**International Journal of Applied Mathematics**
**Volume 38 No. 7s, 2025**
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

# TRUST AND HETEROGENEITY AWARE DECENTRALIZED FEDERATED-LEARNING FRAMEWORK FOR PRIVACY PRESERVED HEALTHCARE CLASSIFICATION

**Neha Kudu, Dr. Manuj Joshi,**

Research Scholar, Pacific Academy of Higher Education and Research University, Udaipur, Rajasthan, India. neha.kudu@vit.edu.in

Associate Professor, Faculty of Engineering, Pacific Academy of Higher Education and Research University, Udaipur, Rajasthan, lndia. manujjoshi@gmail.com

## Abstract

Healthcare centers are becoming essential hubs for processing vast amounts of data used in disease diagnosis. Despite this, practical implementations face issues, like data privacy concerns, insecure storage, and limited sharing efficiency. To tackle such complexity, Trust Heterogeneity aware-based Fractional Football Optimization Algorithm enabled Deep High-order Attention Neural Network (TrustHet aware-based FFboA_DHA-Net) for classifying privacy preserved healthcare system, is proposed. Initially, Local training is conducted on every node using local data, followed by server-side model aggregation, where nodes download global model, update it with local models. In training model, input image is pre-processed, then lesions are segmented, and feature are extracted. Using Deep High-order Attention Neural Network (DHA-Net) health care classification is done, DHA-Net is trained by FFbOA. FFbOA is an integration of Football Optimization Algorithm (FbOA) with Fractional Calculus (FC). Here, Heterogeneity-aware FL allows devices with diverse data to contribute effectively to a shared model. A decentralized aggregation strategy is used, trust establishment mechanism between server and nodes is designed by considering trust factors. Aggregation is enhanced through harmonic analysis, and both local updates and server-side aggregation are extracted using an averaging method. Additionally, optimal results attained are 96.981% of F1-score, 0.020 of Loss function, 97.817% of Mean Average Precision (MAP), 0.111 of Normalized Mean Square Error (MSE), and 0.333 of Normalized Root Mean Squared Error (RMSE).

***Keywords:*** Blockchain, Deep High-order Attention Neural Network, Federated Learning, Football Optimization Algorithm, Heterogeneity.

## 1. Introduction

In current era of digital computing, vast and continuously growing volumes of data are being generated across numerous domains. This exponential increase in data volume and diversity is largely driven by the widespread application of computing technologies that are facilitated by the affordability of devices, storage solutions, and reliable network connectivity. Much of this large-scale data includes highly personal and sensitive information, such as gender, postal codes, medical conditions, caste, shopping preferences, and religious affiliations. Often, this

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

information is stored in public or semi-public databases and may be shared with third-party analysts to extract meaningful insights and discover hidden patterns that support data-driven decision-making [1]. Analyzing such data offers considerable value to various sectors, including healthcare, finance, cybersecurity, commerce, and transportation. However, inclusion of sensitive and private information raises privacy concerns. Privacy is a fundamental right of human in Universal Declaration of Human Rights, yet defining its scope remains complex due to its relevance across multiple domains. Privacy is commonly categorized into four areas: informational, communication, and territorial [2]. Medical images and related data often fall under these privacy-sensitive categories which limits the availability and freshness of accessible datasets. A promising privacy-preserving solution is to keep sensitive data stored locally either on personal devices or secure data centers while training models locally and transmitting only non-sensitive model parameters to centralized servers for aggregation [3].

FL offers an effective solution to alleviate communication burdens in distributed learning environments. In this framework, selected active devices perform multiple training iterations locally using their data. Once local training is complete, these devices synchronously send only the model parameters to a server where parameters are gathered to update global model. These server-client structures allow individual devices to maintain data privacy while still contributing to the learning process. The server integrates the local updates to improve the shared model and then redistributes the refined global model back to the devices for further training [4]. Conventional privacy-preserving approaches, like data summarization or noise addition are often inadequate in clinical environment, appropriate access to accurate data is crucial for treatment. In order to overcome these limitations, researchers focused to blockchain technology for improved data privacy and security. Blockchain functions as an immutable and decentralized ledger maintained by a peer-to-peer network, eliminating need for centralized control. Data is kept in blocks that are connected chronologically and secured through cryptographic hash functions. Each block contains a unique hash and any modification in the data disrupts this hash chain by making it tampering easily detectable [2]. The security and transparency of blockchain make it highly suitable for protecting sensitive information beyond financial transactions. Its integration with FL enhances both privacy and trust, particularly in fields, like healthcare where safeguarding patient data is essential. This combination ensures secure and distributed model training without compromising the confidentiality of users' medical information [5].

Rapid progress in medical technology has made analysis of medical images an essential component of modern healthcare. Techniques, such as pathology imaging, Computed Tomography (CT), Magnetic Resonance Imaging (MRI), and ultrasound, enable physicians to detect diseases with greater precision. It helps to evaluate treatment responses and predict potential health risks [6]. The field of medical imaging involves a diverse set of stakeholders including patients, hospitals, research institutions, developers of algorithms, diagnostic equipment manufacturers, industry players, and regulatory bodies [7]. Based on sensitive nature of medical data, stringent ethical, regulatory, and moral guidelines govern its sharing to protect patient privacy. These restrictions can impede the development of robust algorithms

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

and limit their broad application. Medical images often comprise confidential information, such as medical history, physiological behavior, and diagnostic outcome which makes data sharing particularly complex. Risks of privacy breaches during data transmission, storage, or analysis can result in serious violations or identity theft. As collaborative efforts increase cross-institutional data sharing and Artificial Intelligence (AI) model training for safeguarding patient privacy becomes an urgent technical, legal, and ethical challenge [6]. However, these modifications can reduce data utility and lead to trade-off among performance and privacy. To address these issues, privacy-preserving Deep Learning (DL) methods have been developed to separate sensitive information from the original data, with additional communication and computational costs [8]. Approaches, such as differential privacy, homomorphic encryption, and secure multi-party computation are employed to enhance privacy and security in DL models thereby facilitating safer medical data usage and analysis [9].

Main intention is to develop the novel approach named TrustHet aware-based FFboA_DHA-Net. At every node local training is carried out based on local data. Following that, server is updated and aggregation of model is performed on server. At nodes, global model is downloaded and update is performed using downloaded global model and local model. Furthermore, iterative process is performed at every epoch. In training model, input image undergoes a pre-processing phase, where Midpoint filter is used. Afterward, lesion is segmented using TBConvL-Net, and then the features are extracted. The classification of health care system is done by utilizing DHA-Net, which is fine-tuned using FFbOA. Moreover, it is an integration of FbOA with the FC concept. Here, Heterogeneity-aware FL supports different devices with varying data to work together for improving a shared model while considering these differences. Also, a decentralized model aggregation strategy is adopted; hence, devices communicate with each other to transmit model parameters. Trust should be an integral part of the decision-making process and the trust establishment mechanism between the server and nodes will be designed by considering certain trust factors. Here, the aggregation is performed using the harmonic concept. At last, the aggregation and local updation at the server are modified using Average method.

- **Proposed TrustHet aware-based FFboA_DHA-Net for Privacy-Preserved Healthcare Classification in Blockchain:** Privacy-preserved healthcare data classification enables secure analysis of medical data without compromising patient confidentiality. Here, an efficient model named TrustHet aware-based FFboA_DHA-Net is developed for classifying privacy preserved healthcare system. Furthermore, a heterogeneity-aware decentralized system incorporating various trust factors is adopted to ensure trust in privacy preservation.

Layout of remaining sections is enumerated as follows: Section 2 involves literature survey of existing approaches on Classification of Privacy Preserved Healthcare system; Section 3 includes methodology and architecture of TrustHet aware-based FFboA_DHA-Net; Section 4 provides evaluation results of TrustHet aware-based FFboA_DHA-Net; Section 5 concludes the work.

## 2. Motivation

Received: August 07, 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Privacy-preserved healthcare classification in blockchain with trust heterogeneity involves securely analyzing and classifying medical data from distributed sources while considering the differing trust levels among contributors. Traditional models often struggle to balance data privacy with high performance, especially in decentralized systems. They typically ignore variations in trust across data sources and leading to less dependable results. As blockchain becomes more prominent for secure data management, there is a need for models that incorporate trust and privacy effectively. Hence, there is a need to develop a new model for classification of privacy preserved healthcare system in blockchain with trust heterogeneity.

### 2.1 Literature Survey

A. lakhan, *et al.* [10] presented FL-BETS for privacy preserved health care classification. It provided security in patient privacy and helped to prevent fraudulent activities; however, its complex design and high computational demands resulted in slower performance and increased resource consumption. G. C. Amaizu, *et al.* [11] introduced FedViTBloc for effective classification of healthcare images. Although this method significantly improved security and privacy in medical image analysis while ensuring strong performance across distributed systems, it faced drawback, like increased latency and communication load due to the combined use of FL and blockchain. H. Malik, *et al.* [12] developed CapsNet with IELMs for privacy preserved health care classification. Even though the model offered enhanced diagnostic accuracy within a secure and decentralized framework that preserved patient privacy, the integration of complex learning models and blockchain led to high computational demands which affect scalability in low-resource environments. H. Malik, *et al.* [13] introduced DMFL_Net for COVID-19 detection by using FL. It possessed enhanced detection accuracy in varied dataset, ensuring privacy protection. Nevertheless, it faced issues with communication costs and slower model convergence caused by varied data distributions.

