Journal of Scientific & Industrial Research
Vol. 84, May 2025, pp. 556-566
DOI: 10.56042/jsir.v84i5.11836

VFL-HMF: Enhancing IIoT Security with Federated Learning and Homomorphic Matrix Factorization

Ganesh Kumar Mahato*, Aiswaryya Banerjee & Swarnendu Kumar Chakraborty*

Department of Computer Science and Engineering, National Institute of Technology, Jote 791 113, Arunachal Pradesh, India

Received 14 June 2024; revised 14 November 2024; accepted 30 April 2025

Matrix factorization is a key technique in recommendation systems, offering dimensionality reduction and collaborative filtering benefits. However, in the context of the Industrial Internet of Things (IIoT), implementing matrix factorization raises critical challenges related to data privacy, security, and computational efficiency. To address these concerns, this study introduces Verifiable Federated Learning with Homomorphic Matrix Factorization (VFL-HMF), a novel model designed to secure sensitive data while enabling collaborative learning. The proposed VFL-HMF model integrates homomorphic encryption and federated learning to ensure data privacy and integrity during computation. By leveraging the VGG-16 Convolutional Neural Network (CNN) architecture, the model extracts detailed features from casting dataset obtained from an industry, achieving high accuracy and robust performance. Experimental results demonstrate that VFL-HMF achieves a remarkable accuracy of 93%, surpassing existing approaches, while reducing complexity to $\boldsymbol{O(1)}$.This work bridges the gap between privacy-preserving computation and effective collaborative learning in IIoT environments. The VFL-HMF model not only protects sensitive information but also guarantees the verifiability of results, making it a critical solution for secure and efficient data processing. These findings highlight the potential of this approach to revolutionize IIoT applications, paving the way for further advancements in secure federated learning.

Keywords: Collaborative learning, Convolutional neural network, Data aggregation, Metal casting, Securecomputation

Introduction

Matrix Factorization (MF) is a popular model utilized in diverse fields, including Federated Learning (FL) and signal processing, with applications spanning data clustering, item recommendation, and biological analysis. Its capability to reduce high-dimensional data into lower-dimensional representations makes it highly effective across these domains.[1]However, the growing emphasis on privacy-preserving FL, especially in the context of the IIoT, has highlighted the need for models that can protect user privacy while delivering accurate results. As awareness of data privacy and the enforcement of regulations like the General Data Protection Regulation continue to rise, the demand for such privacy-preserving models has become paramount.

The rapid expansion of the world wide web has brought about unprecedented convenience, but it has also posed significant challenges in filtering relevant information from the vast sea of online data.[2] Real-world applications, such as pattern recognition, frequently encounter massive datasets with extremely high dimensionality, necessitating the development of efficient data processing models.[3] Privacy-preserving FL techniques, including differential privacy and Homomorphic Encryption(HE), have been developed to address these privacy concerns.[4] Differential privacy involves introducing noise into the data to prevent attackers from identifying individual user information, while HEperforms computation onciphertext, thereby privacy is preserved.

Matrix factorization plays a crucial role in signal processing and FL.[5] However, it also presents challenges like overfitting, scalability concerns, data sparsity, and bias. In the ever-expanding landscape of the World Wide Web, efficient data processing for massive, high-dimensional datasets has grown increasingly crucial. Privacy-preserving FL techniques have emerged as vital solutions to address these challenges.[6]

FL, being a distributed machine learning approach, brings the model to the data rather than bringing the data to the model, as illustrated in Fig. 1. This work presents a privacy-preserving verifiable FL framework designed to meet the evolving demands of the IIoT and other digital-age applications. The proposed scheme, which integrates matrix factorization with privacy-preserving methodologies such as Verifiable Federated Learning and Homomorphic Matrix Factorization (VFL-HMF),

*Authors for Correspondence
E-mail: ganesh.phd20@nitap.ac.in; swarnendu@nitap.ac.in

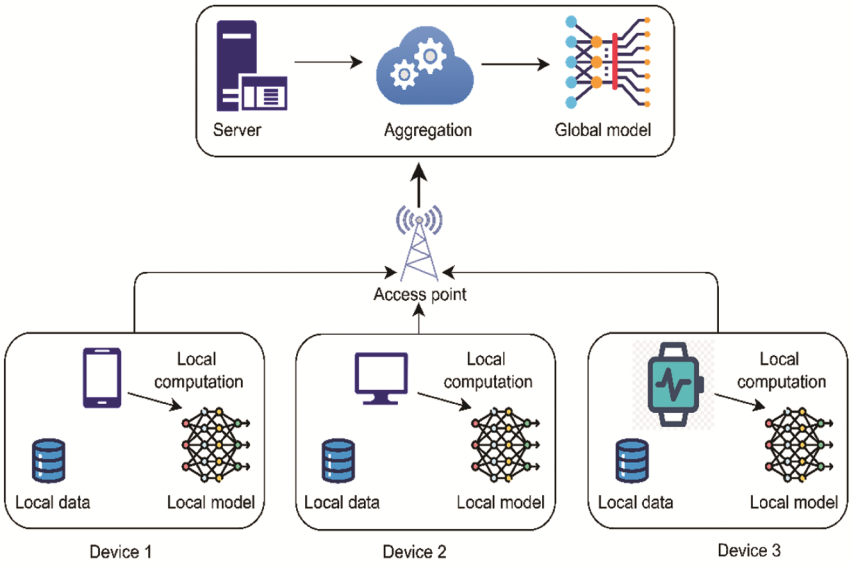

Fig. 1 — Federated learning aggregated model

effectively addresses the inherent challenges of recommendation systems in the Industrial Internet of Things (IIoT).

Additionally, we employed the VGG-16 model from the CNN to extract features from metal casting dataset. By leveraging VGG-16, the proposed approach enhances the learning process and improves data privacy and integrity. This renders the proposed method a valuable asset in the continuously evolving realm of IoT applications, offering robust solutions for efficient and secure data processing.

The key contributions of this paper are as follows:

1 VFL-HMF model presents a novel approach to secure matrix factorization with HE, offering improvements in computation efficiency, security, and scalability, while maintaining high accuracy and low communication overhead.

