Hybrid Machine Learning for Privacy-Preserving Multi-Modal Data Analytics: An Application-Oriented Framework

Rella Usha Rani[1] Bhuvan Unhelkar[2] Siva Shankar S[3] Parasana Sankara Rao[4]

[1]Professor, CSE(AI&ML), CVR College of Engineering, Hyderabad. And Post Doc Researcher, Muma College of Business, University of South Florida 8350 N. Tamiami Trail, Sarasota, Florida. USA. **Teaching.usha@gmail.com**

[2]Professor, Muma College of Business, University of South Florida 8350 N. Tamiami Trail, Sarasota, Florida. USA. **bunhelkar@usf.edu**

[3]Professor & IPR Head, Department of Computer Science and Engineering, KG Reddy College of Engineering and Technology, Hyderabad, Telangana, India**, drsivashankars@gmail.com**

[4]Associate Professor, Department of CS & SE, GSCSE, GITAM (Deemed to be University),Vishakapatnum, **dr.sankararaop@gmail.com**.

Received: 15/01/2026. Accepted:05/03/2026. Published: 10/08/2026

Abstract - In the context of applications in healthcare, finance, and smart cities, the volume of sensitive information is increasing rapidly. The conventional centralized mechanisms pose challenges as ownership losses (unauthorized access), data leakage, and non-compliance with GDPR and HIPAA privacy regulations. To overcome these, two approaches are integrated with best practice components in the architecture, which progress towards a novel framework with modular, integrated FL-DP, such as Federated learning and Differential Privacy. In this, Federated learning uses decentralized training of the model among multiple entities without sharing raw data, whereas differential privacy injects calibrated noise to avoid member attacks and inference attacks for ensuring guaranteed privacy. The hybrid model uses attributes such as sensor data, clinical information, and contextual content by ensuring high modal utility. The hybrid approach provides a state-of-the-art framework for privacy-preserving that enables scalable, secure, and compliant data processing in a distributed environment. Both privacy and accuracy are achieved using client-level differential privacy with adaptive privacy budgeting, cross-modal feature fusion, and momentum-based federated optimization. Experimental results show that the hybrid model outperforms the benchmark methods, such as Centralized frameworks, Homomorphic encryption, Multi-party Computation (MPC), and Trusted execution environments. In addition, it supports multi-party collaboration, and heterogeneous data sources.

Keywords: Centralized framework, Privacy, Distributed processing, Collaboration Learning, Differential Privacy, and Accuracy.

1. Introduction

The use of applications such as healthcare, finance, cloud-based, and smart cities is increasing nowadays, and sensitive information is present in data generated from sensors, clinical records, and contextual data. Approaches like traditional central machine learning would suffer from data

leakage, non-compliance, and unauthorized access, although they would ensure better accuracy. Centralized systems face storage issues in terms of scalability and fail to support collaborative intelligence across distributed organizations, creating motivation for designing secure and privacy-oriented mechanisms. Traditional federated learning, although implemented in a decentralized manner, maintains raw data locally; the federated learning is still vulnerable to inference attacks, data poisoning, and data leakages by shared model updates. This scenario-based activity demands a strong privacy mechanism.

Some gaps in the existing methods are described, such as a lack of adaptive privacy control, and yet, exposing sensitive information by gradients is observed in the traditional federated learning approach. The other approach fixed differential privacy budgets, reducing accuracy because of over noise. Homomorphic Encryption, Trusted Execution, and Multi-party computation communication systems, although protected as cryptographic solutions, but suffer in limited scalability, computational overhead, and increased system complexity. The literature survey emphasizes challenges in maintaining utility, privacy, and performance under non-IID and heterogeneous environments. This scenario requires hybrid architecture to overcome these drawbacks of existing methods.

Hence, a proposed approach of dynamic federated learning, adaptive differential privacy budgets, and core optimization components together to ensure strong privacy. The integration of cross-model fusion via adaptive gated mechanisms and client-level differential privacy, dynamic privacy budgets, and clipping norms guarantees strong privacy with scarifying performance. Further integration of secure aggregation stops individual contributions, and momentum-based federated optimization ensures global model accuracy and convergence stability. The proposed FL+DP+Core optimization mechanisms enable decentralized collaboration across heterogeneous platforms and ensure scalability and regulatory compliance. The hybrid approach proposed would be an effective solution for distributed environments where accuracy is improved, minimized error rate, and balanced utility and privacy against privacy preserving baselines and centralized systems.

2. Literature Review

There are studies to analyze privacy preservation in a network using the traditional, centralized, Federated learning, Differential Privacy, Homomorphic Encryption, and hybrid methods. The studies reviewed in this section are categorized into domains such as Threats and Defenses using Federated Learning, Adaptive and dynamic differential privacy with Federated Learning, Cryptographic enhanced federated learning, Hybrid privacy preserving methods, Incentive mechanisms, and Domain-specific applications.

2.1 Threats and Defenses using Federated Learning:

This domain focuses on identifying security threats such as poisoning, Byzantine, and inference attacks, and recommends defense solutions. Feng, Y., Guo, Y., Hou, Y. et al. (2025) [1] demonstrate that federated learning emerged as a solution towards privacy protection in AI, in which attacks such as byzantine, etc., are possible. The inaccessibility of data in federated

learning makes it difficult to defend against these attacks. The recommendations suggest navigating from data-centric to model and behavioral-centric defenses for ensuring security over federated learning from many sources. Gosselin, R., Vieu, L., et al. (2022) [3] demonstrate that privacy concerns arise when transforming from centralized to decentralized approaches, and countries imposing rules on data use and their safety. Hence, Federated Learning is preferred where local models are trained collaboratively to update the global model to enhance detection. The countermeasures and defending approaches are identified against poisoning, and inference attacks were addressed by FL based approach. Guembe, B. (2024) [4] reviews 11 attacks, 6 countermeasures, and studies categorized into 5 kinds, where 38% were addressed to data poisoning as a regular attack, and 25% were addressed on all kinds of attacks. In addition to FL, Differential privacy was used to combat some attacks, and anomaly detection was used to combat others, based on the results section. Ioannis Makris, Aikaterini Karampasi,et al. (2025)[5], in which attacks evolved due to AI usage, require defending them. Hence, federated IDS is applied over multiple scenario-based applications like IIoT, where security for their operations must be provided. The various attacks, challenges, datasets, and communication protocols were discussed over FL implementation.