R. Myrzashova, *et al.* [14] presented Modified ResNet for decentralized FL. Even though the model minimized reliance on centralized computing, improved resource efficiency and reduced computational expenses, it could not incorporate various medical images and genetic information for efficient disease analysis while maintaining security and privacy. F. Hu, *et al.* [15] developed Convolutional Neural Network-based Federated Learning (FL-CNN-HMChain) for privacy preservation in FL. This strategy achieved privacy protection in healthcare data collaboration by ensuring the security of sensitive information and reliable data sharing and analysis. However, it demanded frequent updates and synchronization among numerous nodes and resulting in increased computational and bandwidth expenses. N. Li, *et al.* [16] introduced Federated Distillation (FD) method with blockchain In Remote Medical System (FedRMD) for privacy preservation using Block chain. It addressed system downtime caused by server failures and enhanced resilience of remote medical system. However, the model was unable to adapt the reputation threshold size that limiting its flexibility and hindering effective cross-chain data sharing. Z. F. Zhu, *et al.* [17] designed Contribution evaluation method for privacy preservation in healthcare data. This approach ensured that participating clients received fair rewards proportional to their contributions and effectively

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

discouraged free-riding. However, it lacked dynamic adaptive mechanisms to modify security protocols and evaluation methods in response to evolving practical threats.

### 2.2 Challenges

Challenges faced by conventional approaches classification of privacy preserved healthcare system are enumerated beneath.

- The FL BETS framework introduced in [10] addressed privacy and security concerns while minimizing resource consumption. However, it lacked support for learning across distributed medical facilities and did not increase fairness in classification of healthcare images.
- The FedViTBloc method presented in [11] aimed to improve system trustworthiness but struggled with challenges related to data diversity and scalability that limiting the creation of globally robust diagnostic models.
- In [12], a combination of CapsNet and IELMs achieved high accuracy; however, its effectiveness in healthcare data identification was hindered by the absence of optimized deep learning techniques.
- DMFL_Net, described in [13], ensured data confidentiality and security during transfers between hospitals but failed to reduce computational complexity and protect user privacy adequately.
- Recently, the adoption of ML-based dynamic Internet of Medical Things (IoMT) systems integrating several technologies has increased for digital healthcare. Nonetheless, addressing data fraud in distributed IoMT environments remains a significant challenge in healthcare applications. Hence, developing a new model to ensure secure preservation of healthcare data is necessary.

## 3. Proposed Trust Heterogeneity aware based Fractional Football Optimization Algorithm for classification of privacy preserved healthcare system in Blockchain

Classifying healthcare system within blockchain presents difficulties in safeguarding patient privacy while handling diverse trust levels across multiple data sources. Moreover, achieving a balance between strong privacy measures and maintaining efficient and accurate model performance remains a significant challenge for many existing approaches. To tackle these challenges, a novel approach is designed for classification of privacy preserved healthcare system in blockchain named TrustHet aware-based FFboA_DHA-Net. Here, servers and nodes are the entities involved in Federated Learning. Local training is carried out at each node based on local data. Following that, server is updated and aggregation of model is performed on server. In the training model, input image undergoes pre-processing phase, where Midpoint filter is used. Afterward, the lesion is segmented using the TBConvL-Net, and the Learned Invariant Feature Transform (LIFT), and Statistical Features are extracted. Health care classification is done using DHA-Net, where parameters of DHA-Net is trained by FFbOA, which is the integration of FbOA with the FC concept. Here, Heterogeneity-aware Federated learning supports different devices with varying data to work together for improving a shared model while considering these differences. Also, a decentralized model aggregation strategy is adopted; hence, devices interconnect with each other to transmit model parameters. Trust

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

should be an integral part of the decision-making process and the trust establishment mechanism between the server and nodes is designed by considering certain trust factors, like Direct, Indirect, Attestation Trust, Mediation trust, Confidence Factor, Conversational Trust, and Bayesian beta method. Here, the aggregation is performed using the harmonic concept. Finally, local updation and accumulation at server are adapted using Average method. Additionally, system model for TrustHet aware-based FFboA_DHA-Net for classifying privacy-preserved healthcare system in blockchain is portrayed in figure 1.

Received: August 07, 2025 

**International Journal of Applied Mathematics**
**Volume 38 No. 7s, 2025**
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

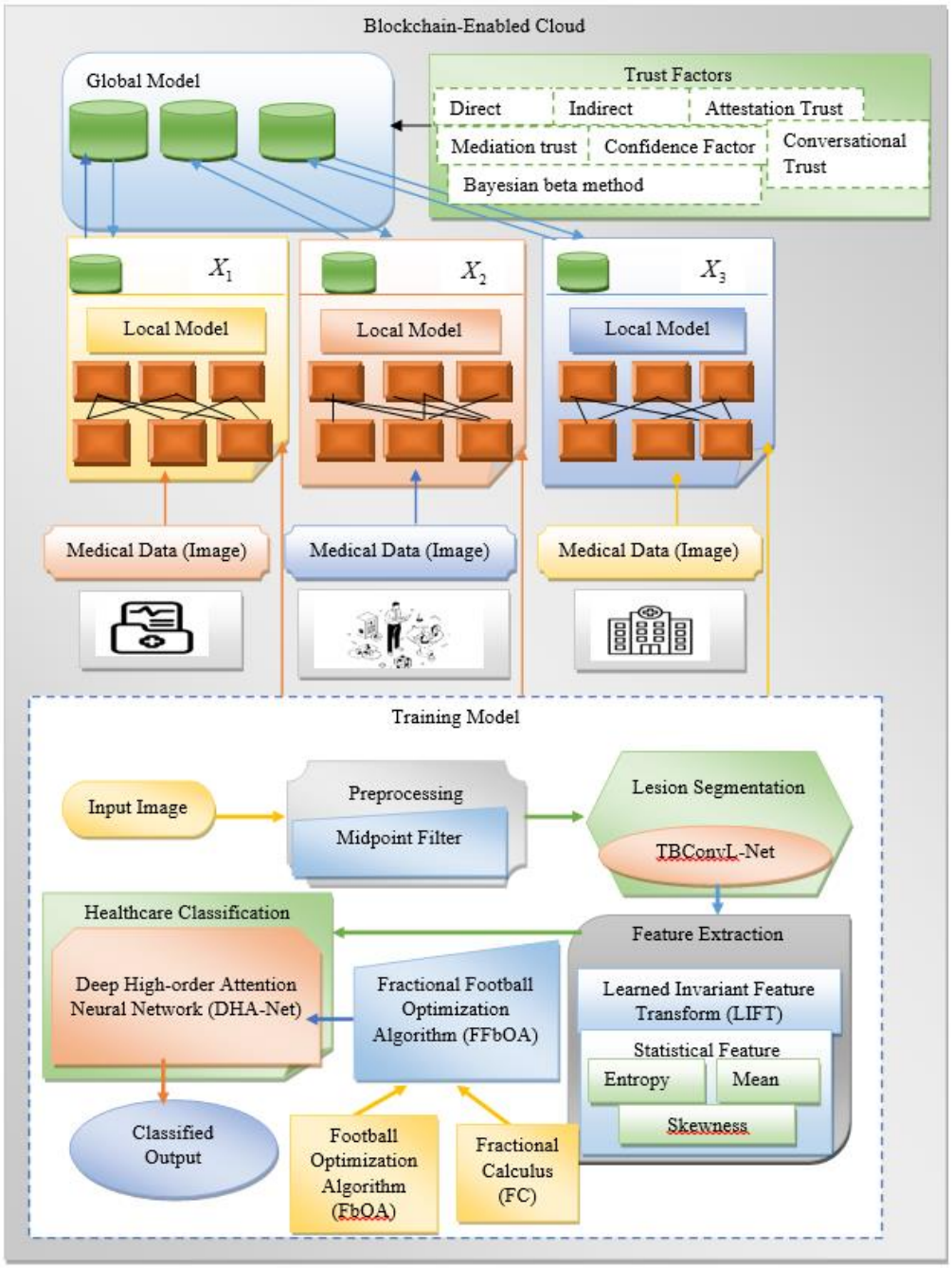



**Figure 1.** Model of TrustHet aware-based FFboA_DHA-Net for classifying privacy preserved healthcare system in blockchain

### 3.1 Local training based on Local data

In federated learning, each client device individually trains a global model using its private dataset. The sensitive data that is available on the device maintains security and privacy. Once local training is completed over several epochs, only updated model parameters are sent to a central server. Then server combines these updates from multiple clients to refine global model. This cycle continues repeatedly and allows collective model improvement without exchanging raw data.

Received: August 07, 2025

International Journal of Applied Mathematics
Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

### 3.1.1 Training at every local node

Training is achieved independently on each local node using medical Image. Here, medical image is trained in each local node, at time $f$ ,

### 3.1.2 Training Model

In training model, Midpoint filter is used to pre-process input image. Afterward, lesion is segmented using TBConvL-Net. In feature extraction phase, features like LIFT feature, and statistical features are extracted. Statistical feature includes mean, entropy and skewness. After that, classification is done using DHA-Net, where parameters of DHA-Net are trained by FFbOA, which is designed by merging FbOA with FC concept. Structure of training model is displayed in figure 2.