2 A gradient processing method is introduced to preserve privacy while significantly reducing computation and communication costs.

3 A verification mechanism is proposed to effectively detect any manipulation of aggregated results by the aggregation server while rigorously proving its validity.

Literature Survey

Xicheng *et al.*[3] proposed VPFedMF, a verifiable federated matrix factorization method. It uses masking-based secure aggregation to protect individual gradient updates and enables users to validate aggregation results using a homomorphic hash function and commitment mechanism. It provides a promising solution for addressing privacy and verifiability concerns in federated learning, with potential for various applications. It needs to be more secure to perform data updation in the cloud. However, with HE, this model could provide security to cloud data. A Correlated Matrix Factorization (CMF) model[4] combines MF and CCA for personalized recommendations. A comprehensive evaluation of four datasets demonstrates that CMF performs better than the existing works. At the same time, security plays a vital role during data computation in the third part cloud server, so security measures must be implemented to make the model workable.

Luo *et al.*[5] introduced the SNMF model, specifically designed for huge manufacturing datasets, highlighting their simplicity and ease of implementation through a single-element approach. The RSNMF model demonstrated superior computational efficiency and prediction accuracy as compared to similar models, but it lacked robust security measures. Additionally, a Weakly Supervised Deep Matrix Factorization (WDMF) algorithm was introduced to refine and assign image tags, effectively managing issues like noisy, incomplete, or redundant data.

Li *et al.*[7] presented RSNMF, an advanced version of NMF that incorporates a block-diagonal architecture to efficiently utilize both labeled and unlabeled data. The model employs a generalized loss function to mitigate the impact of outliers, with experimental results confirming the efficiency of both RSNMF and the block-diagonal architecture. Despite its advancements, security remains a critical issue.

HFT[8] integrates reviews and ratings with latent Dirichlet allocations to enhance performance.

Zheng *et al*.[9] uses latent factors of items and users from the review documents with DeepCoNN. A model proposed by Chen *et al*.[10] uses DNNs and feature vector of the items and users to learn and explore the importance of users' reviews based on the neural attention technique. CARL model[11] is based on dynamic linear fusion and CNN. Data aggregation, verification, and high efficiency proposed by Izmeci & Og¨ud¨uc¨u[12] uses HE with binary classifications but needs to catch up in accuracy.

The schemes presented by Guo *et al*.[13] and Han *et al*.[14] focused privacy preservation in federated learning but lack essential features such as secure aggregation, verification, and HE. While matrix factorization techniques are utilized by both the schemes, they fail to achieve high efficiency and accuracy, limiting their scalability in practical applications. The proposed approach overcomes these shortcomings by integrating advanced cryptographic techniques, ensuring enhanced security, accuracy, and computational efficiency.

Mai & Pang[15] investigate the privacy risks in FL recommender systems, specifically focusing on matrix factorization. They identify significant privacy vulnerabilities, demonstrating that an FL server can infer user information with over 80% accuracy from uploaded gradients. Their contribution includes proposing a privacy-preserving framework, PrivMVMF, based on HE to mitigate these risks.

Zhou *et al*.[16] presented a lightweight distributed recommender system designed with privacy-preserving features using the novel cryptographic framework TMFH-DEM. This approach ensures chosen Ciphertext Attack (CCA) security, ensuring data confidentiality. Unlike conventional methods dependent on Fully Homomorphic Encryption (FHE), this system enables optimized processing on ciphertext, significantly reducing computational overhead. The system's practicality is demonstrated through comprehensive evaluations, showcasing its efficiency in both computational and communication aspects.

Zheng *et al*.[17] introduced a matrix factorization technique, FMFSS, to address privacy issues in conventional recommendation systems. The approach uses secret sharing to decompose gradients locally at the user side and transmits intermediate results securely, eliminating the need for extra encryption. By incorporating user-item interaction values, the method prevents servers from deducing actual gradient data while preserving the accuracy of recommendations.[18] While current methods provide promising solutions for privacy and efficiency, a comprehensive framework is urgently required to seamlessly incorporate cutting-edge cryptographic techniques, such as HE, ensuring robust privacy protection, computational efficiency, and scalability in federated systems. A comparison of related work is presented in Table 1.

Proposed Scheme

In the context of industrial automation, the proposed model leverages metal casting datasets and employs VGG-16 for feature extraction, enabling precise identification of casting characteristics.[22] To enhance data security, the model integrates matrix factorization, ensuring the protection of user

Table 1 — Comparative analysis of related schemes with proposed work

Schemes	Features						
	Privacy-preserving	Secure-aggregation	Verification	High efficiency	Matrix factorization	Homomorphic encryption	High accuracy
Luo *et al*.[5]	√	√	×	×	√	×	×
Li *et al*.[6]	√	×	√	×	√	×	×
Li *et al*.[7]	√	×	×	×	√	×	×
Zheng *et al*.[9]	√	√	√	×	√	×	×
Guo *et al*.[13]	√	×	×	×	√	×	×
Han *et al*.[14]	√	×	×	√	√	×	×
Mai *et al*.[15]	√	×	×	√	√	×	×
Zhou *et al*.[16]	√	√	√	√	√	×	×
Zheng *et al*.[17]	√	√	√	√	×	√	×
Mnih *et al*.[18]	√	×	×	×	√	×	×
Mandal *et al*.[19]	√	√	×	×	√	×	×
Wang *et al*.[20]	√	√	×	×	√	×	×
Xu *et al*.[21]	√	×	×	×	√	×	×
Proposed	√	√	√	√	√	√	√

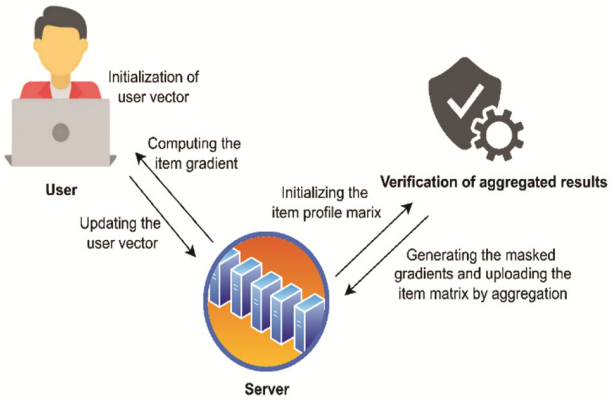

Fig. 2 — Proposed VFL-HMF Model

information while maintaining efficient and accurate processing of extracted features.[23] This process involves generating user and item matrices, updating them using gradient-based optimization, and verifying the aggregated results, as presented in Fig. 2.