2.2 Adaptive and dynamic differential privacy with Federated Learning:

This explores limitations of fixed privacy budgets, and balances privacy and utility by adjusting noise, budgets, or weights in heterogeneous clients, and training. Guiping Zheng, Bei Gong, et al. (2025)[2] explores need for federated learning due to the heterogeneous generation of data by IoT. The fixed differential privacy suffers from issues like a lack of dynamic adjustments as per varying training phases and limited effectiveness. This approach makes use of dynamic adjustment of weights and dynamic privacy budget adjustments. It starts by assigning privacy budgets to client models, then assigning different weights to each client model, which would enhance the global model to ensure a balance between privacy and performance. Shanwei Chen, Xiuzhi Qi (2025)[6] demonstrate privacy of student records of baoji university, china is challenging; hence proposed a MLP model with adaptive private budgets, which produces an accuracy of 92% and an entropy of 0.2, which are better than federated learning and is near to centralized learning. The model ensures a balance between privacy and accuracy using early adaptive differential privacy and federated learning. YANG ZHANG, SHIGONG LONG, et al. (2025)[7] demonstrate integrated differential privacy-based federated learning due to attacks in federated learning usage. This model works on a clustered model with random selection for learning different distributions to address heterogeneity. The usage of differential privacy ensures clients' privacy, and the addition of adaptive clustering ensures high accuracy. The results of the proposed model are observed to be improved over other models on different databases. Tayyeh, H. K., & AL-Jumaili, A. S. A. (2024)[14] demonstrate that the use of FL to ensure model training across multiple entities and hyperparameter tuning to balance privacy and performance is significant. The usage of privacy budget (ϵ), clipping norm (C), is to add noise, which would influence scenarios called independent Identically Distributed (IID) and non-dependent IIDs. The

results observed were better for non-IID in terms of high client interaction and under strict privacy constraints. Guo, S., Yang, J., et al. (2024)[17] state that leakage of data is possible using FL method, but this would be overcome by improved differential privacy with Fast Fourier transforms(FFTs) for computing privacy budgets that are tightly bounded, to reduce the impact of limited resources. The adoption of loss distribution, private budgets improve privacy and minimizes the error rate by truncation. To ensure accuracy and avoid fluctuation in training, sigmoid activation is used with t. MARIA IQBAL, ASADULLAH TARIQ (2023) [18] explore results in terms of accuracy, and privacy are optimized using optimized differential privacy-based FL(FL-ODP) than only individual Federated learning. This model of the study improves to extract specific sensitive content over MNIST dataset and Fedavg aggregator. The model was performed in 3 phases, in which FL was used in the first round, and adjusting hyperparameters like delta and noise using opacus feature in 2nd and 3rd rounds for ensuring efficiency of the proposed approach.

2.3 Cryptographic-enhanced federated learning:

This domain explores cryptographic techniques such as homomorphic encryption, secure aggregation, and secret sharing to ensure the confidentiality of model updates and security against leakages. Gong, C., Zhang, X., et al. (2025)[8] explore the integration of federated learning against machine learning for ensuring privacy, and make a centralized aggregation of heterogeneous data dispersed across numerous places. For safeguarding, the proposed model is integrated with homomorphic encryption and differential privacy for the disclosure of information, and it also ensures three-stage level protection of data. Cong Shen, Wei Zhang, et al. (2024)[9] demonstrate the significance of federated learning as a good entity between cross-device and cross-agency environments. Due to privacy leakage, high traffic, and high complexity in federated learning, a double privacy mask algorithm is required. The combination of secret sharing and homomorphic encryption won't allow compromise in privacy using private gradients by clients. The gradient model Top Q Random R would filter gradient encryption, hence reducing traffic and overhead by a significant %. Shen, J., Zhao, Y., et al. (2024) [10] explore the possibility of data leak may violate privacy at rare times, although it ensures privacy. The single key on client and server, multi-key homomorphic encryption in semi-honest settings poses specific challenges in privacy. Hence, proposed a privacy-preserving FL with multi-key homomorphic encryption in which an aggregated public key for encryption and clients are involved in decryption communication. This model encrypts model updates using fully multi-key homomorphic encryption to ensure confidentiality in the proposed environments. Adnan, A., Kausar, F., et al. (2025)[21] demonstrate that there are privacy issues although federated learning is used in the health domain, where patient records, in which sensitive data is to be protected. Hence, proposed a privacy-preserving FL with homomorphic encryption to ensure secure privacy using the same EfficientNet throughout the network, of multiple organizations. The derived model makes use of CKKS encryption in order to prevent inference attacks, and ensures accuracy of 83% and 81% over the datasets Blindness Detection dataset and MosMedData CT.

2.4 Hybrid privacy-preserving methods:

This domain explores federated learning with multiple privacy-enhancing technologies, including differential privacy, cryptography, and secure collaboration for achieving strong privacy. Abdulrahman Alamer (2024)[11] discussed malware in the digital era, and existing ML models fail to detect new unknown threats due to a lack of dynamic nature. With IoT, data increases in volume, which leads to malware also growing. The centralized approach is outdated due to a lack of privacy assurance. The derived approach in this study is privacy-preserving FL with secure collaboration. Privacy ensured by signcryption and CC is used for the aggregation of data. The specific incentive model stakelberg incentive approach brings IoT devices to collaborate for heterogeneous data. The datasets determine the effectiveness of the proposed model. Oshamah Ibrahim Khalaf, Ashokkumar S.R, et al. (2024) [12] explore that although FL trains model among users without exposing raw data, required to balance privacy and utility. Hence, a hybrid fusing differential privacy with FL is designed. This hybrid approach, when experimented with MNIST and CIFAR observed accuracy improvement of 4 and 9%. In non-IID settings, the diverse DL methods' performance declines. Compared against ML and traditional FL methods, hybrid approach ensured on two datasets in accuracies of 96% and 82%. WANGXIN, LI JIAQIAN, et al. (2024)[15] demonstrate the categorization of approaches for improving privacy. In this, two approaches such as central DP-based FL and Local DP-based, although DP reduces accuracy, but ensures privacy convergence. In this, cental DP base make use of asynchronous privacy and gaussian component for accuracy, and the local DP base uses multidimensional data for accuracy assurance. The varieties such as the shuffle approach, Bayesian, homomorphic encryption, and Direction multipliers are analyzed in terms of challenges and future directions.