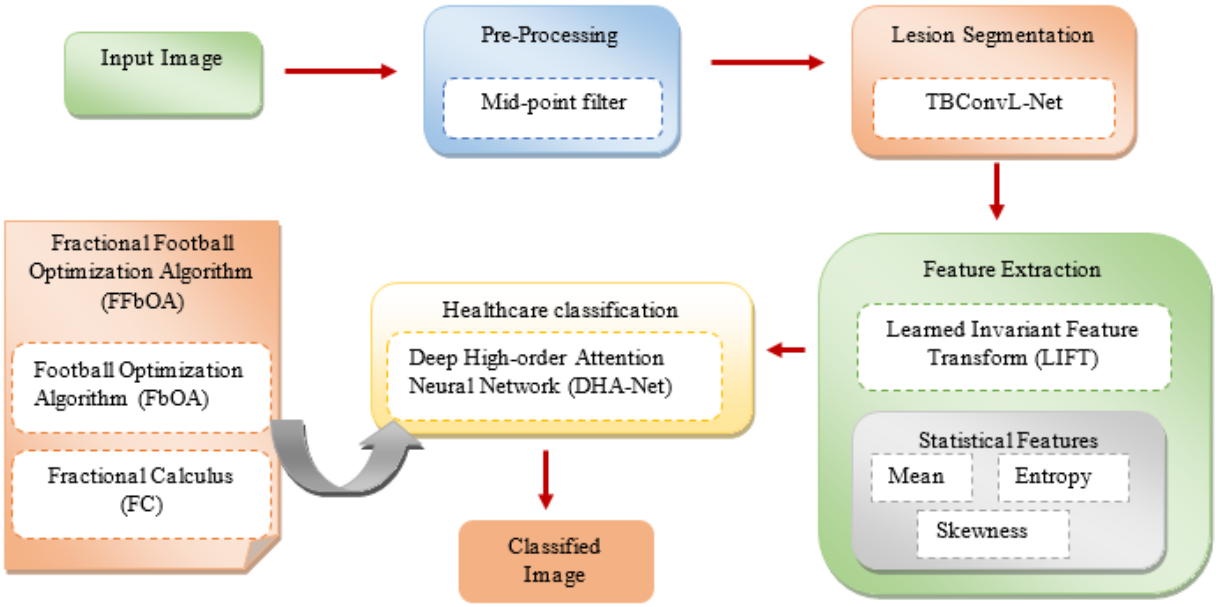



**Figure 2.** Structure of the Training Model

**a) Image acquisition from Indian Diabetic Retinopathy Image Dataset**

The Indian Diabetic Retinopathy Image Dataset (IDRiD) dataset [18] contains retinal images from the Indian population and is marked at the pixel level with typical diabetic retinopathy lesions and normal retinal structures. Here, the IDRiD dataset is expressed as,

$$J = \left\{ J_1, J_2, ..., J_q, ..., J_e \right\} \quad (1)$$

where dataset is expressed as $J$ , with overall count of image samples are denoted as $J_e$ , and the randomly selected sample image is indicated as $J_q$ .

**b) Image pre-processing by Midpoint filter**

Image pre-processing is an enhancement of retinal images by improving quality, removing noise, and standardizing input for accurate analysis. Here, input image $J_q$ is pre-processed

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

using midpoint filter. This filter can effectively reduce noise while preserving image edges better than simple averaging filters.

Midpoint filtering [19] is a nonlinear technique that reduces noise by moving a window across the image and sorting the pixel values within it. The filter output at each position is calculated as average of the largest and smallest values in window. Then, obtained pre-processed image is denoted as $I_q$.

**c) Lesion segmentation using TBConvL-Net**

Lesion segmentation is a detection and outlining of irregular areas in medical images to aid in precise evaluation and diagnosis. Here, pre-processed image $I_q$ is allowed for lesion area segmentation using TBConvL-Net. It has the ability to capture both spatial and temporal features with enhanced accuracy.

TBConvL-Net [20] is a DL model that integrates convolutional operations with temporal dynamics. This fusion allows the network to better grasp both spatial features and contextual features which leads to enhanced segmentation performance. This architecture comprises several key components, including an encoder-decoder block, BConvLSTM, and a transformer block.

The encoder-decoder block includes four stages, each with dual convolutional layers followed by max pooling and ReLU. Where filter counts double at each stage to capture high-level semantic features. Early and current features are fused through densely connected convolutions and enhancing representation while mitigating gradient vanishing or exploding issues. It is given as,

$$(I_q)_{out} = \square\,(o^{3\times3}(o^{3\times3}(Q_3))) \qquad (2)$$

Where $I_q$ indicates pre-processed image, by applying dual consecutive operations $o^{3\times3}$ is the attained resultant is represented as $(I_q)_{out}$.

The Bidirectional LSTM captures contextual dependencies in both forward and backward directions, thereby improving network's capacity to learn intricate data patterns. Swin Transformers adopt a hierarchical structure to process non-overlapping local image patches and enabling the extraction of multi-scale features. This block incorporates key components such as the output gate, input gate, memory cell, and forget gate. Additionally, output from Second Swin Transformer Block (STB) is represented as,

$$\varphi_{out} = \Im\square\ MLP(\square_{l}(\Im_3)) \qquad (3)$$

Where Multilayer Perceptron is indicated as $MLP$, resultant of STB is represented as $\varphi_{out}$, layer norm is signified as $\square_{l}$.

Then, the image obtained from lesion segmented phase is represented as $M_q$.

**d) Feature extraction from Lesion segmented image**

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Feature extraction is transformation of a raw image into useful and descriptive features that can be utilized for classification. Here features, like statistical features and LIFT feature are extracted from the lesion segmented image $M_q$.

***i) LIFT feature***

The segmented image $M_q$ is applied with LIFT to obtain a texture image feature. LIFT [21] It consists of three main components, such as a detector, an orientation estimator, and a descriptor. This approach learns features that are obtained from training data and enabling extraction of texture patches that can be effectively matched across various images.

Then, the output LIFT textural feature is indicated as $O_q$.

***ii) Statistical feature***

The obtained textural feature $O_q$ is applied with the statistical feature [22], like mean, entropy and skewness. Then, the features obtained after applying mean is indicated as $R_{me}$, features obtained from entropy is implied as $R_{en}$, and features obtained from skewness is indicated as $R_{sk}$. Then, the attained feature vectors are expressed as,

$$R_q = \{R_{me}, R_{en}, R_{sk}\} \tag{4}$$

Thus, the obtained feature from feature extraction phase is represented as $R_q$.

**e) Health Care Classification using FFboA_DHA-Net**

Classification is an alignment of medical information based on particular categories to support diagnosis, treatment planning, and patient care. Here, the extracted feature $R_q$ is subjected to DHA-Net to perform health care classification.

***i) DHA-Net***

DHA-Net [23] extends the ResNet-18 framework by incorporating EAM attention modules following each residual block to refine channel attention. Final fully connected layer is added beneath high-order pooling layer to extract intricate statistical features thereby enhancing the classification performance. DHA-Net improves healthcare data classification by combining dense attention with hierarchical feature learning and allowing accurate recognition of complex patterns. Its design maintains essential medical information while delivering reliable and high-performance classification results.

Then, the obtained classified image is denoted as $Y_q$. Moreover, the weight of DHA-Net is trained using FFbOA.

***ii) Tuning of DHA-Net using FFbOA***

DHA-Net is fine-tuned using FFbOA, which is an integration of FbOA with FC. Here, FbOA [24] is an optimization technique inspired by the tactics and movements of football players to effectively tackle challenging problems. Moreover, FC [25] is the extension of derivatives and

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

integrals to arbitrary, non-integer orders within mathematical analysis. Thus, this combination improves optimization performance by utilizing fractional-order properties to achieve faster convergence and more precise results.

**-Fitness evaluation**

Fitness evaluation measures a model's ability to accurately classify important features and is typically quantified using a predefined objective.

$$fn = \frac{1}{e}\sum_{q=1}^{e}\left[ Y_q^{target} - Y_q \right]^2 \tag{5}$$

where the overall sample is denoted as $e$, targeted classified output is implied as $Y_q^{target}$, and healthcare classified output is indicated as $Y_q$.

FFbOA is designed by integrating FbOA with FC. The standard expression of FbOA is given as,

$$T\left(Z\left(l+1\right)\right) = F_u + w_g.T\left(Z\left(l\right)\right) + Y.\sin\left(\frac{\pi}{iter}\right) - T\left(Z\left(l\right)\right) \tag{6}$$

By applying FC [25], the updated solution of FFbOA is given as,

$$T\left(Z\left(l+1\right)\right) = T\left(Z\left(l\right)\right)\left(\Phi + w_g - 1\right) + \frac{1}{2}\Phi.T\left(Z\left(l-1\right)\right) + \frac{1}{6}(1-\Phi)T\left(Z\left(l-2\right)\right) + \frac{1}{24}\Phi(1-\Phi)(2-\Phi)T\left(Z\left(l-3\right)\right) + F_u + Y.\sin\left(\frac{\pi}{iter}\right) \tag{7}$$

where the updated solution to next iteration is indicated as $T\left(Z\left(l+1\right)\right)$, current position is signified as $F_u$, parameter is denoted as $w_g$, current position is indicated as $T\left(Z\left(l\right)\right)$, the exponential factor is represented as $Y$, and the sinusoidal modulation is implied as $\sin\left(\frac{\pi}{iter}\right)$

.

### 3.2 Proposed Trust Computational Model

A decentralized federated learning framework that integrates trust and heterogeneity considerations with blockchain technology provides privacy protection, security, and robust healthcare classification across varied data sources. However, existing methods often struggle with limited privacy, vulnerability to attacks, and poor handling of data heterogeneity across sources. Hence, TrustHet Aware is developed to perform privacy preserved healthcare classification in Blockchain. TrustHet Aware is introduced to ensure privacy-preserving and secured healthcare classification by leveraging blockchain's immutability and decentralized trust. Its core benefit lies in combining heterogeneous model learning with trust evaluation, which enhances both classification accuracy and data integrity across distributed nodes. Here,

**International Journal of Applied Mathematics**
**Volume 38 No. 7s, 2025**
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Heterogeneity-aware Federated learning supports different devices with varying data to work together for improving a shared model while considering these differences. Also, a decentralized model aggregation strategy is adopted. Moreover, trust should be an integral part of the decision-making process and the trust establishment mechanism between the server and nodes is developed by considering direct trust, indirect trust, Attestation trust, Mediation trust, confidence factor, delegation trustworthiness, and Bayesian beta method-based trust. Here, the aggregation is performed using the harmonic concept. At last, aggregation and local updation at the server are updated using Average method.

