```
function KeyGeneration():
    // Generate public and private keys
    // (Details of lattice-based key generation are omitted for brevity)

function HomomorphicAddition(ciphertext_a, ciphertext_b):
    // Perform homomorphic addition on ciphertexts
    return ciphertext_a + ciphertext_b

function HomomorphicMultiplication(ciphertext_a, ciphertext_b):
    // Perform homomorphic multiplication on ciphertexts
    return ciphertext_a * ciphertext_b

function HomomorphicDecryption(ciphertext, private_key):
    // Homomorphically decrypt the result
    return decrypt(ciphertext, private_key)
```

- Encryption:
  - Encrypted addition:  $E(a) + E(b)$
  - Encrypted multiplication:  $E(a) \times E(b)$

**Table 1: Fully Homomorphic Encryption (FHE)**

| Algorithm                    | Homomorphic Property  | Key Generation      | Supported Operations                   | Security Considerations  |
|------------------------------|-----------------------|---------------------|--|--|
| Paillier Encryption          | Partially Homomorphic | Efficient           | Addition and Scalar Multiplication     | Semantic security, Decisional Composite Residuosity Assumption |
| Fully Homomorphic Encryption | Fully Homomorphic     | Complex             | Addition, Multiplication, and More     | Lattice-based security assumptions, Performance challenges     |
| CKKS (Cheon-Kim-Kim-Song)    | Fully Homomorphic     | Parameter-dependent | Approximate Arithmetic on Real Numbers | Ring Learning With Errors (Ring-LWE) assumption                |

|                                       |                   |                     |  |  |
|---------------------------------------|-------------------|---------------------|--|--|
| BGV (Brakerski-Gentry-Vaikuntanathan) | Fully Homomorphic | Parameter-dependent | Ring Operations and Modular Arithmetic | Ideal lattice assumptions, Polynomial ring representation          |
| BFV (Brakerski-Vaikuntanathan-Fitzi)  | Fully Homomorphic | Parameter-dependent | Ring Operations and Modular Arithmetic | Ideal lattice assumptions, Polynomial ring representation          |
| LTV (Lindner-Peikert-Vaikuntanathan)  | Fully Homomorphic | Parameter-dependent | Polynomial Ring Operations             | Lattice-based security assumptions, Polynomial ring representation |

**IV. EXPECTED OUTCOME OF THE PROPOSED WORK**

The seamless integration of privacy-preserving homomorphic encryption schemes into cloud-based machine learning frameworks is expected to benefit significantly from this research. With a focus on enhancing data privacy, security, and the practicality of deploying machine learning models in cloud environments, the proposed work aims to contribute to the state-of-the-art in cryptographic techniques and machine learning methodologies.

**A. Enhanced Homomorphic Encryption Schemes:**

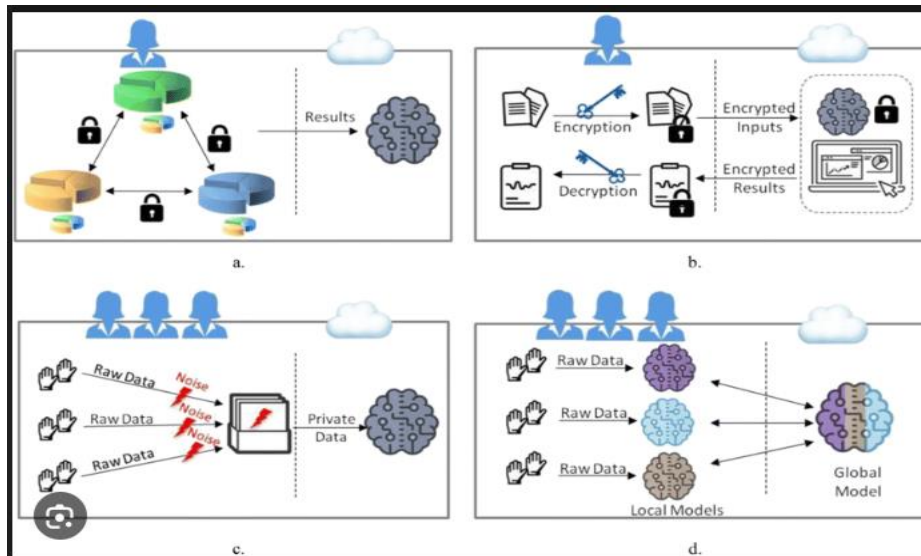
The improvement and refinement of existing homomorphic encryption methods, particularly with machine learning workloads, is one of the primary anticipated outcomes. The examination intends to distinguish and use the qualities of encryption calculations like Paillier and Fully Homomorphic Encryption (FHE) while tending to their constraints. Algorithmic upgrades might incorporate improvements for explicit AI activities, diminishing computational above, and upgrading effectiveness in the cloud climate [32], [12].