2.5 Incentive based privacy mechanisms:

This domain explores incentive models and game-theoretic approaches to motivate participation to enhance stability, fairness, and long-term collaboration. Ni, Z., & Zhou, Q. (2025)[16] explore FL training in ensuring privacy faces certain challenges. To overcome issues, evolutionary game theory was introduced for analyzing strategies, and use utilities for Gaussian noise and training in iterations. The involvement of evolutionarily stable strategies (ESSs) ensures stability through simulations. The incentive allocation and evolutionary gaming theory forms a valuable approach for privacy assurance. Siqin, Z., Xiaohong, W., et al.(2025)[23] demonstrate that personalized privacy protection based on auction-based privacy preserving FL approach, where theoretically dominant strategy incentive compatibility, individual privacy concerns, and privacy budgets are enforced to provide privacy over datasets such as CIFAR and MNIST. The auction-based incentive model ensures 14%, 4%, and 1% improvement in the variety of integrated FL approaches.

2.6 Domain-specific applications:

This domain explores application areas such as healthcare, IoT, education, cloud-based, and location-based services. Regarding healthcare, Nazish Khalid, Adnan Qayyum, et al. (2023)[20]

denote translating AI work into clinically validated applications to assess effectiveness. The barriers identified in AI-validated applications are limited datasets, nonstandard records, and strict ethical requirements. Specific approaches are analyzed, such as federated learning and hybrid approaches, to address the issues of AI-validated applications. Regarding location-based, Wang, B., Li, H., et al. (2023)[13] discuss privacy issues regarding users' location based on mobile devices using location-based services. To provide privacy, location-based differential privacy is recommended for protecting users' locations. Based on location distance and density, a cluster is created. The proposed model of this study ensures a high level of data utility and minimum consumption of time by adding Laplace noise to use points and centroids in the cluster.

2.6.1 Cloud-based distributions:

Dey and Sangaraju (2024) [24] demonstrate particle swarm optimization (PSO) for dynamic resource allocation and reducing response times due to the integration of global and local stabilities of the cloud. Dey and Sangaraju (2023)[25] compared the performance of hybrid load balancing over a data center against traditional methods and observed hybrid model performs better due to the integration of multiple scheduling heuristics. Allamudi and Hrushikesava Raju (2025)[26] provide a hybrid machine learning–based fraud detection to balance accuracy and performance by integrating multiple classifiers, to achieve improved detection rates while mitigating false positives. Raju et al. (2024)[27] discussed a defect detection approach for flyovers, leveraging Faster R-CNN for spatial feature extraction, LSTM for temporal features, and transfer learning to ensure better accuracy.

2.7 Blockchain-based privacy and compliance methods:

This domain depicts blockchain technologies to enhance trust, transparency, and regulatory compliance in federated learning systems, using Smart contracts and decentralized ledgers. Li, K., Lohachab, A., et al.(2025)[19] represent that blockchain-based solutions in terms of regulatory compliance, and maturity levels provided by Technology Readiness Levels (TRLs). Security is ensured using smart contracts and cyphertext policy encryption methods. The review on methods in blockchain analysis concludes that most solutions fall in TRL3 and there is less progress in TRL5. The approaches were reviewed in terms of challenges and benefits based on integration and system design patterns.

Barbaria, S., Jemai, A., et al. (2025)[22] discuss existing methods like central mechanisms suffer in balancing privacy due to inadequate methods, some traditional compliance methods consume more time, and depend on manual auditing. Hence, required a blockchain based that maximum take advantage of HL7 and Hyperledger to automate regulatory compliance using smart contracts. Security is ensured using a decentralized control mechanism and protection using cryptographic protocols.

3. Methodology

In this, three aspects were demonstrated in terms of significant modules identification in Fig.1, flow of activities demonstration in Fig.2, architectural diagram of proposed system is

demonstrated in Fig.3, and implementation of hybrid FL+DP+Core components addition framework in PS1.

Fig.1 demonstrates modules such as data acquisition after application selection, data preprocessing, fusion of multimodalities, federated learning orchestrator, client level differentia privacy budgets, core components involved such as clipping norms, noise injection, adaptive privacy budgets, momentum based federated learning, and effectiveness of the model evaluation.

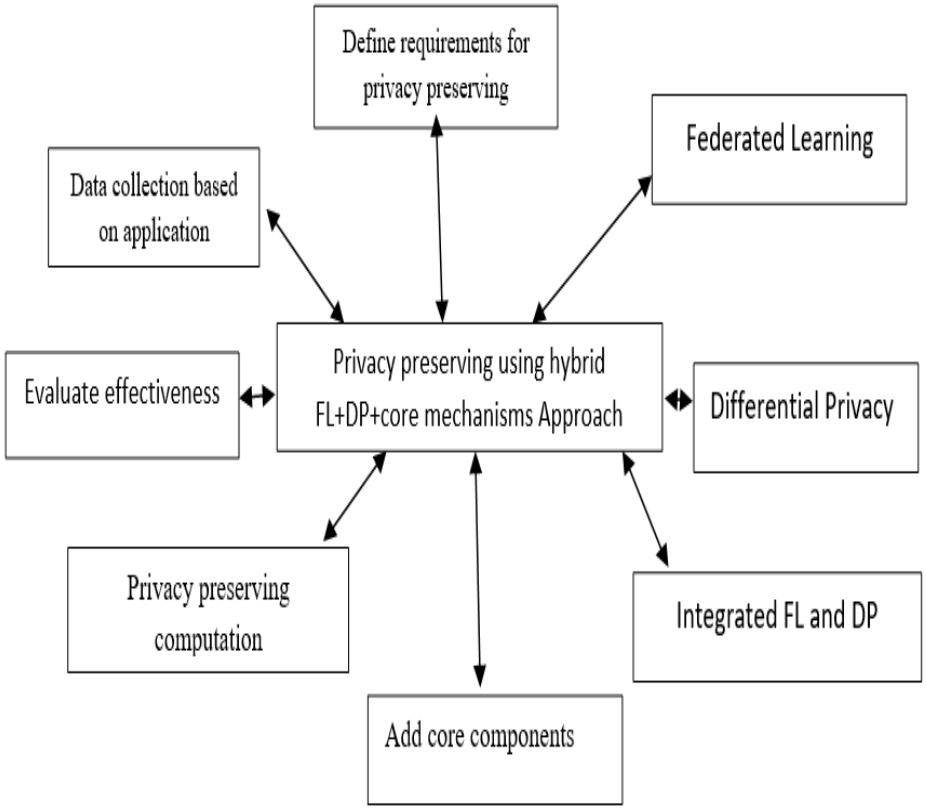

Fig.1. Significant modules involved in Hybrid FL+DP+Core components Approach

Fig.2 demonstrates the flow of activities involved in proposed model where selection of multi-domain and multi-modal datasets is done first and preprocessed through context standardization and missing-modality simulation. From sensor and contextual inputs are combined for defining Feature embeddings using gated multimodal fusion, and the complementary information is captured using prediction head. A federated orchestrator performs scheduling of rounds and client sampling in which parallel client-side training is performed with preserving data locality. Then, client-level differential privacy is applied using clipped updates, noise injection, and adaptive privacy budgeting. Then, Secure aggregation aggregates model updates that reach the server. Then, momentum-based federated optimization updates global model at the server, then concludes evaluation that measures the model's effectiveness.