### 3.2.1 Direct trust

Direct trust [26] refers to an interactive record formed between two entities through firsthand observation without involving a third party. It arises from this direct interaction between node $m$ and node $n$ and is denoted as $E_{mn}$, where node $m$ and node $n$ indicate the respective node indices. Since time intervals between consecutive events follow an exponential distribution, this distribution is used as prior model for interactions between nodes. Considering that future interactions behave similarly to past ones, the direct trust $E$ can be expressed as follows.

$$E_{mn} = \frac{r}{r+s} \tag{8}$$

where the successful iterative behavior of node $m$ is represented as $r$, and the successful iterative behavior of node $n$ is represented as $s$.

### 3.2.2 Indirect trust

When a node is considered unreliable or uncertain, recommendations from third-party nodes become necessary [26]. In such cases, the evaluating node $m$ gathers trust information about node $n$ through their mutual neighboring nodes $a$, collectively denoted as $Z_a$. Node $m$ already possesses prior reputation information regarding these mutual neighbors. To proceed, node $m$ sends out inquiry messages to its neighbors and those that are common to both node $m$ and node $n$ respond by providing their interaction records with node $n$ in the form of $\left(r_{an}, s_{an}\right)$. Based on this information, node $m$ estimates the reputation of node $n$ and is represented as $\left(r_m, s_m\right)$. Importantly, the selection of neighbor nodes is limited to those within one-hop communication range.

$$V_{mn} = \sum_{a=1}^{x} b_a \times B_{mn}^{a} \tag{9}$$

where the indirect trust is represented as $V$, $B_{mn}^{a}$ indicates the recommendations provided by the neighbor node $a$, and the overall received recommendations are signified as $x$. Moreover, the weight of $B_{mn}^{a}$ is denoted as $b_a$.

### 3.2.3 Attestation trust

Received: August 07, 2025 

**International Journal of Applied Mathematics**
**Volume 38 No. 7s, 2025**
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Attestation trust [27] is the trust gained by validating a node's integrity and behavior through formal attestation processes. It confirms that the node functions securely and adheres to expected protocols within the network. This trust is formed using cryptographic proofs and past interaction records. Moreover, the attestation trust is given as,

$$W_{mn}(y) = as(n,y) \Rightarrow ac(m,y) \quad (10)$$

where the trustor is signified as $m$, and the trustee is denoted as $n$, and the corresponding information is indicated as $y$. Moreover, assertion containing information is indicated as $as(n,y)$, and the acceptance of $y$ is true by $m$ is represented as $ac(m,y)$.

### 3.2.4 Mediation trust

Mediation trust [27] is the trust between two nodes with the help of a trusted third party or intermediary. It comes into play when there is no direct trust between the involved nodes. The intermediary provides validated recommendations history to support trust evaluation. It is mathematically expressed as,

$$S_{mn}(y) \equiv ac(n,y) \Rightarrow ac(m,y) \quad (11)$$

Here, if the information $y$ is accepted as true by $n$ then, $m$ also accepts it as true.

### 3.2.5 Self-Confidence Factor

The self-confidence factor [28] helps to reinforce trust based on direct interactions and mitigates the risk of being misled by false or malicious recommendations. The self-confidence factor is denoted as $\rho$ and is defined by the formula:

$$\rho = 1 - \beta^d \quad (12)$$

Here, $d$ represents number of direct interactions between nodes $m$ and $n$, and $\beta$ denotes a parameter specific to the application context ranges between 0 and 1. For number of direct interactions $d$, if the number increases, the weight assigned to direct trust $E$ also increases, which indicates that the node $m$ increasingly relies on its own experience.

### 3.2.6 Conversational Trust

A longer and more balanced exchange between two nodes suggests a higher likelihood of a trust relationship. Furthermore, an increased number of such interactions indicates a stronger connection between the nodes. The initial step involves determining when a conversation is taking place between them [29].

Conversational trust is evaluated based on the set of interactions that are guided by key principles. Trust increases with longer conversations, a higher frequency of exchanges, and balanced participation between both parties. These factors highlight the strength and consistency of the relationship. Although other considerations, such as a decline in communication over time can signal weakening trust and the outlined criteria provide a strong foundational approach for measuring conversational trust. It is expressed as follows,

**International Journal of Applied Mathematics**
**Volume 38 No. 7s, 2025**
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

$$C(F,G)=\sum_{\alpha=1}^{\gamma}\|U_{\alpha}\|.D(U_{\alpha}) \tag{13}$$

where $F,G$ represents two users, measure of balance in conversation is implied as $D(U_{\alpha})$, and the message is indicated as $\alpha$ . Moreover, $D(U_{\alpha})$ is calculated as,

$$D(U_{\alpha})=-\delta\log\delta-(1-\delta)\log(1-\delta) \tag{14}$$

Here, the fraction of messages in conversation is represented as $\delta(\alpha)$.

### 3.2.7 Trust value calculation using Bayesian Beta Method

The Bayesian beta method estimates trust by adjusting the likelihood of cooperation according to previous interactions through beta distributions [30]. Trust is determined by the expected value of this distribution and reflecting the ratio of cooperative to non-cooperative actions. The trust values are calculated using the Bayesian beta method, which is known for its quick and sensitive response to changes in trust metrics. Bayesian beta method calculates the trust using the below expression,

$$K_{mn}=L\left(beta\{\mu_m+1,\upsilon+1\}\right)=\frac{\mu_m+1}{\mu_m+\upsilon+2} \tag{15}$$

Here, $\mu_m$ and $\upsilon_m$ represent counts of cooperative and non-cooperative interactions between nodes $m$ and $n$ .

Then, the total values of trust are expressed as below.

$$X_m=\frac{E_{mn}+V_{mn}+W_{gh}+S_{gh}+\rho+C+K_{mn}}{7} \tag{16}$$

where $E_{mn}$ represents Direct trust, $V_{mn}$ denotes Indirect trust, $W_{gh}$ signifies Attestation trust, $S_{gh}$ implies Mediation trust, $\rho$ indicates Self-confidence factor, $C$ represents Conversational trust, and $K_{mn}$ denotes Trust value.

### 3.3 Aggregation at server

Trust weights from multiple local device are combined at server using harmonic mean technique. This method emphasizes lower trust values and allows them to have a stronger impact on the final trust calculation. As a result, the aggregation produces a more balanced and equitable trust evaluation across all devices. It also prevents high trust scores from disproportionately influencing the overall trust measure.

In trust value aggregation, Harmonic analysis [31] involves breaking down of aggregated trust data into fundamental components to better understand variations and underlying trust patterns.

Harmonic analysis can be expressed as,

**International Journal of Applied Mathematics**
**Volume 38 No. 7s, 2025**
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

$$v(\lambda) = i_0 + \sum_{t=1}^{\varepsilon}\left( i_t \cos\left(\frac{2\pi t\lambda}{k}\right) + j_t \sin\left(\frac{2\pi t\lambda}{k}\right)\right) \quad (17)$$

where, the level of time-series is signified as $i$, number of cycles is denoted as $\varepsilon$, overall count of time-series is implied as $k$ and specific cycle is represented as $t$.

where,

$$i_0 = \frac{1}{k}\sum_{\lambda=1}^{k} v(\lambda) \quad (18)$$

$$i_t = \frac{2}{k}\sum_{\lambda=1}^{k} v(\lambda)\cos\left(\frac{2\pi t\lambda}{k}\right) \quad (19)$$

$$j_t = \frac{2}{k}\sum_{\lambda=1}^{k} v(\lambda)\sin\left(\frac{2\pi t\lambda}{k}\right) \quad (20)$$

Let us assume the values of $k = 2$ and $\varepsilon = 1$, and substituting these values in Eq. (17).

Then, Eq. (17) becomes

$$v(\lambda) = i_0 + i_1 \cos\left(\frac{2\pi\lambda}{2}\right) + j_t \sin\left(\frac{2\pi\lambda}{2}\right) \quad (21)$$

It can be rewritten as,

$$v(\lambda) = i_0 + i_1 \cos(\pi\lambda) + j_t \sin(\pi\lambda) \quad (22)$$

Applying $k = 2$ and $\varepsilon = 1$ in Eq. (18), then it can be written as,

$$i_0 = \frac{1}{2}\sum_{\lambda=1}^{1} v(\lambda) \quad (23)$$

Then, it is written as

$$i_0 = \frac{1}{2}[v_1 + v_2] \quad (24)$$

Applying $k = 2$ and $\varepsilon = 1$ in Eq. (19), then it can be written as,

$$i_1 = \frac{2}{2}\sum_{\lambda=1}^{2} v(\lambda)\cos\left(\frac{2\pi t\lambda}{2}\right) \quad (25)$$

It becomes,

$$i_1 = v_1 \cos\left(\frac{2\pi}{2}\right) + v_2 \cos\left(\frac{2\pi\times 2}{2}\right) \quad (26)$$

It can be written as,

**International Journal of Applied Mathematics**
**Volume 38 No. 7s, 2025**
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

$$i_1 = v_1(-1) + v_2(1) \tag{27}$$

Applying $k = 2$ and $\varepsilon = 1$ in Eq. (20), then it can be written as,

$$j_1 = \frac{2}{2}\sum_{\lambda=1}^{2} v(\lambda)\sin\left(\frac{2\pi t\lambda}{2}\right) \tag{28}$$

It becomes,

$$j_1 = v_1 \sin\left(\frac{2\pi}{2}\right) + v_2 \sin\left(\frac{2\pi \times 2}{2}\right) \tag{29}$$