The proposed VFL-HMF model effectively deals with the challenges of unauthorized access to confidential user data, particularly in environments managed by Cloud Service Providers (CSPs). To mitigate this risk, data is decomposed item matrices and user, which are progressively refined through gradient-based optimization methods, ensuring that only an approximate representation of the raw data is retained. This masking technique blocks external entities from interpreting the data, ensuring that CSPs cannot access sensitive information. The matrix computation process is outlined in Algorithm 1.

Tested on an industrial automation dataset, the proposed approach further strengthens security by partitioning the data into user and item matrices, updating them through gradient-based methods, and restricting access to only an approximate version of the original data. Additionally, both the regularization parameter (λ) and learning rate are optimized through cross-validation to improve model performance. Furthermore, Algorithm 2 demonstrates how matrix factorization can be verifiably implemented, making it highly applicable to areas such as recommendation systems and image processing.

Initialization of User Vectors

In the IIoT for metal casting, VGG-16 plays an important role in enhancing the inspection process by extracting critical features from metal casting images.[24] These features facilitate defect identification and classification by capturing intricate surface textures, shape irregularities, and structural integrity of the castings. First, metal casting images are fed into VGG-16 model which is already trained and has learned from a vast collection of images.

The model identifies and captures important patterns and details, which are then used to construct item vectors that encapsulate the essential characteristics of each casting. Meanwhile, user vectors are initially set utilizing past data that have earlier evaluated similar castings. By synchronizing user vectors with item vectors, the model can effectively determine which castings need further examination or are meeting optimal standards.[25] It does this by comparing them to previously analyzed items, improving the accuracy of quality assessments and recommendations. This seamless integration of VGG-16 improves both the speed and precision of the evaluation process, making it more efficient and reliable, reducing manual effort and improving defect detection in industrial automated system.

Initializing Item Profile Matrix

VGG-16 identifies and captures essential features from metal casting images to generate a comprehensive representation of each item. These features encapsulate distinct properties, such as surface texture variations and shape anomalies, essential for defect detection.[26] To construct the item profile matrix, the extracted features are transformed into item vectors, which can be randomly initialized or derived from prior knowledge. These vectors serve as compact representations of each item's unique characteristics, ensuring consistent feature dimensions across all items. This uniform representation enhances inspection accuracy, enabling effective defect detection and quality assessment throughout the manufacturing process.

Secure Aggregation

Secure aggregation plays a vital role in maintaining privacy and security in decentralized processing systems.[12] In this method, user vectors and item profile matrices are spread across different servers, ensuring that no single entity has full access to the entire dataset. By utilizing advanced cryptographic methods, such as HE and Secure Multi-Party Computation (SMPC), the dot product of these vectors can be determined without sharing sensitive information and individual data.[27] This method guarantees that sensitive user and item information remains protected throughout the computation process, ensuring confidentiality while maintaining accuracy and efficiency in data processing.

Computing Item Gradients

In this scheme VGG-16 is involved for feature extraction, facilitating the computation of item gradients through the dot product of user and item vectors.[28] These computed gradients are subsequently utilized to modify item vectors, aiming to minimize prediction errors and enhance model accuracy. To ensure efficiency and privacy, gradient computation is performed locally on each server, preventing unnecessary data exposure. Additionally, secure aggregation methods, including SMPC and HE, are implemented to securely combine gradients, as presented in Algorithm 3. This approach guarantees that confidential data remains protected throughout the update process while still enabling accurate and reliable model updates.

Updating User Vector

User vectors are refined by performing a dot product operation between item vectors and the user's image data for particular casts, improving the precision of recommendations. These computations are executed locally on each server, ensuring efficient processing while minimizing data exposure. To uphold data privacy and security, secure aggregation methods, such as SMPC and HE, are utilized to merge the computed updates without revealing sensitive information.[29] This approach guarantees that confidential data remains protected while simultaneously improving the precision and reliability of recommendations.

Verification of Aggregated Results

To maintain the system's accuracy and reliability, it's essential to verify the aggregation results. This process involves comparing the item gradients and user vectors against the results derived from plaintext vectors, ensuring consistency and correctness in the computations.[30] This comparison helps identify any inconsistencies or errors in the aggregated data. If any discrepancies are found, they are addressed before proceeding to the next iteration, ensuring that the system's outputs remain reliable and trustworthy.[31] This process plays a key role in guaranteeing that the recommendations generated are both accurate and secure.

Algorithm 1: Matrix Computation

1. Split the dataset across K clients: $A = \bigcup_{k=1}^{K} A_k$
2. Initialize user vectors: $U_k \leftarrow$ random or prior knowledge for client k
3. Partition user vectors and item profile matrix across L servers: $U_k = \bigcup_{l=1}^{L} U_{k,l}, V = \bigcup_{l=1}^{L} V_l$
4. for $t = 1$ to T do

i. Clients compute encrypted dot products: $zk, l = \text{Enc}\left(U_{k,l}V_l^T\right)$ for $k = 1, \ldots, K$ and $l = 1, \ldots, L$

ii. Servers securely aggregate encrypted dot products:

$$z = \sum_{k=1}^{K} \sum_{l=1}^{L} zk, l$$

iii. Servers compute item gradients: $\nabla V_l = \text{HE\_Dec}\ (z)R(U_k)^T$ for $l = 1, \ldots, L$

iv. Servers encrypt item gradients: $\nabla V_{k,l} = \text{HE\_Enc}\ (\nabla V_l)$ for $k = 1, \ldots, K$ and $l = 1, \ldots, L$

v. Clients decrypt item gradients: $\nabla V_{k,l} = \text{HE\_Dec}\left(\nabla V_{k,l}\right)$ for $k = 1, \ldots, K$ and $l = 1, \ldots, L$