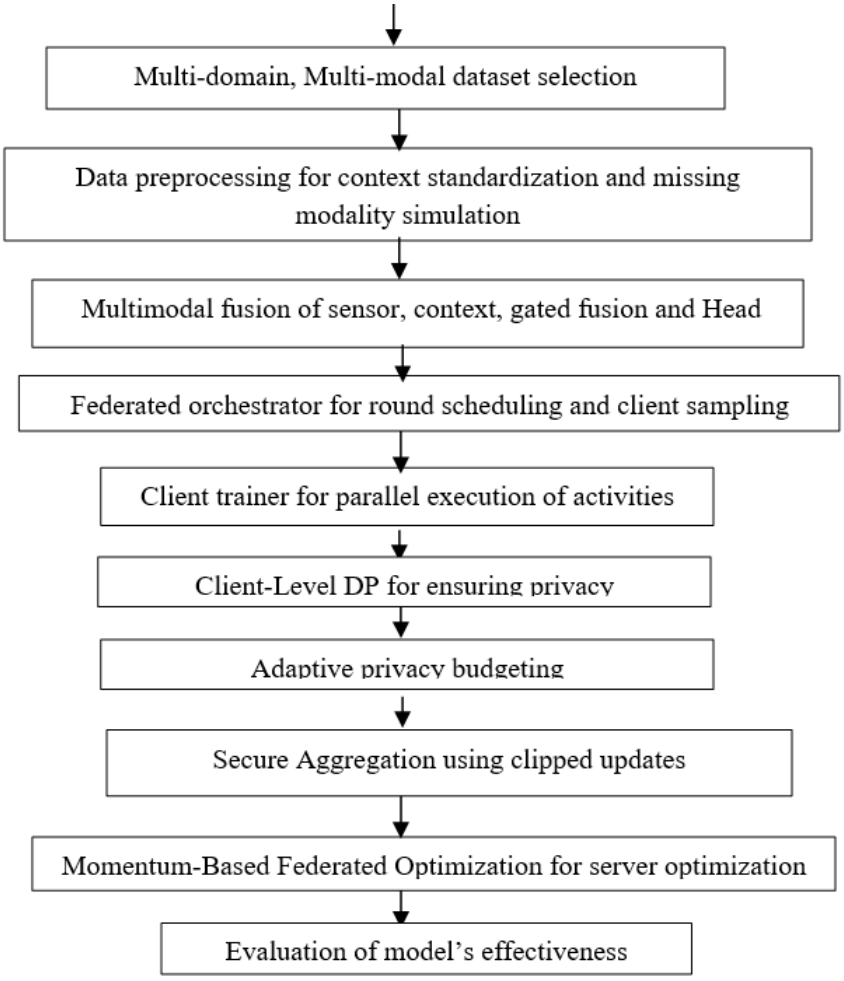

Fig.2. Flowchart of hybrid FL+DP+Core components privacy preserving approach

PS1: Pseudo Procedure Hybrid FL+DP+Core components privacy preserving approach():
Inputs: Clients $\mathcal{K} = \{1, \dots, K\}$, Rounds: R, local epochs: E, batch size: B, Global model parameters at round t: W_t, Learning rates: client η, server η_s, server momentum $\beta \in [0,1)$, DP params: total privacy budget $(\varepsilon_{\text{tot}}, \delta)$, clip norm C, noise scale schedule σ_t, Client sampling rate per round $q = \frac{|S_t|}{K}$, and Loss: $\ell(\hat{y}, y)$
Outputs: Final global model $W^{\setminus *}$, Metrics $\mathcal{M}$(Accuracy, Precision, Recall, F1, AUC,), and Privacy report: consumed (ε, δ)across rounds

Step1: Selection of multi-domain, multi-modal dataset to be denoted as

$D_k = \{(x_s^{(i)}, x_c^{(i)}, y^{(i)})\}_{i=1}^{n_k}$ (1) where x_s= sensor modality, x_c= context modality, y= label, and Total data $N = \sum_{k=1}^{K} n_k$.

Step2: Applying data preprocessing for context standardization and missing modality simulation

2.1 Context standardization is achieved using z-score and is defined as

$\tilde{x}_c = \frac{x_c - \mu_c}{\sigma_c + \epsilon}$ (2) where μ_c, σ_c: mean and standard deviation

2.2 Define Bernouli mask for missing modality simulation, which is forwarded to gated fusion and is defined as

$m_s, m_c \in \{0,1\}$

$\bar{x}_s = m_s x_s, \bar{x}_c = m_c \tilde{x}_c$ (3) where m_s, m_c are modality availability indicators

Step3: Perform multi-modal fusion with adaptive gating

3.1 Encoders embeddings are represented by

$z_s = f_s(\bar{x}_s; \theta_s), z_c = f_c(\bar{x}_c; \theta_c)$ (4)

3.2 Do gated computation by

$\alpha = \sigma(W_g[z_s; z_c; m_s; m_c] + b_g)$ (5) where $\sigma(\cdot)$is sigmoid and [;]is concatenation.