Then, it can be written as,

$$j_1 = v_1(0) + v_2(0) \tag{30}$$

Then applying Eq. (24), Eq. (27), and Eq. (30) in Eq. (22)

$$v(\lambda) = \frac{1}{2}[v_1 + v_2] + [v_1(-1) + v_2(1)]\cos(\pi\lambda) + [v_1(0) + v_2(0)]\sin(\pi\lambda) \tag{31}$$

It can be written as,

$$v(\lambda) = \frac{1}{2}[v_1 + v_2] + [v_1(-1) + v_2(1)]\cos(\pi\lambda) \tag{32}$$

By representing in time series model, $v(\lambda-1), v(\lambda), v(\lambda+1)$

$$v_1 = v(\lambda-1) \tag{33}$$

$$v_2 = v(\lambda) \tag{34}$$

$$v(\lambda) = v(\lambda+1) \tag{35}$$

By substituting Eq. (33), Eq. (34), and Eq. (35) in Eq. (32), it becomes

$$v(\lambda+1) = \frac{1}{2}[v(\lambda-1) + v(\lambda)] + [v(\lambda-1)(-1) + v(\lambda)(1)]\cos(\pi\lambda) \tag{36}$$

$$v(\lambda+1) = v(\lambda)\left[\frac{1}{2} + \cos(\pi\lambda)\right] + v(\lambda-1)\left[\frac{1}{2} - \cos(\pi\lambda)\right] \tag{37}$$

Let us consider,

$$v(\lambda) = X_m(\lambda) \tag{38}$$

$$v(\lambda+1) = X_m(\lambda+1) \tag{39}$$

$$v(\lambda-1) = X_m(\lambda-1) \tag{40}$$

Then, Eq. (37) can be written as,

Received: August 07, 2025

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

$$X_m(\lambda+1) = X_m(\lambda)\left[\frac{1}{2}+\cos(\pi\lambda)\right] + X_m(\lambda-1)\left[\frac{1}{2}-\cos(\pi\lambda)\right] \quad (41)$$

where, trust value at $\lambda^{th}$ is denoted as $X_m(\lambda)$, trust value at $(\lambda+1)^{th}$ is indicated as $X_m(\lambda+1)$, and trust value at $(\lambda-1)^{th}$ is signified as $X_m(\lambda-1)$.

### 3.4 Applying Trained model on every device node

Calculated average trust weight is shared with each device node and server. This process maintains uniformity in trust assessment across the network. By broadcasting the updated trust values, all nodes remain consistent with the network's trust framework. The server handles the aggregation process while individual devices update their local trust metrics. Such a mechanism enables coordinated and adaptive trust management throughout the system.

## 4. Results and Discussion

Results of TrustHet aware-based FFboA_DHA-Net for classifying Privacy-Preserved Healthcare system are discussed in this part.

### 4.1 Experimental Setup

Developed TrustHet aware-based FFboA_DHA-Net model for classifying Privacy-Preserved Healthcare system is implemented in Python tool.

### 4.2 Dataset Description

The Indian Diabetic Retinopathy Image Dataset (IDRiD) [18] is a detailed retinal image collection designed to reflect the Indian population. It involves precise pixel-level annotations of normal and Diabetic Retinopathy (DR) lesions' anatomical features. Each image is categorized based on severity of DR and presence of Diabetic Macular Edema (DME). This dataset is well-suited for building and testing computer-aided diagnostic systems aimed at early detection of DR.

### 4.3 Experimental Result

Experimental outcome of TrustHet aware-based FFboA_DHA-Net for classifying Privacy-Preserved Healthcare system is portrayed in figure 3. Figure 3 a) shows Input image-1. Figure 3 b) illustrates input image-2. Figure 3 c) demonstrates input image-3, and Figure 3 d) portrays input image-4. Figure 3 e) displays filtered image of image-1. Figure 3 f) demonstrates filtered image of image-2. Figure 3 g) demonstrates filtered image of image-3. Figure 3 h) portrays filtered image of image-4, Figure 3 i) shows segmented image of image-1, Figure 3 j) illustrates segmented image of image-2. Figure 3 k) demonstrates segmented image of image-3. Figure 3 l) portrays segmented image of image-4. Figure 3 m) represents LIFT feature extracted image of image-1. Figure 3 n) illustrates LIFT feature extracted image of image-2. Figure 3 o) displays LIFT feature extracted image of image-3. Figure 3 p) illustrates LIFT feature extracted image of image-4. Figure 3 q) shows Output of image-1 (Normal case). Figure 3 r) displays output of image-2 (Mild case). Figure 3 s) illustrates output of image-3 (Moderate case). Figure 3 t) portrays output of image-4 (Severe case).

Received: August 07, 2025 

**International Journal of Applied Mathematics**
**Volume 38 No. 7s, 2025**
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

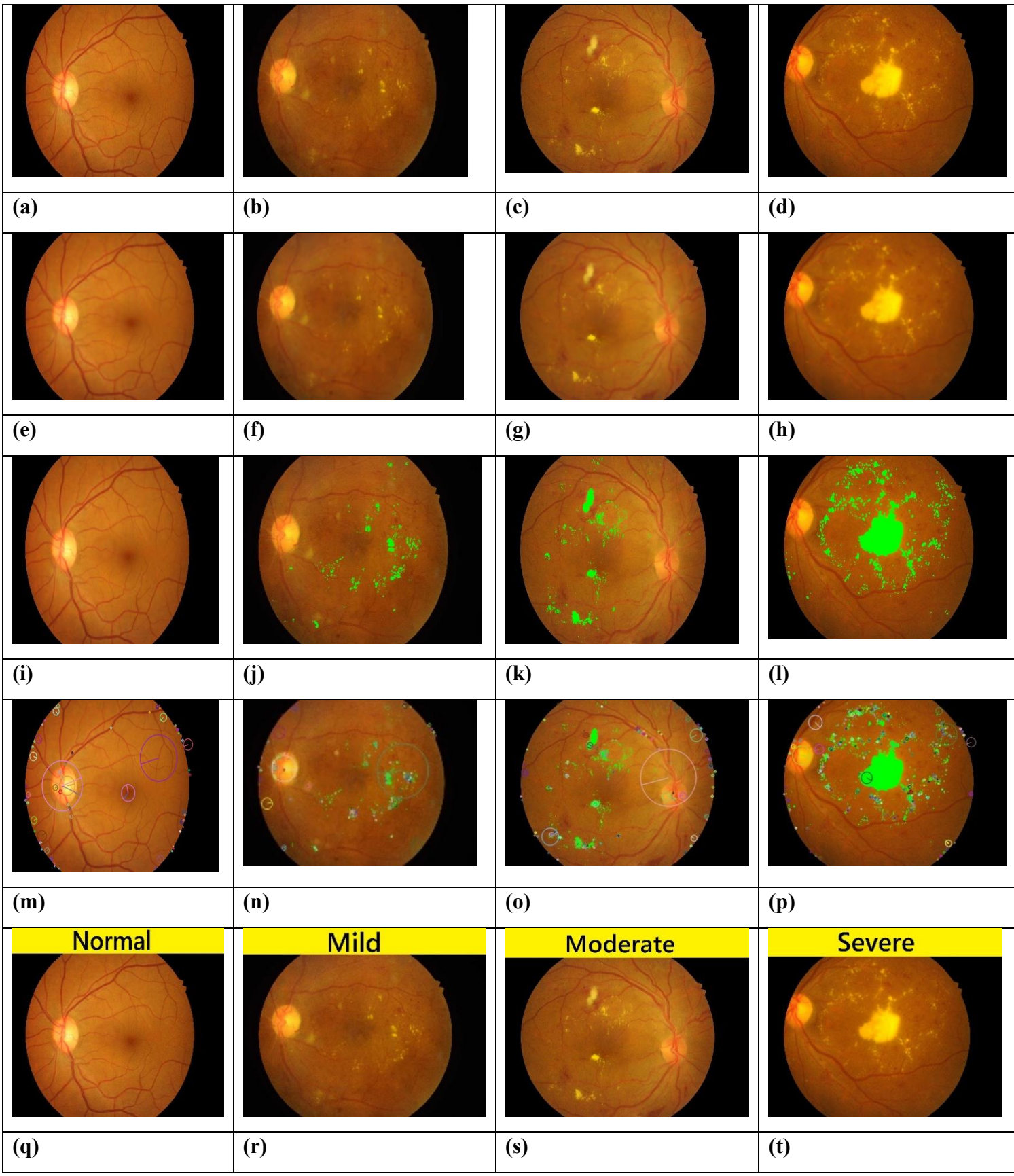



**Figure 3.** Experimental outcome of TrustHet aware-based FFboA_DHA-Net, a) Input image-1, b) Input image-2, c) Input image-3, d) Input image-4, e) Filtered image of image-1, f) Filtered

Volume 38 No. 7s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

image of image-2, g) Filtered image of image-3, h) Filtered image of image-4, i) Segmented image of image-1, j) Segmented image of image-2, k) Segmented image of image-3, l) Segmented image of image-4, m) LIFT feature extracted image of image-1, n) LIFT feature extracted image of image-2, o) LIFT feature extracted image of image-3, p) LIFT feature extracted image of image-4, q) Outcome of image-1 (Normal), r) Outcome of image-2 (Mild), s) Outcome of image-3 (Moderate), t) Outcome of image-4 (Severe)

### 4.4 Evaluation Metrics

Metrics that are used to analyze performance of TrustHet aware-based FFboA_DHA-Net are detailed as follows.

#### 4.4.1 F1-score

The F1-score [32] is the integration of both precision and recall, and is calculated as their harmonic mean which highlights a balance between the two metrics, and is computed as follows,

$$f1score = \frac{2 * Q_{pr} * Q_{re}}{\left(Q_{pr} + Q_{re}\right)} \tag{42}$$

Where $Q_{pr}$ denotes the precision and $Q_{re}$ represents the recall.