**B. Optimized Data Preprocessing and Homomorphic Similarity:**

The proposed work expects to convey enhanced methodologies for information preprocessing that flawlessly line up with homomorphic encryption necessities. This entails developing methods that strike a delicate balance between preserving the utility of the data for subsequent machine-learning tasks and protecting the privacy of the data [13]. Preprocessing algorithms will be tailored to be compatible with homomorphic encryption, increasing the privacy-preserving system's overall efficiency and effectiveness.

**C. Efficient Encrypted Training Data Transformation:**

The examination expects to deliver calculations that effectively change preparing information into an encoded design reasonable for computation. This includes further investigation of methods to adjust information protection and model utility during the preparation stage [14]. The normal result is an algorithmic methodology that guarantees the protection of delicate data while streamlining the AI model's capacity to gain from the scrambled information portrayals.



**Figure 1: Privacy-Preserving Machine Learning and Multi-Party Computation**

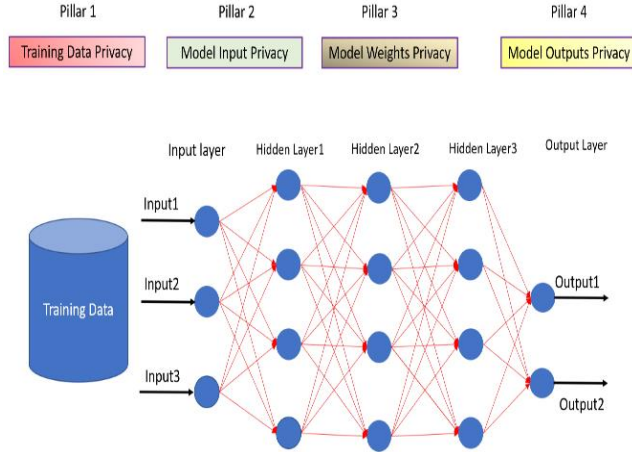


Figure 2: Privacy Preservation of Data-Driven Models in Smart Grids Using Homomorphic

**D. Secure Model Training Strategies:**

One of the key results is the improvement of cutting-edge secure model preparation procedures equipped for working on scrambled information. Cryptographic protocols, secure aggregation techniques, and novel strategies for enabling collaborative model training in multi-party scenarios will be the focus of the study [27]. This result is vital for guaranteeing that AI models can be prepared safely without compromising the privacy of individual datasets.

**E. Comprehensive Encrypted Model Evaluation Metrics:**

Comprehensive metrics for evaluating the performance of machine learning models on encrypted data are anticipated to be developed in the proposed work. This incorporates calculations for evaluating the compromises between model exactness and the computational intricacy presented by homomorphic encryption [28]. The result is a set of metrics that show how useful the model is and help people make decisions about how to use it in real-world situations.