3.3 The fused representation is defined as

$z_f = \alpha \odot z_s + (1 - \alpha) \odot z_c$ (6) where $\odot$: element-wise multiplication

3.4 Predict the head using $\hat{y} = h(z_f; \theta_h)$ (7)

3.5 Loss, local objective on client k is computed by $\mathcal{L}_k(W) = \frac{1}{n_k} \sum \ell(\hat{y}, y)$ (8)

Step4: Define federate orchestrator and client sampling using

4.1 Client subnet nothing but participating clients is denoted

$S_t \subseteq \{1, \dots, K\}, | S_t | = m$ (8) where S_t: active clients at round t

4.2 Sampling probability is computed by $q = \frac{m}{K}$ where q is participation rate

Step5: Local training parallel in client

5.1 With $W_{t,0}^k = W_t, l$ocal computation for client k is computed as $W_{t,j+1}^k = W_{t,j}^k - \eta \nabla \mathcal{L}_k(W_{t,j}^k)$ (9)

5.2 Model update from E epochs is represented as $\Delta W_t^k = W_{t,J}^k - W_t$ (10)

Step6; Do Client level differential privacy using clipping and noise are computed as

6.1 Clipping norm is defined as $\Delta \bar{W}_t^k = \Delta W_t^k \cdot \min\left(1, \frac{C}{\|\Delta W_t^k\|_2}\right)$ (11)

6.2 Noise added using gaussian mechanism is defined as $\widetilde{\Delta W}_t^k = \Delta \bar{W}_t^k + \mathcal{N}(0, \sigma_t^2 C^2 I)$ (12)

Where $\|\cdot\|_2$: Euclidean norm, I: identity matrix, and $\mathcal{N}(0,\cdot)$: Gaussian distribution

Step7: Perform adaptive privacy budgeting

7.1 Allocate budget ε_t for each round using $\sum_{t=1}^{R} \varepsilon_t \leq \varepsilon_{\text{tot}}$ (13) where ε_t: privacy cost at round t

7.2 Schedule noise when budget is tight using $\sigma_t = \sigma_{\min} + \lambda\left(\frac{\varepsilon_{\text{used}}}{\varepsilon_{\text{tot}}}\right)$ (14) where λ: adaptation coefficient

7.3 Accounting privacy using $(\varepsilon, \delta) = \text{Accountant}(q, \{\sigma_t\}, \delta)$ (15)

Step8: Perform secure aggregation by updating the aggregation as $\widetilde{\Delta W}_t^{\text{sum}} = \sum_{k \in S_t} \widetilde{\Delta W}_t^k$ (16)

Step9: Perform momentum based federated optimization using

9.1 Aggregate the weights using $g_t = \sum_{k \in S_t} \frac{n_k}{\sum_{i \in S_t} n_i} \widetilde{\Delta W}_t^k$ (17)

9.2 Define server momentum using $v_t = \beta v_{t-1} + (1 - \beta) g_t$ (18)

9.3 Global model update using $W_{t+1} = W_t + \eta_s v_t$ (19)

where v_t: server velocity vector, and β: momentum coefficient

Step10: Evaluate model effectiveness using accuracy, error rate, precision and recall

Accuracy $= \frac{1}{|D_{\text{test}}|} \sum 1[\hat{y} = y]$ (20)

Error rate: Error $= 1 -$ Accuracy (21)

Precision/Recall/F1: Precision $= \frac{TP}{TP+FP}$, Recall $= \frac{TP}{TP+FN}$, $F1 = \frac{2PR}{P+R}$ (22) (23) (24)

where TP, FP, FN denote confusion matrix components

Step11: Initiate termination using $t = R$or $\| W_{t+1} - W_t \|_2 < \tau$ (or) $\varepsilon_{\text{used}} \geq \varepsilon_{\text{tot}}$ (25)

Where τ: convergence threshold

Client-side components:

Local encoders f_s, f_c , Gating weights α , Local gradient $\nabla \mathcal{L}_k$, Clipped update $\Delta \bar{W}_t^k$, and Noisy update $\widetilde{\Delta W}_t^k$

Server-side components:

Client set S_t , Aggregated gradient g_t , Momentum vector v_t , Global model W_t , and Privacy accountant (ε, δ)