#### 4.4.2 Loss Function

Difference between predicted and actual values is defined as loss, where a smaller loss indicates a more accurate and optimal model.

#### 4.4.3 MAP

MAP [33] is the average of the precision values computed for each class, and is calculated as,

$$map = \frac{1}{e}\sum_{q=1}^{e} P_q \tag{43}$$

Here, overall sample is indicated as $e$, and the average precision is denoted by $P_q$.

#### 4.4.4 MSE

MSE [34] measures the average of the squared differences between the predicted and actual values and is computed in Eq. (5).

#### 4.4.5 RMSE

RMSE [34] represents the square root of the mean squared difference between the predicted and actual results, and is expressed as,

$$rmse = \sqrt{\frac{1}{e}\sum_{q=1}^{e}\left[Y_q^{target} - Y_q\right]^2} \tag{44}$$

Received: August 07, 2025 

**International Journal of Applied Mathematics**
**Volume 38 No. 7s, 2025**
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

where overall sample is denoted as $e$, $Y_q^{target}$ signifies targeted classified outcome, and classified outcome is indicated as $Y_q$.

### 4.5 Training Loss

Training loss is a crucial metric used to evaluate the learning efficiency during the training phase by measuring difference between model's predictions and actual target values. Purpose of the training loss graph is to track reduction of this loss over time and aiming for minimal loss to achieve accurate predictions. Figure 4 illustrates the training loss at varying epochs. It shows 0.277 at epoch 0, 0.056 at epoch 20, 0.011 at epoch 40, 0.002 at epoch 60, 0.0005at epoch 80, and 0.0001 at epoch 100.

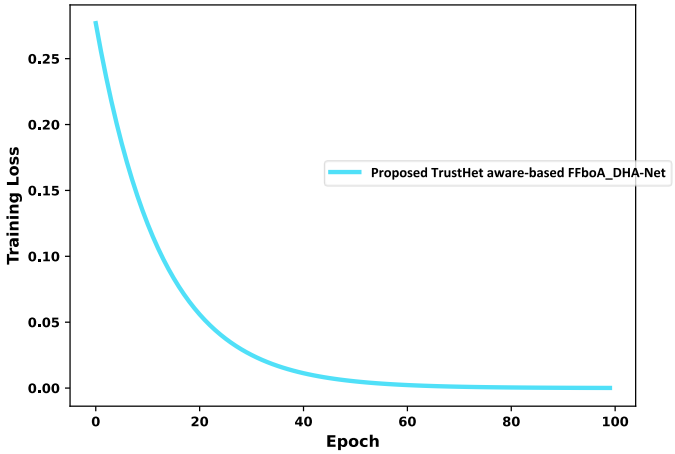



**Figure 4.** Training loss

### 4.6 Comparative Methods

FL-BETS [10], FedViTBloc [11], CapsNet with IELMs [12], DMFL_Net+DenseNet-169 [13], FFbOA_DHA-Net, and AGME_DRNet are the comparative methods that are used to analyze the performance of the developed TrustHet aware-based FFboA_DHA-Net.

### 4.7 Comparative Assessment

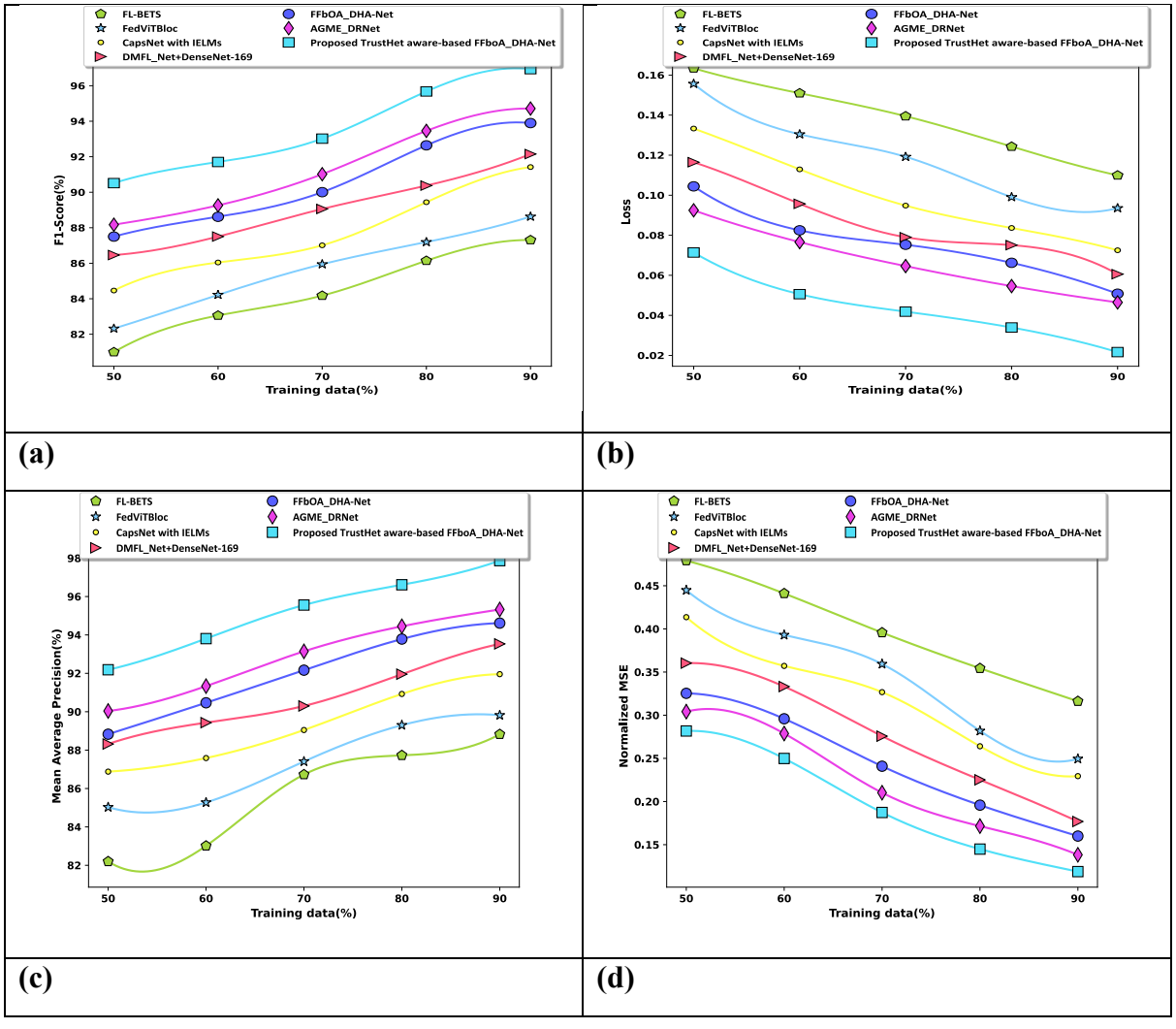
The performance of TrustHet aware-based FFboA_DHA-Net method is analysed by comparing with traditional approaches using metrics by varying time stamps and training data.

#### 4.7.1 Assessment based on Training data

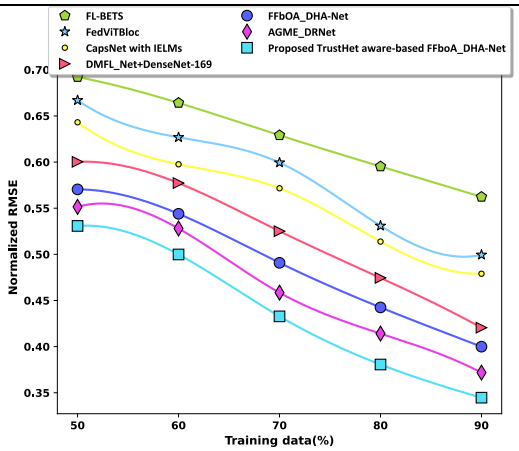
Evaluation of TrustHet aware-based FFboA_DHA-Net while comparing with existing methods like FL-BETS, FedViTBloc, CapsNet with IELMs, DMFL_Net+DenseNet-169, FFbOA_DHA-Net, and AGME_DRNet based on training data using several metrics is portrayed in Figure 4. For further analysis, training data of 90% is considered. In figure 5 a) Assessment of TrustHet aware-based FFboA_DHA-Net in terms of F1-score is portrayed. Here, TrustHet aware-based FFboA_DHA-Net has attained F1-score of 96.933%, while the existing methods have gained the F1-score of 87.309%, 88.626%, 91.418%, 92.151%,

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

93.896%, and 94.714%. The evaluation of TrustHet aware-based FFboA_DHA-Net with respect to Loss function is illustrated in figure 5 b). Traditional approaches have reached loss function of 0.110, 0.094, 0.073, 0.061, 0.051, and 0.046. However, TrustHet aware-based FFboA_DHA-Net has reached the loss function of 0.022. Figure 5 c) portrays evaluation of TrustHet aware-based FFboA_DHA-Net for MAP. Here, 97.870% of MAP is attained by TrustHet aware-based FFboA_DHA-Net while conventional strategies have reached the MAP of 88.826%, 89.818%, 91.957%, 93.534%, 94.616%, and 95.326%. Figure 5 d) demonstrates the assessment of TrustHet aware-based FFboA_DHA-Net for normalized MSE. Here, TrustHet aware-based FFboA_DHA-Net has attained Normalized MSE value of 0.119. However, existing approaches have attained the Normalized MSE value of 0.316, 0.249, 0.229, 0.177, 0.160, and 0.138. Evaluation of TrustHet aware-based FFboA_DHA-Net with respect to Normalized RMSE is illustrated in figure 5 e). Existing approaches have reached Normalized RMSE values of 0.562, 0.499, 0.479, 0.421, 0.400, and 0.372. TrustHet aware-based FFboA_DHA-Net method has reached Normalized RMSE value of 0.345.