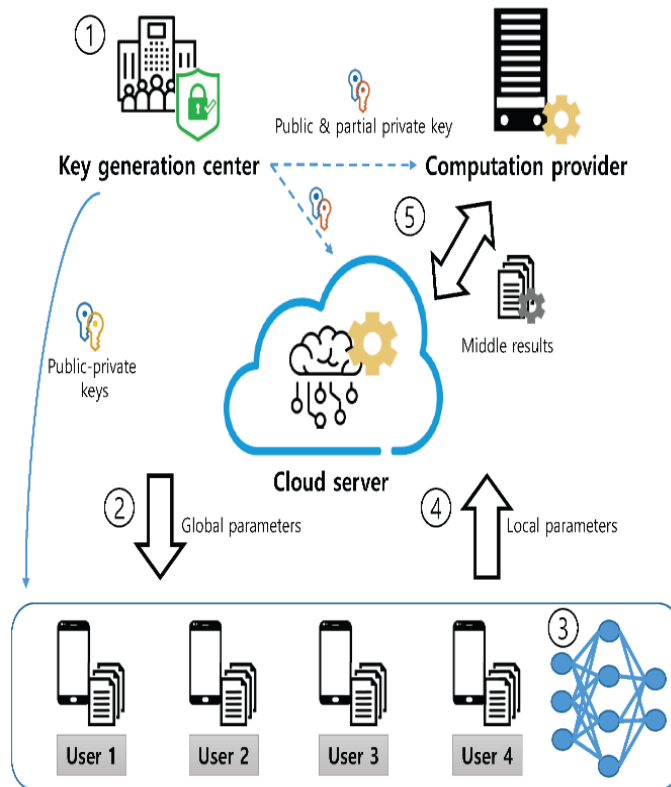


Figure 3: Privacy-Preserving Federated Learning Using Homomorphic Encryption

**F. Effective Countermeasures and Security Analysis:**

A fundamental result is a hearty security examination system that recognizes likely weaknesses in homomorphic encryption executions. Algorithms for implementing countermeasures, such as secure key management and additional cryptographic protocols, are the goal of the research [29]. This result is crucial for supporting the common security position of the assurance shielding system against likely dangers or ambushes.

**G. Cloud Integration and Real-World Application Testing:**

The exploration hopes to convey calculations for flawlessly coordinating homomorphic encryption plans inside a cloud-based AI foundation. Assessing compatibility with prevalent cloud stages, versatility, and asset utilization are all portion of this [30]. Moreover, the proposed work plans to donate calculations to genuine application testing, tending to challenges associated with inaction, resource utilization, and flexibility to changing duties in utilitarian circumstances.

**H. User-Centric Convenience and Input Components:**

The creation of user-centric algorithms that evaluate the privacy-preserving homomorphic encryption system's usability is an important outcome. To gather user experiences from stakeholders in various domains, the research anticipates the incorporation of feedback mechanisms. This iterative cycle guarantees the refinement of calculations given commonsense bits of knowledge, cultivating a framework that isn't just secure but also easy to use and versatile to different applications.

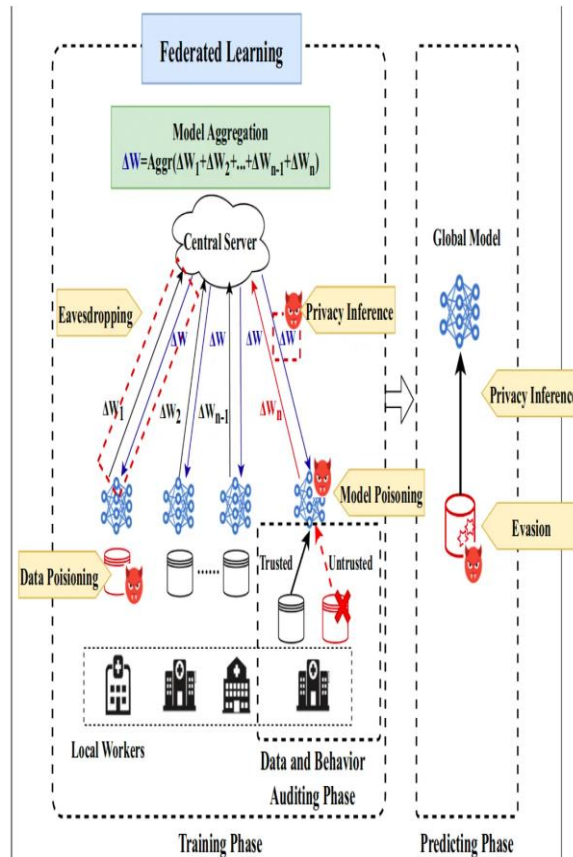


Figure 1. Attacks on the federated learning process [32].