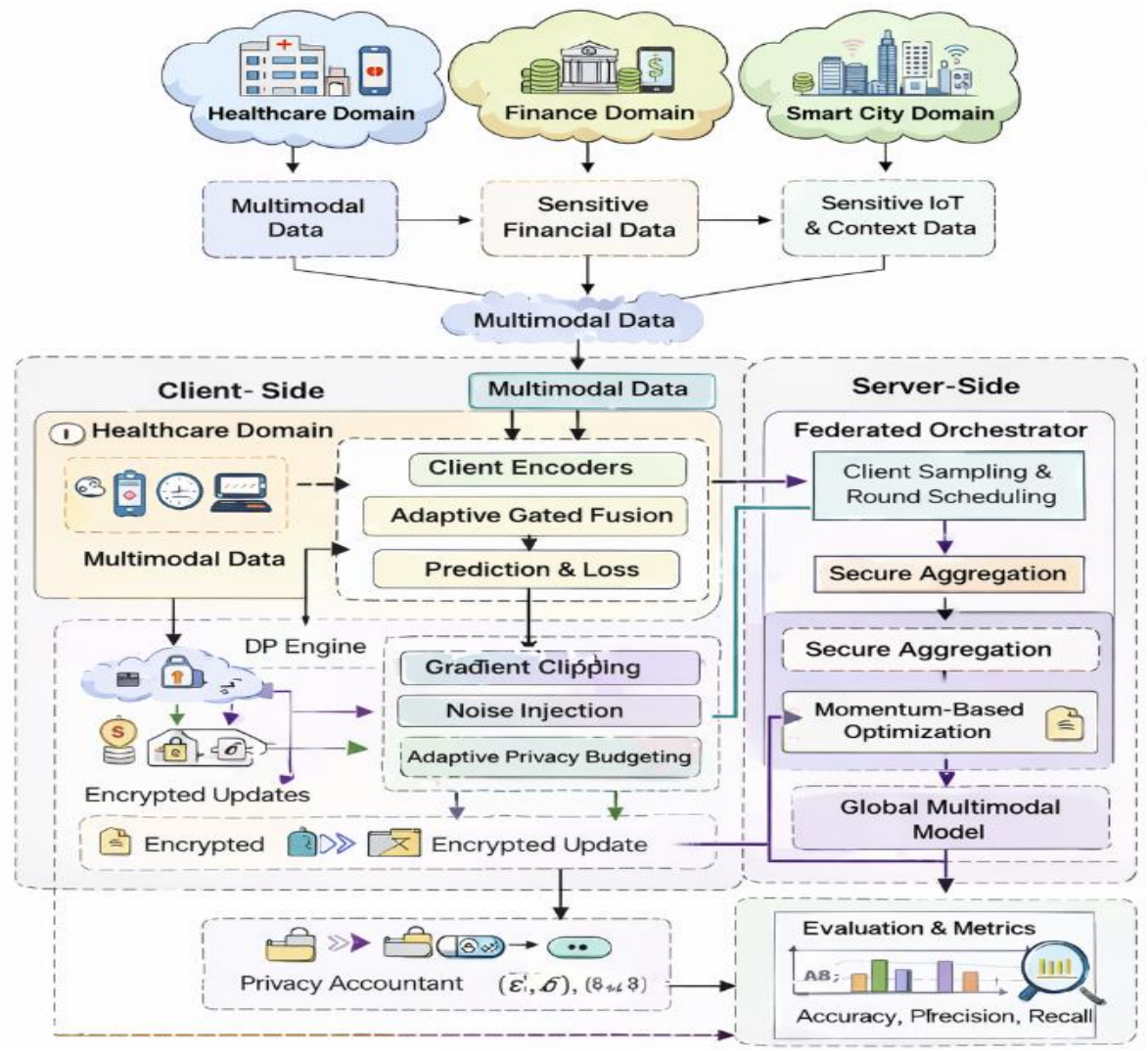

Fig.3. Architectural diagram of the proposed hybrid model for privacy preservation

Based on PS1, The hybrid privacy-preserving federated learning Differential privacy with core components addition framework, selects multi-domain, multi-modal dataset $D_k$at each client, where sensor inputs x_s, contextual inputs x_c, and labels y for distributed data space for total samples N. Then, preprocessing is applied through z-score standardization and Bernoulli-based modality masking for handling missing information, to enable robust multimodal representation learning. Feature embeddings using modality-specific encoders and an adaptive gated fusion mechanism combinedly produce a fused representation z_f with dynamic weight modalities, to compute local loss computation and make prediction. Federated orchestrator applied over a subset of active clients $S_t$per round, and made client model update using parallel local training through gradient-based optimization. Then, uses client-level differential privacy is applied using norm clipping and Gaussian noise injection to ensure privacy using adaptive privacy budgeting that regulates noise and privacy expenditures under (ε,δ). Secure aggregation combines noisy client updates, after then uses momentum-based federated optimization for the global model. The

measures accuracy, error rate, precision, recall, and F1-score are computed, which defines the effectiveness of the model, and then initiates termination based on convergence or completion of rounds.

Fig.3 demonstrates architectural diagrams of domains such as healthcare, finance, and smart cities. At client side, data of multimodal data sources is taken from sensor, clinical, and contextual areas. Then, preprocessing, feature encoding, and adaptive gated fusion are applied to form fused feature representation. Then, local model training and loss computation are performed. In mean time, dedicated differential privacy engine uses components such as gradient clipping, Gaussian noise injection, and adaptive privacy budgeting for model updates. At server-side, federated orchestrator performs client sampling and round scheduling, and secure aggregation combines updates. Then, momentum-based optimization refines global model, and privacy accountant ensures cumulative privacy expenditure under (ε, δ). Then, the evaluation of the optimized global model is performed to ensure scalability, collaboration, and regulatory-compliant privacy protection.

4. Results

In this, evaluation is considered in two aspects: dataset description and experimental setup, and comparison of the hybrid model against baseline approaches, and an ablation study to determine the effectiveness of the models.

4.1 Dataset description and experimental setup:

The dataset would be a multi-domain, multi-modal distributed kind, which is built to emulate applications such as finance, healthcare, and smart cities, where pooling of data centrally is not done due to sensitivity and regulatory constraints. The federated environment involves Kclients, where each client $k$stores a local dataset $D_k = \{(x_s^{(i)}, x_c^{(i)}, y^{(i)})\}_{i=1}^{n_k}$ with sensor modality features x_s, context modality features x_c, and a binary label y. Sensor modality $x_s \in \mathbb{R}^{d_s}$ denotes time-series/IoT measurements such as vitals, transaction streams, and traffic sensors, while context modality $x_c \in \mathbb{R}^{d_c}$represents structured metadata like demographics, device attributes, location, and environmental context. The overall data size is $N = \sum_{k=1}^{K} n_k$, and the heterogeneity by clients via domain shifts of feature distributions in order to simulate cross-organization data variation (non-IID behavior). During preprocessing, missing modality is modelled using Bernouli masks removes sensors information such as sensor failures, feature suppression, and incomplete records. To ensure stable learning, the context features are standardized using z-score normalization before training.

The experimental setup describes the hybrid model as during its processing, the federated orchestrator at each communication round t processes a subset of clients $S_t \subseteq \{1, \dots, K\}$of size $| S_t | = m$, with sampling rate $q = m/K$, and broadcasts the current global model W_t. Each selected client performs local training for Eepochs using SGD with a learning rate η, yields a model update $\Delta W_t^k = W_{t,J}^k - W_t$. The local model contains two modality-specific encoders $f_s(\cdot\,; \theta_s)$and $f_c(\cdot; \theta_c)$, whose embeddings (z_s, z_c) are fused by an adaptive gated fusion module that

computes $\alpha = \sigma\big(W_g[z_s; z_c; m_s; m_c] + b_g\big)$ and forms the fused representation $z_f = \alpha \odot z_s + (1-\alpha) \odot z_c$, then followed by a prediction head $h(\cdot;\theta_h)$. To ensure privacy, client-level DP is applied to each update by clipping to the norm C: $\Delta\bar{W}_t^k = \Delta W_t^k \cdot \min(1, C/\| \Delta W_t^k \|_2)$, and injecting Gaussian noise: $\Delta\widetilde{W}_t^k = \Delta\bar{W}_t^k + \mathcal{N}(0, \sigma_t^2 C^2 I)$. The privacy budget $\varepsilon_{\text{tot}}$is ensured using adaptive privacy budgeting, where increased noise as privacy consumption rises when $\sigma_t = \sigma_{\min} + \lambda(\varepsilon_{\text{used}}/\varepsilon_{\text{tot}})$), and privacy loss is tracked using an accountant returning (ε, δ). Updates are combined using secure aggregation, like a server observes only aggregated sums/means, and the global model is updated using momentum-based server optimization: $v_t = \beta v_{t-1} + (1-\beta)g_t$, $W_{t+1} = W_t + \eta_s v_t$, where $g_t$is the weighted average of aggregated updates. The evaluation of model efficiency is assessed in terms of accuracy, error rate, precision, recall, and F1-score, while the privacy report includes the consumed (ε, δ) and the corresponding noise schedule.