vi. Clients update item profile matrices: $V_{k,l} \leftarrow V_{k,l} - \eta \nabla V_{k,l}$ for $k = 1, \ldots, K$ and $l = 1, \ldots, L$

vii. Clients compute encrypted dot products with updated matrices: $wk, l = \text{Enc}\left(U_{k,l}V_l^T\right)$ for $k = 1, \ldots, K$ and $l = 1, \ldots, L$

viii. Servers securely aggregate encrypted dot products:

ix. $w = \sum_{k=1}^{K} \sum_{l=1}^{L} wk, l$

x. Servers compute user vector updates: $\nabla U_l = \text{HE\_Dec}\ (w)V_l R^T$ for $l = 1, \ldots, L$

xi. Servers encrypt user vector updates: $\nabla U_{k,l} = \text{HE\_Enc}\ (\nabla U_l)$ for $k = 1, \ldots, K$ and $l = 1, \ldots, L$

xii. Clients decrypt user vector updates: $\nabla U_{k,l} = \text{HE\_Dec}\left(\nabla U_{k,l}\right)$ for $k = 1, \ldots, K$ and $l = 1, \ldots, L$

Clients update user vectors**:**

$U_{k,l} \leftarrow U_{k,l} - \eta \nabla U_{k,l}$ for $k = 1, \ldots, K$ and $l = 1, \ldots, L$

Algorithm 2: Verifiable Matrix Factorization

Input: A matrix $A \in \{R\}^{m \times n}$, tolerance $\epsilon > 0$
Output: VGG-16 of A: $U \in \{R\}^{m \times m}, V^T \in \{R\}^{n \times n}, \Sigma \in \{R\}^{m \times n}$

1. A: $A = U, \Sigma, V^T, U$ is an orthogonal matrix of $m \times m, \Sigma$ which containsthe singular values of A is of $m \times n$, and V is an orthogonal matrix of $n \times n$.
2. Compute the Frobenius norm of the residual matrix R:
   $|R|_F = | A - U, \Sigma V^T |_F$
3. if then $|R|_F \leq \epsilon$
4. Output U, Σ, and V^T as the output.
5. else
6. Compute the largest singular value of R, denoted by σ.
7. Let U and V be extended to $m \times (m + 1)$ and $n \times (n + 1)$ matrices, respectively, by appending

a column of zeros to each of them. Similarly, extend Σ to an $(m+1)\times(n+1)$ matrix by appending a row of zeros anda zero in the bottom right corner.

8. Set the bottom right entry of Σ to be σ
9. Compute the extended matrix A': $A' = U', \Sigma', V'^T$, where U' and $V'$are the orthogonal matrices of $(m+1)\times(m+1)$ and $(n+1)\times(n+1)$ respectively. While Σ' is a diagonal matrix of $(m+1)\times(n+1)$ containing the singular values of A', it is an orthogonal matrix.
10. Let U be the first m columns of U', Σ be the first $m \times n$ submatrix of Σ', and V is the first columns of V'.
11. Output U, Σ, and V^T as the output.

end if

Algorithm 3: Gradient homomorphic encryption algorithm (GHE_Enc)

Input: Gradient plaintext $g_i = \left(g_{i_1}, g_{i_2}, \dots, g_{i_n}\right)$;
The constant sequence $a = (a_1, a_2, \dots, a_{l+1})$ and $b = (b_1, b_2, \dots, b_n)$;
Output: Gradient ciphertext Y_i and secret shares $f_i(b_1), \dots, f_i(b_n)$;

1. Select a random seed b and t-1 random numbers $y_1, y_2, \cdots, y_{t-1}$;
2. Generate a $l+1$ dimensional vector $r_i = PRG(b)$;
3. Calculate $R_i = CRT(r_i)$;
4. Generate a polynomial using g_i as coefficients and R_i as the constant term: $F_i(x) = R_i + \sum_{j=1}^{l} g_{ij}x^j$;
5. Input $(a_1, a_2, \dots, a_{l+1})F_i(a_1), \cdots, F_i(a_{l+1})$;
6. Blind the $F_i(a_1), \dots, F_i(a_{l+1})$ and package it to be $Y_i = CRT\left(F_i(a_1), \dots, F_i(a_{l+1})\right) + R_i$;
7. Generate a polynomial using $(y_1, y_2, \dots, y_{t-1})$ as coefficients and R_i as the constant term: $f_i(x) = R_i + \sum_{j=1}^{t-1} y_j x^j \bmod q$;
8. input $(b_1, \dots, b_n)$ into $f_i(x)$ to get $f_i(b_1), \dots, f_i(b_n)$;
9. return $\left(Y_i, f_i(b_1), \dots, f_i(b_n)\right)$

Performance Analysis

Experimental Environment and Dataset

The experiments were conducted on an Intel i3 10th generation processor with integrated graphics, using Jupyter Notebook (Anaconda) as the development platform. For the security environment, the PyCrypto library was utilized. The model leverages VGG-16, CNN model with 16 layers, to process image data. The tests were carried out using Python 3.10. The metal casting dataset[32] used in the proposed VFL-HMF model for matrix factorization contains both defective and non-defective castings, collected during industrial automation processes. This dataset, shown in Fig. 3, includes images of metal castings with various defects such as blow holes, burrs, mold material issues, pinholes, pouring metal irregularities, shrinkage, and metallurgical defects, all common in IIoT-driven manufacturing environments.

Experimental Results

The variation in Mean Square Error (MSE) over 10 epochs for the training and validation phases of VFL-HMF is depicted in Fig. 4(a) and classification report of the experiment in Fig. 4(b). The MSE decreases significantly during the initial epochs, reflecting rapid learning and optimization. By epoch 4, the MSE stabilizes, showcasing the model's convergence. The "Best" MSE value remains constant at approximately 0.8649 throughout the process, emphasizing the model's ability to achieve consistent performance. The MSE fluctuates within a narrow range of 0.8645 to 0.8658, with an average value of 0.8651, highlighting the reliability of the model as shown in Table 2. Notably, the training phase shows continuous improvement, achieving the lowest MSE by the 10th epoch, suggesting the model effectively minimizes errors as it learns. The model achieved a testing accuracy of 61.54%, as calculated from the predicted class labels which is depicted in Fig. 5.