**Figure 4: Future-Proofing Privacy: Securing AI, LLMs and Data with Homomorphic Encryption**

**I. Standardization and Documentation Contributions:**

The proposed work aims to add to the normalization of protection by safeguarding homomorphic encryption conventions. This entails creating extensive documentation that explains the methodology, specifics about how it was implemented, and the insights gained during the research process. The outcome is a useful resource for researchers, making it easier to share knowledge and encouraging more people to use privacy-preserving methods.

### **J. Framework for Continuous Improvement and Adaptation:**

The research hopes to provide a framework for the proposed methodology's ongoing adaptation and improvement. As the field of homomorphic encryption and cloud-based AI advances, calculations created in this exploration will be refreshed to consolidate the most recent headways, address arising difficulties, and upgrade the general viability of the security-saving framework.

In a nutshell, the proposed work is expected to lead to a comprehensive improvement in cloud-based machine learning's integration of privacy-preserving homomorphic encryption. Through algorithmic developments and far-reaching philosophies, the examination means to add to a change in outlook in getting delicate information while opening the maximum capacity of AI in cloud conditions. The imagined results can affect the scholarly scene as well as prepare for commonsense applications that focus on both security and effectiveness in the period of information-driven navigation.

## **V. CONCLUSION AND FUTURE WORK**

All in all, this exploration attempts to propel the coordination of protection safeguarding homomorphic encryption in cloud-based AI, addressing basic worries connected with information security and protection. The proposed strategy, roused by striking commitments from ongoing examinations [15][16][17][18][19], intends to upgrade the proficiency and reasonableness of conveying AI models while protecting the privacy of delicate data. The foundation of this study is the investigation of homomorphic encryption algorithms like Paillier and Fully Homomorphic Encryption (FHE). By fitting these calculations to explicit AI tasks and upgrading their similarity with preprocessing pipelines, the review means to figure out some kind of harmony between protection conservation and keeping up with information utility. Secure model preparation strategies, consolidating cryptographic conventions and secure accumulation techniques, are fundamental to the proposed system. The advancement of encoded model assessment measurements guarantees the evaluation of model execution without compromising touchy data. Strong security examination and countermeasure execution are essential to strengthening the general security stance of the framework, tending to likely weaknesses in the homomorphic encryption execution. The seamless integration of homomorphic encryption inside a cloud-based AI framework is a key concentration, with an accentuation on similarity, versatility, and certifiable application testing. By addressing difficulties connected with dormancy, asset utilization, and versatility to shifting jobs, the exploration means to exhibit the commonsense attainability of security-saving AI in assorted settings.

### **A. Future Work:**

Looking forward, future exploration in this space ought to investigate headways in homomorphic encryption plans, adjusting them to rising AI standards and tending to adaptability challenges. The joining of post-quantum cryptography methods can additionally upgrade the flexibility of security-protecting frameworks against advancing dangers. Also, the examination can reach out to explore the client-driven parts of protection-saving AI, taking into account ease of use, client input systems, and the improvement of easy-to-use interfaces. Joint effort with industry partners and policymakers is crucial for overcoming any barrier between scholastic progressions and true execution, guaranteeing that security-saving arrangements line up with administrative systems. The investigation of novel applications, for example, combined learning, edge processing, and Web of Things (IoT) situations, presents invigorating roads for future exploration. Fitting security-saving philosophies to explicit industry spaces, like medical care and money, can likewise yield significant bits of knowledge and add to the improvement of area explicitly prescribed procedures.