**International Journal of Applied Mathematics**
**Volume 38 No. 7s, 2025**
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)




**(e)**

**Figure 5.** Comparative assessment of TrustHet aware-based FFboA_DHA-Net in accordance to Training data, a) F1-score, b) Loss function, c) MAP, d) Normalized MSE, e) Normalized RMSE

### 4.7.2 Assessment based on Time stamp

Figure 6 depicts evaluation of TrustHet aware-based FFboA_DHA-Net comparing with existing methods, like FL-BETS, FedViTBloc, CapsNet with IELMs, DMFL_Net+DenseNet-169, FFbOA_DHA-Net, and AGME_DRNet based on time stamp using various metrics. For further analysis, time stamp of 100 sec is considered. In figure 6 a) depicts the assessment of TrustHet aware-based FFboA_DHA-Net in terms of F1-score. Here, TrustHet aware-based FFboA_DHA-Net has attained F1-score of 96.981%, while the existing methods have gained the F1-score of 88.280%, 90.269%, 91.160%, 92.197%, 93.069%, and 94.525%. Figure 6 b) portrays the evaluation of TrustHet aware-based FFboA_DHA-Net for Loss function. The traditional methods have reached the loss function of 0.105, 0.090, 0.068, 0.062, 0.058, and 0.047. However, TrustHet aware-based FFboA_DHA-Net has attained loss function of 0.020. Figure 6 c) shows evaluation of TrustHet aware-based FFboA_DHA-Net in terms of MAP. Here, TrustHet aware-based FFboA_DHA-Net has 97.817% of MAP, while conventional strategies have reached the MAP of 89.264%, 91.425%, 92.096%, 94.149%, 94.817%, and 95.638%. The assessment of TrustHet aware-based FFboA_DHA-Net for normalized MSE is demonstrated in Figure 6 d). Here, TrustHet aware-based FFboA_DHA-Net has reached normalized MSE value of 0.111. and existing approaches have reached the MSE value of 0.268, 0.218, 0.193, 0.179, 0.157, and 0.140. In figure6 e), evaluation of TrustHet aware-based FFboA_DHA-Net with respect to Normalized RMSE is shown. Conventional approaches have reached the Normalized RMSE values of 0.518, 0.467, 0.439, 0.423, 0.396, and 0.374. Moreover, TrustHet aware-based FFboA_DHA-Net method has reached Normalized RMSE value of 0.333.

**International Journal of Applied Mathematics**
**Volume 38 No. 7s, 2025**
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

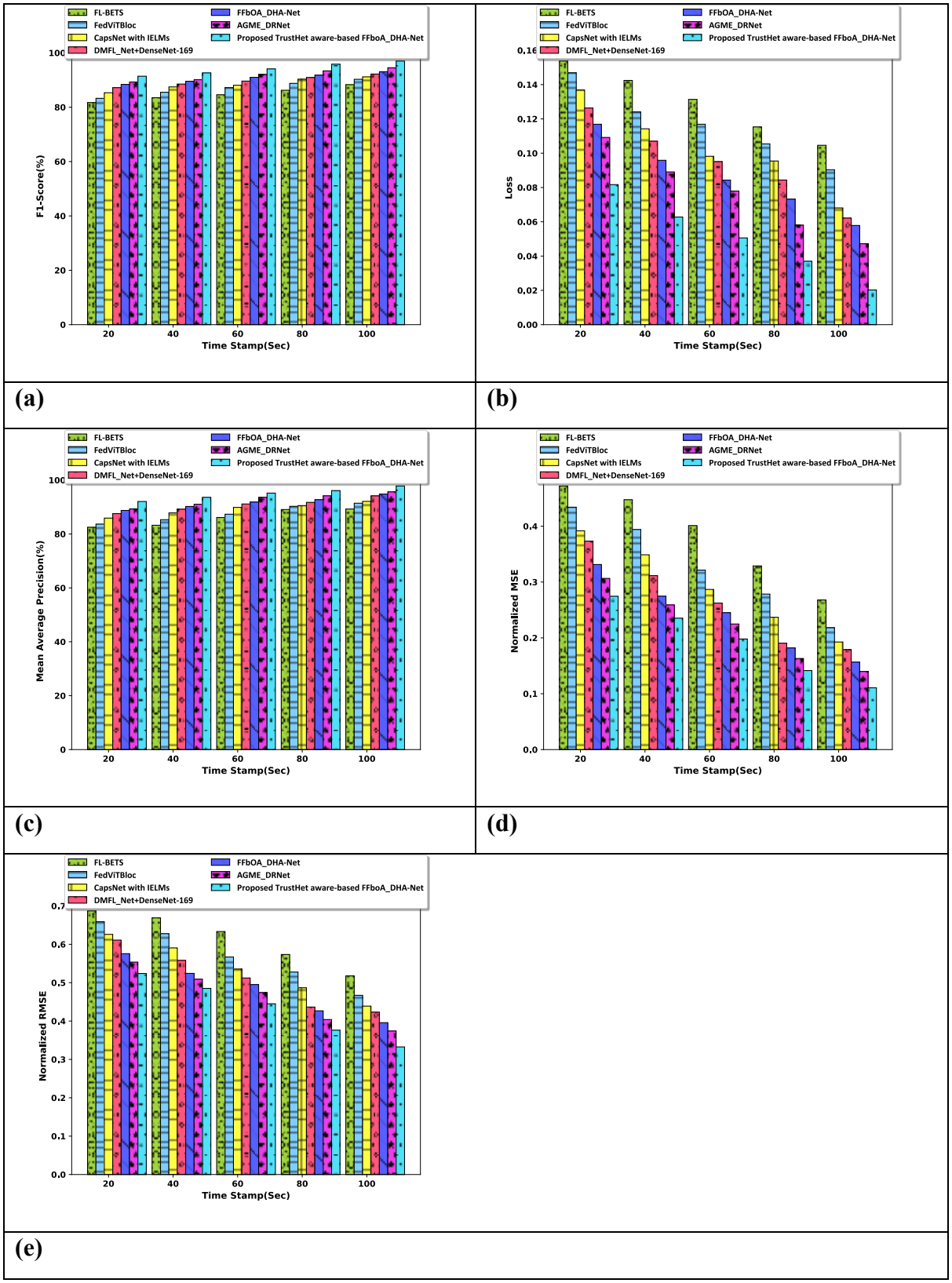



**Figure 6.** Comparative assessment of TrustHet aware-based FFboA_DHA-Net based on Time stamp, a) F1-score, b) Loss function, c) MAP, d) Normalized MSE, e) Normalized RMSE

### 4.8 Comparative Discussion

Received: August 07, 2025

**International Journal of Applied Mathematics**
**Volume 38 No. 7s, 2025**
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Table 1 shows comparative discussion of TrustHet aware-based FFboA_DHA-Net with conventional approaches, like FL-BETS, FedViTBloc, CapsNet with IELMs, DMFL_Net+DenseNet-169, FFbOA_DHA-Net, and AGME_DRNet. Here, the performance of TrustHet aware-based FFboA_DHA-Net is assessed based on metrics, such as F1-score, Loss function, MAP, Normalized MSE, and Normalized RMSE. The best outcomes of TrustHet aware-based FFboA_DHA-Net are attained by varying the time stamp. In terms of F1-score, TrustHet aware-based FFboA_DHA-Net has gained F1-score of 96.981%, while conventional methods have gained F1-score of 88.280%, 90.269%, 91.160%, 92.197%, 93.069%, and 94.525%. It demonstrates a superior precision-recall balance and classification effectiveness. For loss function, traditional methods have reached the loss function of 0.105, 0.090, 0.068, 0.062, 0.058, and 0.047. However, TrustHet aware-based FFboA_DHA-Net has attained the loss function of 0.020. This highlights efficient learning and accurate predictions while validating its effectiveness in privacy preservation. In terms of MAP, TrustHet-aware-based FFboA_DHA-Net achieves a MAP of 97.817%, while conventional strategies have reached MAPs of 89.264%, 91.425%, 92.096%, 94.149%, 94.817%, and 95.638%. This demonstrates its strong ability to accurately detect and classify relevant healthcare data. Moreover, TrustHet aware-based FFboA_DHA-Net has attained the MSE value of 0.111 and existing approaches have reached the MSE value of 0.268, 0.218, 0.193, 0.179, 0.157, and 0.140. This indicates high prediction accuracy and minimal deviation while supporting its effectiveness. For RMSE, conventional approaches have reached the RMSE values of 0.518, 0.467, 0.439, 0.423, 0.396, and 0.374. Moreover, TrustHet aware-based FFboA_DHA-Net method has achieved the RMSE value of 0.333. This shows precise predictions with minimal errors while validating its reliability in privacy-preserving healthcare classification. This reflects the TrustHet aware-based FFboA_DHA-Net model's effective feature fusion and trust heterogeneity awareness in enhancing data reliability and performance.