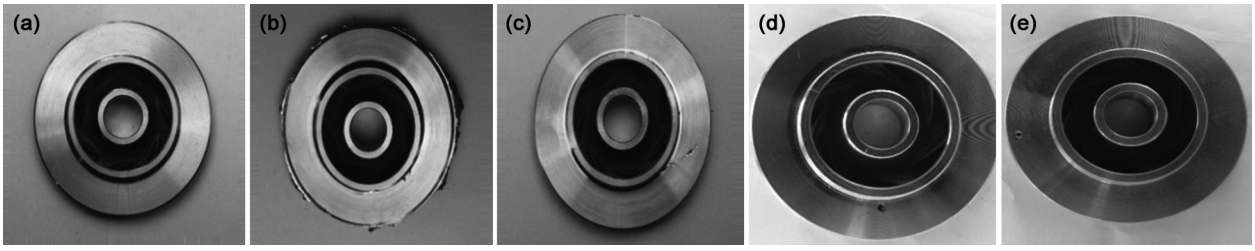

Fig. 3 — Data set samples: (a) Correct sample, (b) Burr, (c) Mould material defect, (d) Pinhole, and (e) Shrinkage defect sample

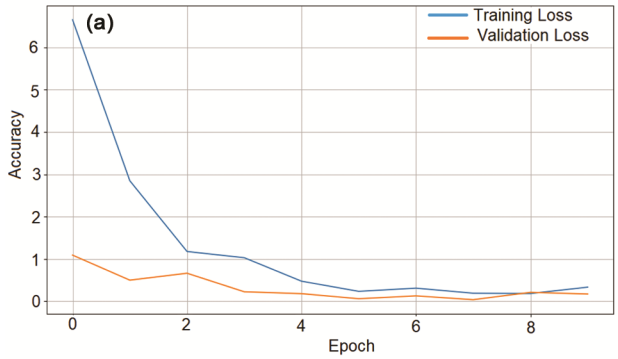

Fig. 4 — (a) Training and validation loss, and (b) Classification report of the experiment

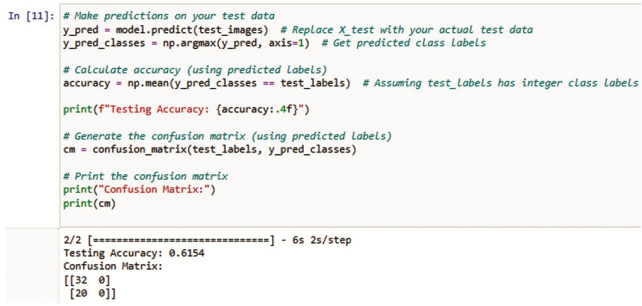

Fig. 5 — Testing accuracy

Table 2 — Mean square error across various data subsets

Characteristics of a metadata set	MSE
Continuous valued metadata (CVM)	3.24
CVM + casting data	2.88
Discrete valued metadata (DVM)	4.65
DVM + casting data	5.31
Continuous and DVM	1.87
Continuous, DVM and casting data	1.18
Experimented MSE of VFL-HMF on casting dataset	0.86

The confusion matrix shows that the model correctly identified all 32 instances of the 'defect' class but failed to classify any of the 20 'ok' instances, predicting all test samples as 'defect' and resulting in a biased classification outcome as illustrated in the Fig. 6(a) and Fig. 6(b).

The Computation on encrypted data (Comp) is the most time-intensive task, reflecting the overhead of

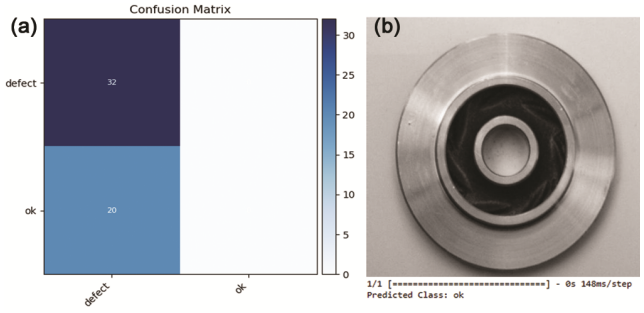

Fig. 6 — (a) Confusion matrix, and (b) Predication validation

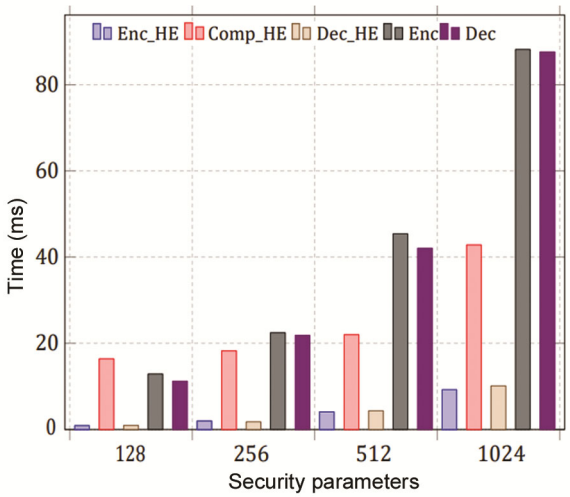

Fig. 7 — Time taken for various steps of security processing against different security parameters

Table 3 — Performance comparison of Encryption (Enc), Computation (Comp), and Decryption (Dec) times with and without Homomorphic Encryption (HE) across different security parameters (λ)

Security Parameter	Using HE (ms)			Without HE (ms)	
	Enc	Comp	Dec	Enc	Dec
$\lambda = 128$	0.92	16.42	0.95	12.86	11.24
$\lambda = 256$	1.98	18.25	1.79	22.44	21.88
$\lambda = 512$	4.10	22.02	4.35	45.43	42.12
$\lambda = 1024$	9.25	42.85	10.12	88.20	87.65

performing secure operations without decryption. Standard encryption (Enc) and decryption (Dec) are significantly faster and scale more efficiently with input size, making them suitable for real-time applications where security during computation is not a requirement as represented in Table 3. The execution time of various cryptographic operations, including homomorphic encryption (Enc_HE), computation on encrypted data (Comp_HE), and decryption (Dec_HE), alongside standard encryption (Enc) and decryption (Dec), is compared in Fig. 7 for input security parameters ranging from 128 to 1024.