## **VI. REFERENCE**

- [1] Y. Bai et al, "cuSCNN: A Secure and Batch-Processing Framework for Privacy-Preserving Convolutional Neural Network Prediction on GPU," *Frontiers in Computational Neuroscience*, 2021. Available: <https://www.proquest.com/scholarly-journals/cuscnn-secure-batch-processing-framework-privacy/docview/2612984974/se-2>. DOI: <https://doi.org/10.3389/fncom.2021.799977>.
- [2] Y. Son et al, "Privacy-preserving breast cancer recurrence prediction based on homomorphic encryption and secure two party computation," *PLoS One*, vol. 16, (12), 2021. Available: <https://www.proquest.com/scholarly-journals/privacy-preserving-breast-cancer-recurrence/docview/2612008839/se-2>. DOI: <https://doi.org/10.1371/journal.pone.0260681>.
- [3] L. Zhang, Z. Zehui and G. Cong, "Accelerating privacy-preserving momentum federated learning for industrial cyber-physical systems," *Complex & Intelligent Systems*, vol. 7, (6), pp. 3289-3301, 2021. Available: <https://www.proquest.com/scholarly-journals/accelerating-privacy-preserving-momentum/docview/2588792677/se-2>. DOI: <https://doi.org/10.1007/s40747-021-00519-2>.
- [4] S. Sharma and K. Chen, "Confidential machine learning on untrusted platforms: a survey," *Cybersecurity*, vol. 4, (1), 2021. Available: <https://www.proquest.com/scholarly-journals/confidential-machine-learning-on-untrusted/docview/2567803602/se-2>. DOI: <https://doi.org/10.1186/s42400-021-00092-8>.
- [5] S. A. Ala, B. Kane and S. Fischer-Hübner, "Machine Learning-Based Analysis of Encrypted Medical Data in the Cloud: Qualitative Study of Expert Stakeholders' Perspectives," *JMIR Human Factors*, vol. 8, (3), 2021. Available: <https://www.proquest.com/scholarly-journals/machine-learning-based-analysis-encrypted-medical/docview/2577891441/se-2>. DOI: <https://doi.org/10.2196/21810>.