4.2 Comparison of the hybrid model against baseline approaches, and an ablation study:

In this, the centralized approach is not considered, although it produces better accuracy and performance due to a lack of privacy, and is not able to cope with larger applications. Table 1 demonstrates a comparison of the proposed system against other models with respect to measures such as Error rate, performance, and accuracy, along with scalability support and privacy guarantee. Table 2 demonstrates confusion matrix-based evaluation results, and also the ablation study comparison, followed by Fig.4 for depicting effectiveness.

Table 1 depicts that the proposed hybrid model ensures better evaluated values than other models, such as Homomorphic encryption (HE), Multi-party computation (MPC), Trusted Execution environments, Federated learning in varieties such as No DP, Fixed privacy budget, and Adaptive privacy budgets (ε).

Table 1. Comparison of the proposed approach against other models considered

Approach	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Error Rate (%)	Privacy Guarantee	Scalability
Homomorphic Encryption (HE)	92.4	91.8	93.1	92.4	7.6	Strongly supporting	Low
Secure Multi-Party Computation (MPC)	93.1	92.5	94.0	93.2	6.9	Strongly supporting	Low
Trusted Execution Environment (TEE)	95.0	94.6	95.3	94.9	5.0	Machine based	Moderate
Federated	98.4	98.2	98.6	98.4	1.6	Partial	Highly

Learning (FL – No DP)						support	support
FL + Differential Privacy (Fixed ε)	96.8	97.1	96.5	96.8	3.2	Support	Highly support
Proposed Hybrid FL–DP (Adaptive ε)	99.1	99.0	99.2	99.1	0.9	Support	Highly support

Table 2 demonstrates results derived from the confusion matrix by assuming a scenario of test samples 10k, positive class prevalence 50%, measures computed, and values evaluated over 5 FL runs. The proposed hybrid model is observed to be better and effective in terms of computed measures such as error rate, accuracy, and performance metrics. The visual comparison of Table 2 is transformed into Fig.4.

Table 2. Derived results of confusion matrix as ablation study

Model	TP	FP	TN	FN	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Error Rate (%)
FL Only (No DP)	4,930	90	4,910	70	98.4	98.2	98.6	98.4	1.6
FL + Fixed ε DP	4,825	145	4,855	175	96.8	97.1	96.5	96.8	3.2
FL + DP (No Cross-Modal Interaction)	4,890	120	4,880	110	97.9	97.6	98.1	97.8	2.1
FL + DP (No Weighted Aggregation)	4,910	100	4,900	90	98.2	98.0	98.3	98.1	1.8
Proposed Hybrid FL–DP	4,955	50	4,945	45	99.1	99.0	99.2	99.1	0.9

Fig.4 demonstrates proposed model ensures better accuracy, precision, recall, F2-score, and less error rte than other methods considered in the comparison.

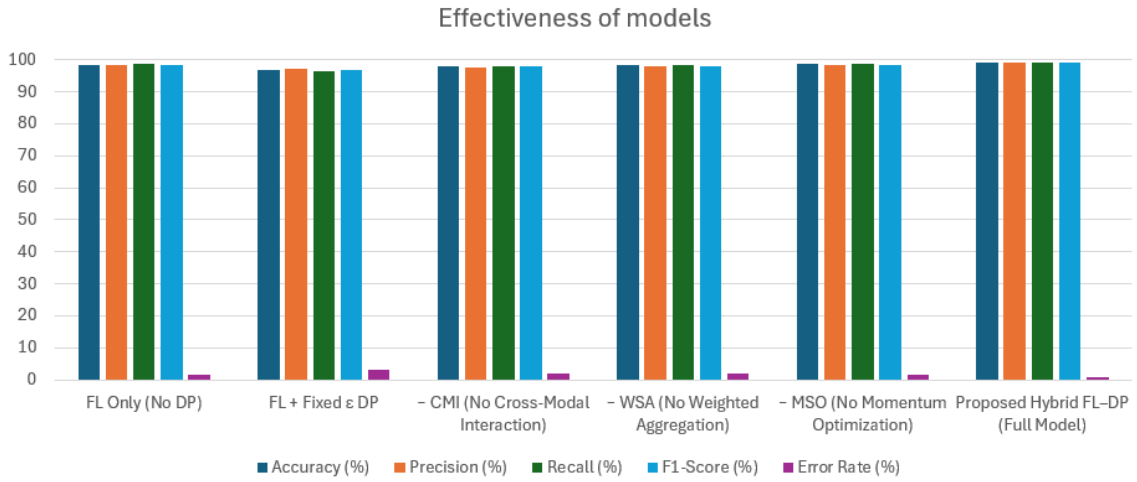

Fig.4. Effectiveness of the models for privacy preserving

5. Conclusion

The proposed model is a hybrid Federated Learning–Differential Privacy (FL–DP) with core optimization components framework designed for addressing high-utility, privacy-preserving learning in distributed sensitive environments like smart cities, healthcare, and finance. The proposed model applies decentralization across multiple clients without exposing raw data, mitigates issues with centralized mechanism such as data leakage, unauthorized access, and non-compliance regulations. The combination of multimodal fusion uses sensor attributes and contextual features, and integrating of client level differential privacy with adaptive privacy budget ensures strong protection against variety of attacks but not affecting the performance. The momentum based federated optimization and secure aggregation enhances collaborative learning, convergence stability, and scalability. Compared with considered models such as Muti-party computation, centralized system, Homomorphic encryption, fixed differential based federated learning, the proposed hybrid model ensures balance in data utility, privacy enforcement, scalable, and compliance regulatory solution for distributed environment privacy preserving. The future research possible towards adaptive multimodal fusion, development of domain aware privacy methods, and easy deployments for heterogeneous large scale environments. In the future, the development of domain-aware privacy mechanisms for patient monitoring, healthcare diagnostics of healthcare, and smart city analytics, where data sensitivity and regulatory constraints are significant.

REFERENCES

[1] Feng, Y., Guo, Y., Hou, Y. et al. (2025). A survey of security threats in federated learning. *Complex Intell. Syst.* **11**, 165 (2025). https://doi.org/10.1007/s40747-024-01664-0.

[2] Guiping Zheng, Bei Gong, et al. (2025), AWE-DPFL: Adaptive weighting and dynamic privacy budget federated learning for heterogeneous data in IoT, Computers and Electrical

Engineering, Volume 123, Part A, April 2025, https://doi.org/10.1016/j.compeleceng.2025.110070.