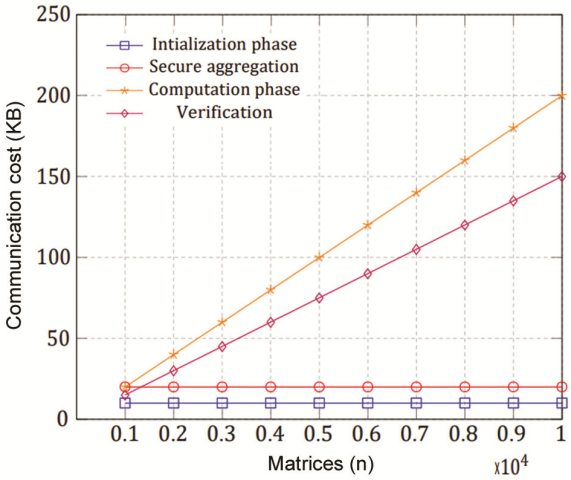

Fig. 8 — Communication cost across different phases as a function of matrix size (n)

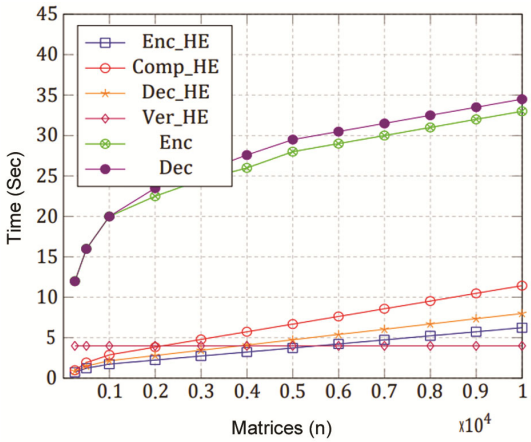

Fig. 9 — Time consumption for secure processing against the number of matrices

Execution times increase with input size, particularly for homomorphic operations, due to their computational complexity. The graph underscores the trade-off in HE, where enhanced security is achieved at the cost of computational performance.

The communication cost (in kilobytes) across various phases of secure data processing—initialization, secure aggregation, computation, and verification—is illustrated in Fig. 8 relative to the number of matrices processed. Communication cost increases linearly with the number of matrices. The computation and verification phases dominate, as they involve extensive data transfer and processing. Conversely, initialization and secure aggregation incur minimal costs, even for larger datasets, indicating their optimization.

Processing times (in seconds) for various cryptographic operations as the number of matrices

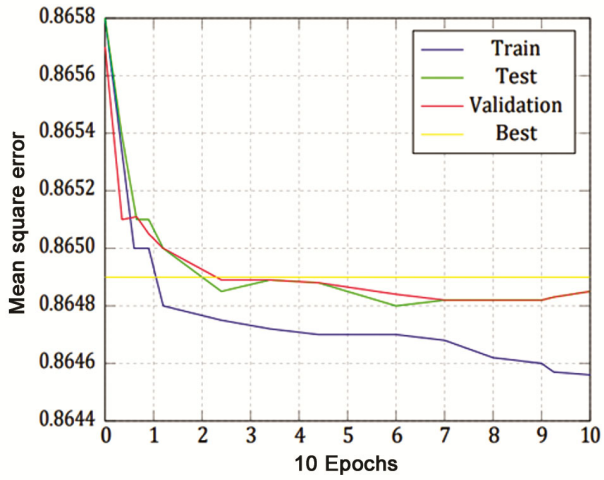

Fig. 10 — Mean Square Error against 10 epochs

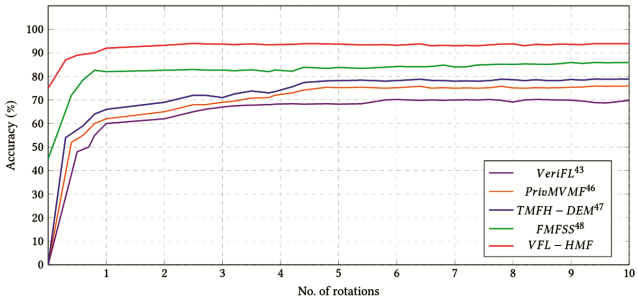

Fig. 11 — Accuracy of different schemes compared with the proposed model

(scaled by 10^4) increases are shown in Fig. 9. HE operations (Enc_HE, Comp_HE, Dec_HE, Ver_HE) initially outperform traditional methods (Enc, Dec) for smaller matrix sizes. However, as the number of matrices grows, the time difference narrows. Among HE operations, Comp_HE shows the slowest growth, indicating better scalability for encrypted computations, while traditional methods remain efficient for smaller datasets.

The Mean Square Error (MSE) during training, testing, and validation over 10 epochs is depicted in Fig. 10. The x-axis represents the number of epochs, while the y-axis indicates the MSE values. The training error (blue line) decreases steadily, indicating effective learning and model fitting. Validation (red) and test (green) errors stabilize after a few epochs, reflecting good generalization. The "Best" line (yellow) highlights the optimal MSE achieved, serving as a benchmark for performance.