- [6] Y. Liu et al, "Verifiable Privacy-Preserving Neural Network on Encrypted Data," *Journal of Information Hiding and Privacy Protection*, vol. 3, (4), pp. 151-164, 2021. Available: <https://www.proquest.com/scholarly-journals/verifiable-privacy-preserving-neural-network-on/docview/2646008984/se-2>. DOI: <https://doi.org/10.32604/jihpp.2021.026944>.
- [7] R. Hou et al, "Multi-Party Verifiable Privacy-Preserving Federated k-Means Clustering in Outsourced Environment," *Security and Communication Networks*, vol. 2021, 2021. Available: <https://www.proquest.com/scholarly-journals/multi-party-verifiable-privacy-preserving/docview/2618118126/se-2>. DOI: <https://doi.org/10.1155/2021/3630312>.
- [8] J. Shin, S. Choi and C. Yoon-Ho, "Is Homomorphic Encryption-Based Deep Learning Secure Enough?" *Sensors*, vol. 21, (23), pp. 7806, 2021. Available: <https://www.proquest.com/scholarly-journals/is-homomorphic-encryption-based-deep-learning/docview/2608145995/se-2>. DOI: <https://doi.org/10.3390/s21237806>.
- [9] X. Sun et al, "A Privacy-Preserving Reinforcement Learning Approach for Dynamic Treatment Regimes on Health Data," *Wireless Communications & Mobile Computing (Online)*, vol. 2021, 2021. Available: <https://www.proquest.com/scholarly-journals/privacy-preserving-reinforcement-learning/docview/2606664425/se-2>. DOI: <https://doi.org/10.1155/2021/8952219>.
- [10] J. Liu et al, "Secure KNN Classification Scheme Based on Homomorphic Encryption for Cyberspace," *Security and Communication Networks*, vol. 2021, 2021. Available: <https://www.proquest.com/scholarly-journals/secure-knn-classification-scheme-based-on/docview/2597344181/se-2>. DOI: <https://doi.org/10.1155/2021/8759922>.
- [11] Z. Chen et al, "Bibliometrics of Machine Learning Research Using Homomorphic Encryption," *Mathematics*, vol. 9, (21), pp. 2792, 2021. Available: <https://www.proquest.com/scholarly-journals/bibliometrics-machine-learning-research-using/docview/2596046878/se-2>. DOI: <https://doi.org/10.3390/math9212792>.
- [12] A. Vizitiu et al, "Framework for Privacy-Preserving Wearable Health Data Analysis: Proof-of-Concept Study for Atrial Fibrillation Detection," *Applied Sciences*, vol. 11, (19), pp. 9049, 2021. Available: <https://www.proquest.com/scholarly-journals/framework-privacy-preserving-wearable-health-data/docview/2580962714/se-2>. DOI: <https://doi.org/10.3390/app11199049>.
- [13] M. S. Mikail et al, "Homomorphic Encryption Based Privacy-Preservation for IoMT," *Applied Sciences*, vol. 11, (18), pp. 8757, 2021. Available: <https://www.proquest.com/scholarly-journals/homomorphic-encryption-based-privacy-preservation/docview/2576378470/se-2>. DOI: <https://doi.org/10.3390/app11188757>.
- [14] Q. Lou, "Efficient Private Deep Learning." Order No. 28716959, Indiana University, United States -- Indiana, 2021.
- [15] K. Edemacu, "Multi-Party Privacy-Preserving Logistic Regression with Poor Quality Data Filtering for IoT Contributors," *Electronics*, vol. 10, (17), pp. 2049, 2021. Available: <https://www.proquest.com/scholarly-journals/multi-party-privacy-preserving-logistic/docview/2570775454/se-2>. DOI: <https://doi.org/10.3390/electronics10172049>.
- [16] A. B. Popescu et al, "Privacy Preserving Classification of EEG Data Using Machine Learning and Homomorphic Encryption," *Applied Sciences*, vol. 11, (16), pp. 7360, 2021. Available: <https://www.proquest.com/scholarly-journals/privacy-preserving-classification-eeeg-data-using/docview/2564633685/se-2>. DOI: <https://doi.org/10.3390/app11167360>.
- [17] M. Alkhalaiwi et al, "An Efficient Approach Based on Privacy-Preserving Deep Learning for Satellite Image Classification," *Remote Sensing*, vol. 13, (11), pp. 2221, 2021. Available: <https://www.proquest.com/scholarly-journals/efficient-approach-based-on-privacy-preserving/docview/2539968255/se-2>. DOI: <https://doi.org/10.3390/rs13112221>.
- [18] Z. Tan et al, "Distributed Outsourced Privacy-Preserving Gradient Descent Methods among Multiple Parties," *Security and Communication Networks*, vol. 2021, 2021. Available: <https://www.proquest.com/scholarly-journals/distributed-outsourced-privacy-preserving/docview/2520675503/se-2>. DOI: <https://doi.org/10.1155/2021/8876893>.
- [19] F. Kuang et al, "Multiparty Homomorphic Machine Learning with Data Security and Model Preservation," *Mathematical Problems in Engineering*, vol. 2021, 2021. Available: <https://www.proquest.com/scholarly-journals/multiparty-homomorphic-machine-learning-with-data/docview/2480125564/se-2>. DOI: <https://doi.org/10.1155/2021/6615839>.
- [20] X. Jin et al, "Efficient blind face recognition in the cloud," *Multimedia Tools Appl*, vol. 79, (17-18), pp. 12533-12550, 2020. Available: <https://www.proquest.com/scholarly-journals/efficient-blind-face-recognition-cloud/docview/2397280274/se-2>. DOI: <https://doi.org/10.1007/s11042-019-08280-y>.
- [21] A. Alharbi, H. Zamzami and E. Samkri, "Survey on Homomorphic Encryption and Address of New Trend," *International Journal of Advanced Computer Science and Applications*, vol. 11, (7), 2020. Available: <https://www.proquest.com/scholarly-journals/survey-on-homomorphic-encryption-address-new/docview/2655153973/se-2>. DOI: <https://doi.org/10.14569/IJACSA.2020.0110774>.
- [22] Anonymous "Privacy-Preserving K-Nearest Neighbors Training over Blockchain-Based Encrypted Health Data," *Electronics*, vol. 9, (12), pp. 2096, 2020. Available: <https://www.proquest.com/scholarly-journals/privacy-preserving-k-nearest-neighbors-training/docview/2469886806/se-2>. DOI: <https://doi.org/10.3390/electronics9122096>.
- [23] L. Cheng, L. Yang and J. Ma, "A Secure and Verifiable Outsourcing Scheme for Assisting Mobile Device Training Machine Learning Model," *Wireless Communications & Mobile Computing (Online)*, vol. 2020, 2020. Available: <https://www.proquest.com/scholarly-journals/secure-verifiable-outsourcing-scheme-assisting/docview/2465233914/se-2>. DOI: <https://doi.org/10.1155/2020/8825623>.
- [24] M. Y. Hong, J. S. Yoo and J. W. Yoon, "Homomorphic Model Selection for Data Analysis in an Encrypted Domain," *Applied Sciences*, vol. 10, (18), pp. 6174, 2020. Available: <https://www.proquest.com/scholarly-journals/homomorphic-model-selection-data-analysis/docview/2441101493/se-2>. DOI: <https://doi.org/10.3390/app10186174>.
- [25] S. Carpov et al, "Privacy-preserving semi-parallel logistic regression training with fully homomorphic encryption," *BMC Medical Genomics*, Suppl.7, vol. 13, pp. 1-10, 2020. Available: <https://www.proquest.com/scholarly-journals/privacy-preserving-semi-parallel-logistic/docview/2435109810/se-2>. DOI: <https://doi.org/10.1186/s12920-020-0723-0>.
- [26] J. Andrew, S. M. Shaun and B. Mohit, "A Comprehensive Analysis of Privacy-preserving Techniques in Deep learning based Disease Prediction Systems," *Journal of Physics: Conference Series*, vol. 1362, (1), 2019. Available: <https://www.proquest.com/scholarly-journals/comprehensive-analysis-privacy-preserving/docview/2568470021/se-2>. DOI: <https://doi.org/10.1088/1742-6596/1362/1/012070>.