[3] Gosselin, R., Vieu, L., et al. (2022). Privacy and Security in Federated Learning: A Survey. Applied Sciences, 12(19), 9901. https://doi.org/10.3390/app12199901.

[4] Guembe, B. (2024). Privacy issues, attacks, countermeasures, and open problems in federated learning. Applied Artificial Intelligence, Volume 38, 2024, Issue 1, https://doi.org/10.1080/08839514.2024.2410504.

[5] Ioannis Makris, Aikaterini Karampasi, et al.(2025), A comprehensive survey of Federated Intrusion Detection Systems: Techniques, challenges and solutions, Computer Science Review, Volume 56, May 2025, https://doi.org/10.1016/j.cosrev.2024.100717.

[6] Shanwei Chen, Xiuzhi Qi (2025), Entropy-adaptive differential privacy federated learning for student performance prediction and privacy protection: a case study in Python programming, Front. Artif. Intell., September 2025, Sec. Machine Learning and Artificial Intelligence, Volume 8 - 2025, https://doi.org/10.3389/frai.2025.1653437.

[7] YANG ZHANG , SHIGONG LONG, et al. (2025), DP-FedCMRS: Privacy-Preserving Federated Learning Algorithm to Solve Heterogeneous Data, IEEE Access, Multidisciplinary, DOI: 10.1109/ACCESS.2025.3546473.

[8] Gong, C., Zhang, X., et al. (2025). Federated Learning for Heterogeneous Data Integration and Privacy Protection. Preprints. https://doi.org/10.20944/preprints202503.2211.v1.

[9] Cong Shen, Wei Zhang, et al. (2024), An Efficient and Secure Privacy-Preserving Federated Learning Framework Based on Multiplicative Double Privacy Masking, Computers, Materials & Continua, https://doi.org/10.32604/cmc.2024.054434.

[10] Shen, J., Zhao, Y., et al. (2024). Secure and Flexible Privacy-Preserving Federated Learning Based on Multi-Key Fully Homomorphic Encryption. Electronics, 13(22), https://doi.org/10.3390/electronics13224478.

[11] Abdulrahman Alamer (2024), A privacy-preserving federated learning with a secure collaborative for malware detection models using Internet of Things resources, Internet of Things, Volume 25, https://doi.org/10.1016/j.iot.2023.101015.

[12] Oshamah Ibrahim Khalaf, Ashokkumar S.R, et al. (2024), Federated learning with hybrid differential privacy for secure and reliable cross-IoT platform knowledge sharing, Security and privacy, Wiley, https://doi.org/10.1002/spy2.374.

[13] Wang, B., Li, H., et al. (2023). An Efficient Differential Privacy-Based Method for Location Privacy Protection in Location-Based Services. Sensors, 23(11), 5219. https://doi.org/10.3390/s23115219.

[14] Tayyeh, H. K., & AL-Jumaili, A. S. A. (2024). Balancing Privacy and Performance: A Differential Privacy Approach in Federated Learning. Computers, 13(11), 277. https://doi.org/10.3390/computers13110277.

[15] WANGXIN, LI JIAQIAN, et al. (2024), A Survey of Differential Privacy Techniques for Federated Learning, IEEE Access, Multidisciplinary, 10.1109/ACCESS.2024.3523909.

[16] Ni, Z., & Zhou, Q. (2025). Differential Privacy in Federated Learning: An Evolutionary Game Analysis. Applied Sciences, 15(6), 2914. https://doi.org/10.3390/app15062914.

[17] Guo, S., Yang, J., et al.(2024), Federated learning with differential privacy via fast Fourier transform for tighter-efficient combining. Sci Rep 14, 26770 (2024). https://doi.org/10.1038/s41598-024-77428-0.

[18] MARIA IQBAL, ASADULLAH TARIQ (2023), FL-ODP: An Optimized Differential Privacy
Enabled Privacy Preserving Federated Learning, IEEE Access, Multidisciplinary, 10.1109/ACCESS.2023.3325396.

[19] Li, K., Lohachab, A., et al.(2025), Privacy preservation in blockchain-based healthcare data sharing: A systematic review. Peer-to-Peer Netw. Appl. 18, 302 (2025). https://doi.org/10.1007/s12083-025-02148-9

[20] Nazish Khalid, Adnan Qayyum, et al. (2023), Privacy-preserving artificial intelligence in healthcare: Techniques and applications, Computers in Biology and Medicine, Volume 158, https://doi.org/10.1016/j.compbiomed.2023.106848.

[21] Adnan, A., Kausar, F., et al. (2025), Data Collaboration. Symmetry, 17(7), 1139. https://doi.org/10.3390/sym17071139.

[22] Barbaria, S., Jemai, A., et al. (2025). Advancing Compliance with HIPAA and GDPR in Healthcare: A Blockchain-Based Strategy for Secure Data Exchange in Clinical Research Involving Private Health Information. Healthcare, 13(20), 2594. https://doi.org/10.3390/healthcare13202594.

[23] Siqin, Z., Xiaohong, W., et al.(2025), Auction-based incentive mechanism with personalized privacy protection in federated learning. Mach Learn 114, 199 (2025). https://doi.org/10.1007/s10994-025-06836-8.

[24] Dey N.S., Sangaraju H.K.R.(2024), A particle swarm optimization inspired global and local stability driven predictive load balancing strategy, Indonesian Journal of Electrical Engineering and Computer Science, Volume 35, Issue 3,10.11591/ijeecs.v35.i3.pp1688-1701.

[25] Dey N.S., Sangaraju H.K.R.(2023), Hybrid Load Balancing Strategy for Cloud Data Centers with Novel Performance Evaluation Strategy, International Journal of Intelligent Systems and Applications in Engineering, Volume 11, Issue 3, Pages 883 - 908, https://ijisae.org/ index.php/IJISAE/article/view/3345.

[26] Anil Kumar Allamudi and Hrushikesava raju.S (2025), Hybrid Machine Learning for Fraud Detection: Balancing Accuracy and Security in Digital Transactions, International Journal of Safety and Security Engineering, Volume 15, Issue 2, Pages 331 - 337, February 2025, 10.18280/ijsse.150214.

[27] Raju, S. Hrushikesava; Adinarayna, S., et al.(2024), An Optimized Approach for Defect Detection in the Flyovers Using Faster R-CNN, LSTM, and Transfer Learning, MMEP, 2025, Vol 12, Issue 8, 10.18280/mmep.120828.