The accuracy of the proposed VFL-HMF model is compared with existing methods such as VeriFL[13], PriMV-MF[15], TMFH-DEM[16], and FMFSS[17] across 10 rotations, as shown in Fig. 11. The VFL-HMF

Table 4 — Comparative Analysis of communication overheads between data users (DU) and cloud service providers (CSP)

Models	Participants	DU → CSP	CSP → DU	Time complexity
SNMF[5]	Each DU	5(d+1)λ	1	$O(n^2)$
	CSP	0	5λ	O(n2)
WDMF[6]	Each DU	6(7d+1)λ	0	O(n)
	CSP	0	6+λ	O(log n)
RSNMF[7]	Each DU	(d+1)λ	0	O(n)
	CSP	0	12λ	$O(n^2)$
VeriFL[13]	Each DU	(d+1)λ+(15d+1)λ	0	$O(n^3)$
	CSP	0	7λ	O(n)
Mask[14]	Each DU	(d+1)λ+(12d+13)λ	0	O(log n)
	CSP	0	2κ+13λ	O(n)
PrivMVMF[15]	Each DU	(d+1)λ+2λ	0	O(log n)
	CSP	1	3λ+2λ	O(n log n)
TMFH-DEM[16]	Each DU	4λ+λ	0	O(log n)
	CSP	0	λ+2λ	O(log n)
FMFSS[17]	Each DU	λ	0	O(n)
	CSP	0	λ+λ	O(n log n)
PrivFL[19]	Each DU	3(d+1)λ	1	O(n log n)
	CSP	0	λ	O(n2)
VANE[20]	Each DU	(7d+1)λ	1	O(n2)
	CSP	0	2λ	O(n)
V-Net[21]	Each DU	5(d+1)λ	0	O(n2)
	CSP	0	12λ	O(log n)
VFL-HMF (Proposed Model)	Each DU	2λ	0	O(1)
	CSP	0	2λ	O(1)

model outperforms its counterparts, achieving the highest accuracy of 93%, which stabilizes after the fourth rotation. FMFSS demonstrates the second-best performance with an accuracy plateau of around 85%, while TMFH-DEM and PriMV-MF achieve lower accuracies of approximately 75% and 70%, respectively. VeriFL exhibits the poorest performance, leveling off at around 60%. The rapid convergence of VFL-HMF within the first few rotations highlights its efficiency, and its consistent accuracy beyond four rotations demonstrates its robustness and reliability compared to the other models.

Discussions

The results derived from the experimental analysis highlight the performance and efficiency of the proposed model, as observed in Figs. 3–11 and Tables 2–4. The approximate rating generated by the model demonstrates its capability to provide precise predictions. Over 10 epochs, the MSE fluctuates between 0.8645 (minimum) and 0.865 (maximum), with an average value of 0.865. The optimal result obtained, 0.864, underscores the model's ability to predict efficiently. The application of HE in matrix factorization under different security parameters is analyzed in and the obtained results indicate that the encryption, decryption, and computation times decrease gradually as the security parameter increases. Despite this, the time complexity remains constant at $O(1)$, and the space complexity is also $O(1)$. These findings validate the computational efficiency of the proposed scheme under varying security levels. Further experiments involving 10,000 matrix sets reveal that computations performed in the encrypted state, such as encryption, decryption, computation, and verification takes less time compared to traditional methods. The average time for computation using the proposed method is less than 5 seconds; this demonstrates the model's effectiveness in secure and efficient computation on encrypted data within a cloud environment.

The data exchange overhead between the client and server across various operational stages is also analysed. The cost remains constant at 10 KB for the initialization phase across 1,000 to 10,000 matrices, and the secure aggregation shows no significant variation regardless of the number of matrices. However, the computation phase exhibit a gradual rise in communication cost as the matrix size grows, indicating their dependence on data volume. The comparative analysis, presented in Table 4, shows that the proposed VFL-HMF model outperforms existing works[32] in terms of verification, aggregation of data, and HE.[33] It achieves these outcomes with

reduced communication time and cost, highlighting its practical advantages. Additionally, accuracy comparisons with recent similar works[15] reveal that the proposed scheme achieves better accuracy; with an average of 93% at 10 rotations.[16] This demonstrates the robustness and reliability of the proposed model in delivering high accuracy and efficient performance in matrix factorization tasks.

Overall, the results confirm that VFL-HMF model is highly efficient in secure computations, communication cost optimization, and prediction accuracy, making it a viable solution for advanced machine learning applications on encrypted data.

Conclusions

This research introduces the VFL-HMF model which a significant development in mitigating the challenges of privacy and security in IIoT systems. The primary contribution lies in integrating homomorphic encryption with federated learning, enabling secure, verifiable computations while preserving data privacy. Employing the VGG-16 architecture for feature extraction, the model demonstrates exceptional performance in industrial applications, particularly for analyzing casting datasets, achieving remarkable computational efficiency and accuracy. While the proposed model effectively addresses major concerns, certain limitations remain. The reliance on homomorphic encryption increases computational overhead, albeit to a manageable degree, and scalability to highly diverse datasets requires further optimization. Despite these constraints, the VFL-HMF model shows immense potential for applications in predictive maintenance, defect detection, and other IIoT domains where data security is paramount.

Future work will focus on reducing computational costs, enhancing real-time processing capabilities, and integrating advanced cryptographic methods. These efforts focus on making the model more versatile, robust, and adaptable to complex IIoT environments.

References

1 Yazdinejad A, Dehghantanha A, Parizi R M, Hammoudeh M, Karimipour H & Srivastava G, Federated learning for cyber threat hunting in blockchain-based IIoT networks, *IEEE T Ind Inform*, **18(11)** (2022) 8356–8366,doi: 10.1109/TII.2022.3168011.

2 Si S, Wang J, Zhang R, Su Q & Xiao J, Federated non-negative matrix factorization for short texts topic modeling with mutual information, *Int Joint Conf Neural Net* (Padua, Italy) 2022, 1–7, doi: 10.1109/IJCNN55064.2022.9892602.

3 Xicheng W, Yifeng Z, Qun L, Anmin F, Mang S & Yansong G, Towards privacy-preserving and verifiable federated matrix factorization, *Knowledge Based Syst*, **250** (2022) 109193, doi: 10.1016/j.knosys.2022.109193

4 He Y, Wang C & Jiang C, Correlated matrix factorization for recommendation with implicit feedback, *IEEE Trans Knowl Data Eng*, **31(3)** (2019) 451–464, doi: 10.1109/TKDE.2018.2840993.

5 Luo X, Zhou M, Xia Y & Zhu Q, An efficient non-negative matrix factorization based approach to collaborative filtering for recommender systems, *IEEE T Ind Inform*, **10(2)** (2014) 1273–1284, doi: 10.1109/TII.2014.2308433.

6 Li Z & Tang J, Weakly supervised deep matrix factorization for social image understanding, *IEEE Trans Img Proc*, **26(1)** (2017) 276–288, doi: 10.1109/TIP.2016.2624140.