- [27] A. Liu et al, "Confidential State Verification for the Delegated Cloud Jobs with Confidential Audit Log," EAI Endorsed Transactions on Security and Safety, vol. 6, (20), 2019. Available: <https://www.proquest.com/scholarly-journals/confidential-state-verification-delegated-cloud/docview/2342353633/se-2>. DOI: <https://doi.org/10.4108/eai.13-7-2018.162290>.
- [28] T. Lakum and B. Thirumala Rao, "A Key-Ordered Decisional Learning Parity with Noise (DLPN) Scheme for Public Key Encryption Scheme in Cloud Computing," International Journal of Advanced Computer Science and Applications, vol. 10, (11), 2019. Available: <https://www.proquest.com/scholarly-journals/key-ordered-decisional-learning-parity-with-noise/docview/2655163325/se-2>. DOI: <https://doi.org/10.14569/IJACSA.2019.0101121>.
- [29] F. Tang et al, "Privacy-Preserving Distributed Deep Learning via Homomorphic Re-Encryption," Electronics, vol. 8, (4), pp. 411, 2019. Available: <https://www.proquest.com/scholarly-journals/privacy-preserving-distributed-deep-learning-via/docview/2548382292/se-2>. DOI: <https://doi.org/10.3390/electronics8040411>.
- [30] M. Salem and S. Taheri, "Utilizing Transfer Learning and Homomorphic Encryption in a Privacy Preserving and Secure Biometric Recognition System," Computers, vol. 8, (1), pp. 3, 2019. Available: <https://www.proquest.com/scholarly-journals/utilizing-transfer-learning-homomorphic/docview/2548363513/se-2>. DOI: <https://doi.org/10.3390/computers8010003>.
- [31] Preyaa Atri, "Unlocking Data Potential: The GCS XML CSV Transformer for Enhanced Accessibility in Google Cloud", International Journal of Science and Research (IJSR), Volume 8 Issue 10, October 2019, pp. 1870-1871, <https://www.ijsr.net/getabstract.php?paperid=SR24608145221>
- [32] Preyaa Atri. (2021). Automated Object Deletion in Google Cloud Storage: Introducing the Clean-up-gcs-bucket Library. European Journal of Advances in Engineering and Technology, 8(7), 79–83. <https://doi.org/10.5281/zenodo.11408114>