7 Li Z, Tang J & He X, Robust structured nonnegative matrix factorization for image representation, *IEEE Trans Neural Net Learn Syst*, **29(5)** (2018) 1947–1960, doi: 10.1109/TNNLS.2017.2691725.

8 McAuley J & Leskovec J, Hidden factors and hidden topics: Understanding rating dimensions with review text, *In Proc 7th ACM Conf Recommender Syst* (Association of Computing Machinery) 2013, 165–172.

9 Zheng L, Noroozi V & Yu P S, Joint deep modeling of users and items using reviews for recommendation, in *Proc. 20th ACM Int Conf Web Search Data Mining* (Association of Computing Machinery) 2017, 425–434.

10 Chen C, Zhang M, Liu Y & Ma S, Neural attentional rating regression with review-level explanations, in *Proc World Wide Web Conf* (Association of Computing Machinery) 2018, 1583–1592.

11 Wu L, Quan C, Li C, Wang Q, Zheng B & Luo X, A context aware user-item representation learning for item recommendation, *ACM Trans InfSyst*, **37(2)** (2019) 1–29, doi: 10.1145/3298988.

12 Izmeci B C & Og¨ud¨uc¨u S G, Predicting IMDb ratings of pre-release movies with factorization machines using social media, *2018 3rd Int Conf Comp Sci Eng, Sarajevo* (Bosnia and Herzegovina) 2018, 173–178.

13 Guo X, Liu Z, Li J, Gao J, Hou B, Dong C, & Baker T, VeriFL: Communication-efficient and fast verifiable aggregation for federated learning, *IEEE T InfForens Sec*, **16** (2020) 1736–1751, doi: 10.1109/TIFS.2020.3043139.

14 Han S, Ding H, Zhao S, Ren S, Wang Z, Lin J & Zhou S, Practical and robust federated learning with highly scalable regression training, *IEEE Trans Neural Netw Learn Syst*, **35(10)** (2024) 13801–13815.

15 Mai P & Pang Y, Privacy-preserving multiview matrix factorization for recommender systems, *IEEE T Artific Int*, **5(1)** (2024) 267–277, doi: 10.1109/TAI.2023.3240700.

16 Zhou J, Gao G, Cao Z, Choo K-K R &Dong X, Lightweight privacy-preserving distributed recommender system using tag-based multikey fully homomorphic data encapsulation, *IEEE T Depend Secure*, **20(6)** (2023) 5230–5246, doi: 10.1109/TDSC.2023.3243598.

17 Zheng X, Guan M, Jia X, Sun L & Luo Y, Federated matrix factorization recommendation based on secret sharing for privacy preserving, *IEEE Trans Comput Soc Syst*, **11(3)** (2023) 1–11.

18 Mnih A & Salakhutdinov R, Probabilistic matrix factorization, in *Adv Neural Inf Proc Sys*, (2007) 1257–1264.

19 Mandal K & Gong G, PrivFL: Practical privacy-preserving federated regressions on high dimensional data over mobile

networks, in *Proc 2019 ACM SIGSAC Conf Cloud Comput Security Workshop,* (2019) 57–68.

20 Wang F, Zhu H, Lu R, Zheng Y & Li H, A privacy-preserving and non-interactive federated learning scheme for regression training with gradient descent, *Inf Sci*, **552** (2021) 183–200, doi: 10.1016/ j.ins.2020.12.007.

21 Xu G, Li H, Liu S, K Yang & Lin X, VerifyNet: Secure and verifiable federated learning, *IEEE T Inf Forens Sec*, **15** (2020) 911–926, doi: 10.1109/TIFS.2019.2929409.

22 Pan S, Zheng F, Zhu W T & Wang Q, Harnessing the cloud for secure and efficient outsourcing of non-negative matrix factorization, *IEEE Conf Commu Netw Sec,* (Beijing, China) 2018, 1–9.

23 Kotsia I, Zafeiriou S & Pitas I, A novel discriminant non negative matrix factorization algorithm with applications to facial image characterization problems, *IEEE Trans Inform Forensic Secur*, **2(3)** (2007) 588–595.

24 Liu T & Tao D, On the performance of manhattan nonnegative matrix factorization, *IEEE Trans Neural Netw Learn Syst*, **27(9)** (2016) 1851–1863, doi: 10.1109/ TNNLS.2015.2458986.

25 Mohammadiha N, Smaragdis P & Leijon A, Supervised and unsupervised speech enhancement using nonnegative matrix factorization, *IEEE Trans Audio Speech Lang Proc*, **21(10)** (2013) 2140–2151.

26 Sawada H, Kameoka H, Araki S & Ueda N, Multichannel extensions of non-negative matrix factorization with complex-valued data, *IEEE Trans Audio Speech Lang Proc*, **21(5)** (2013) 971–982, doi: 10.1109/TASL.2013.2239990.

27 Mahato G K & Chakraborty S K, Securing edge computing using cryptographic schemes: A review, *Multimed Tools Appl,* **83(12)** (2024) 34825–348481–24, doi: 10.1007/s11042-023-15592-7.

28 Cao X, Zhao Q, Meng D, Chen Y & Zu Z, Robust low-rank matrix factorization under general mixture noise distributions, *IEEE Trans Imag Proc*, **25(10)** (2016) 4677–4690.

29 MahatoG K, Banerjee A, Chakraborty S K & Gao X-Z, Privacy-preserving verifiable federated learning scheme using blockchain and homomorphic encryption, *Appl Soft Comput*, **167** (2024) 112405, doi: 10.1016/ j.asoc. 2024.112405.

30 Luo X, Zhou M, Xia Y & Zhu Q, An Efficient non-negative matrix factorization-based approach to collaborative filtering for recommender systems, *IEEE T Ind Inform*, **10(2)** (2014) 1273–1284, doi: 10.1109/TII.2014.2308433.

31 Mahato G K & Chakraborty S K, A comparative review on homomorphic encryption for cloud security, *IETE J Res*, **69(8)** (2023) 5124–5133, doi: 10.1080/03772063. 2021. 1965918.

32 https://www.kaggle.com/datasets/ravirajsinh45/real-life-industrial-dataset-of-casting-product [Accessed on 5 May 2024].