**Table 1.** Comparative Discussion

| **Variation** | **Metrics** | **FL-BETS** | **FedViTBloc** | **CapsNet with IELMs** | **DMFL_Net +DenseNet-169** | **FFbOA_DHA-Net** | **AGME_DRNet** | **Proposed TrustHet aware-based FFboA_DHA-Net** |
|---|---|---|---|---|---|---|---|---|
| **Training Data 90%** | *F1-score (%)* | 87.309 | 88.626 | 91.418 | 92.151 | 93.896 | 94.714 | 96.933 |
| | *Loss function* | 0.110 | 0.094 | 0.073 | 0.061 | 0.051 | 0.046 | 0.022 |
| | *MAP (%)* | 88.826 | 89.818 | 91.957 | 93.534 | 94.616 | 95.326 | 97.870 |
| | *Normalized MSE* | 0.316 | 0.249 | 0.229 | 0.177 | 0.160 | 0.138 | 0.119 |

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | *Normalized RMSE* | 0.562 | 0.499 | 0.479 | 0.421 | 0.400 | 0.372 | 0.345 |
| **Time Stamp 100 sec** | *F1-score (%)* | 88.280 | 90.269 | 91.160 | 92.197 | 93.069 | 94.525 | **96.981** |
| | *Loss function* | 0.105 | 0.090 | 0.068 | 0.062 | 0.058 | 0.047 | **0.020** |
| | *MAP (%)* | 89.264 | 91.425 | 92.096 | 94.149 | 94.817 | 95.638 | **97.817** |
| | *Normalized MSE* | 0.268 | 0.218 | 0.193 | 0.179 | 0.157 | 0.140 | **0.111** |
| | *Normalized RMSE* | 0.518 | 0.467 | 0.439 | 0.423 | 0.396 | 0.374 | **0.333** |

## 5. Conclusion

Privacy-preserving healthcare data classification uses advanced encryption and secure computing methods to safeguard patient information while categorizing medical records. Current approaches often struggle with trust dynamics and lead to reduced classification performance or weakened privacy protection, thereby limiting their practical value in practical healthcare scenarios. To tackle these challenges, an efficient method named TrustHet aware-based FFboA_DHA-Net for classifying Privacy Preserved Healthcare system in Blockchain is proposed. Initially, local training takes place at local nodes based on local data. Input image undergoes pre-processing, lesion segmentation, and feature extraction in training model. Moreover, classification is performed by employing DHA-Net, and is tuned using FFbOA, a hybrid of FbOA and FC. Heterogeneity-aware Federated Learning enables diverse devices to contribute through decentralized aggregation with trust established between server and nodes, includes trust factors, like Direct, Indirect, Attestation Trust, Mediation trust, Confidence Factor, Conversational Trust, and Bayesian beta method. Aggregation is improved using a harmonic-based approach, which refines both local updates and server-side aggregation using averaging method. The optimal results attained by TrustHet aware-based FFboA_DHA-Net are 96.981% of F1-score, 0.020 of loss function, 97.817% of MAP, 0.111of Normalized MSE, and 0.333 of Normalized RMSE. Future work lies in incorporating adaptive learning and practical trust evaluation for improved healthcare classification and security.

## References

[1] R. Mendes and J. P. Vilela, "“Privacy-preserving data mining: methods, metrics, and applications," *IEEE Access,* vol. 5, pp. 10562-10582, 2017.

[2] K. M. Hossein, E. M. Esmaeil, T. Dargahi and A. khonsari, "Blockchain-based privacy-preserving healthcare architecture," in *In Proceedings of 2019 IEEE Canadian conference of electrical and computer engineering (CCECE), IEEE*, 2019.

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[3] J. Cao, Z. Lian, W. Liu, Z. Zhu and C. Ji, "HADFL: Heterogeneity-aware decentralized federated learning framework," in *In Proceedings of 2021 58th ACM/IEEE Design Automation Conference (DAC), IEEE*, 2021.

[4] A. Tariq, M. A. Serhani, F. M. Sallabi, E. S. Barka, T. Qayyum, H. M. Khater and K. A. Shuaib, "Trustworthy federated learning: A comprehensive review, architecture, key challenges, and future research prospects," *IEEE Open Journal of the Communications Society,* 2024.

[5] J. Liu, C. Chen, Y. Li, L. Sun, Y. Song, J. Zhou, B. Jing and D. Dou, "Enhancing trust and privacy in distributed networks: a comprehensive survey on blockchain-based federated learning," *Knowledge and Information Systems,* vol. 66, no. 8, pp. 4377-4403, 2024.

[6] Y. Zhu, X. Yin, A. W.-C. Liew and H. Tian, "Privacy-Preserving in Medical Image Analysis: A Review of Methods and Applications," *arXiv preprint arXiv:2412.03924,* 2024.

[7] G. A. Kaissis, M. R. Makowski, D. Rückert and R. F. Braren, "Secure, privacy-preserving and federated machine learning in medical imaging," *Nature Machine Intelligence,* vol. 2, no. 6, pp. 305-311, 2020.

[8] A. Vizitiu, C. I. Nit, A. Puiu, C. Suciu and L. M. Itu, "Towards privacy-preserving deep learning based medical imaging applications," in *In Proceedings of 2019 IEEE international symposium on medical measurements and applications (MeMeA), IEEE, pp. 1-6*, 2019.

[9] J. A. Onesimu and J. Karthikeyan, "An efficient privacy-preserving deep learning scheme for medical image analysis," *Journal of Information Technology Management,* vol. 12, pp. 50-67, 2020.

[10] A. lakhan, M. A. Mohammed, J. Nedoma, R. Martinek, P. Tiwari, A. Vidyarthi, A. Alkhayyat and W. Wang, "Federated-learning based privacy preservation and fraud-enabled blockchain IoMT system for healthcare.," *IEEE journal of biomedical and health informatics,* vol. 27, no. 2, pp. 664-672, 2022.

[11] G. C. Amaizu, A. . M. V. V. Sai, S. Bwardwaj, D.-S. Kim, M. Siddula and Y. Li, "FedViTBloc: Secure and privacy-enhanced medical image analysis with federated vision transformer and blockchain," *High-Confidence Computing,,* p. 100302, 2025.

[12] H. Malik, T. Anees, A. Naeem, R. A. Naqvi and W.-K. Loh, "Blockchain-federated and deep-learning-based ensembling of capsule network with incremental extreme learning machines for classification of COVID-19 using CT scans," *Bioengineering,* vol. 10, no. 2, p. 203, 2023.

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[13] H. Malik, A. Naeem, R. A. Naqvi and W.-K. Loh, "A federated learning-based framework for the classification of COVID-19 from multiple chest diseases using X-rays.," *Sensors,* vol. 23, no. 2, p. 743, 2023.

[14] R. Myrzashova, S. H. Alsamhi, A. Hawbani, E. Curry, M. Guizani and X. Wei, "Safeguarding patient data-sharing: Blockchain-enabled federated learning in medical diagnostics," *IEEE Transactions on Sustainable Computing,* 2024.

[15] F. Hu, X. Yang, C. Wu and M. B. Nunes, "Privacy-Preserving Healthcare and Medical Data Collaboration Service System Based on Blockchain and Federated Learning," *Computers, Materials & Continua,* vol. 80, no. 2, 2024.

[16] N. Li, R. Zhang, C. Zhu, W. Ou, W. Han and Q. Zhang, "A data sharing method for remote medical system based on federated distillation learning and consortium blockchain," *Connection Science,* vol. 35, no. 1, p. 2186315, 2023.

[17] Z. F. Zhu, F. Hu, Y. Zhao, B. Chen and X. Tan, ""“A Secure and Fair Federated Learning Framework Based on Consensus Incentive Mechanism," *Mathematics,* vol. 12, no. 19, p. 3068, 2024.

[18] "Indian Diabetic Retinopathy Image Dataset (IDRiD)dataset," [Online]. Available: https://ieee-dataport.org/open-access/indian-diabetic-retinopathy-image-dataset-idrid. [Accessed June 2025].

[19] E. Srinivasan and D. Ebenezer, "New nonlinear filtering strategies for eliminating short and long tailed noise in images with edge preservation properties," *International Journal of Information and Communication Engineering,* vol. 4, no. 3, pp. 175-181, 2008.

[20] S. Iqbal, T. M. Khan, S. S. Naqvi, A. Naveed and E. Meijering, "TBConvL-Net: A hybrid deep learning architecture for robust medical image segmentation," *Pattern Recognition,* vol. 158, p. 111028, 2025.

[21] K. M. Yi, E. Trulls, V. Lepetit and P. Fua, "Lift: Learned invariant feature transform.," in *In Computer Vision–ECCV 2016: 14th European Conference, Amsterdam, The Netherlands, October 11-14, 2016, Proceedings, Part VI 14 (pp. 467-483). Springer International Publishing.*, Amsterdam, 2016.

[22] V. Lessa and M. Marengoni, "Applying artificial neural network for the classification of breast cancer using infrared thermographic images," in *In International conference on computer vision and graphics (pp. 429-438). Cham: Springer International Publishing.*, 2016.

[23] M. Waqas, A. Ahmed, T. Maul and I. Y. Liao, "Enhancing breast cancer histopathological image classification using attention-based high order covariance pooling," *Neural Computing and Applications,* vol. 36, no. 36, pp. 23275-23293, 2024.

Received: August 07, 2025 

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[24] E.-S. M. El-Kenawy, F. H. Rizk, A. M. Zaki, M. E. Mohamed, A. Ibrahim, A. A. Abdelhamid, N. Khodadadi, E. M. Almetwally and M. M. Eid, "Football optimization algorithm (fboa): A novel metaheuristic inspired by team strategy dynamics," *J. Artif. Intell. Metaheuristics,* vol. 8, no. 1, pp. 21-38, 2024.

[25] . P. Bhaladhare and D. Jinwala, "A clustering approach for the l-diversity model in privacy preserving data mining using fractional calculus-bacterial foraging optimization algorithm.," *Advances in Computer Engineering,* vol. 2014, no. 1, p. 396529, 2014.

[26] J. Huang, J. Zhao and N. Xiong, "An effective exponential-based trust and reputation evaluation system in wireless sensor networks.," *IEEE Access,* vol. 7, pp. 33859-33869, 2019.

[27] H. Gomi, "Authentication trust metric and assessment for federated identity management systems.," *IEICE TRANSACTIONS on Information and Systems,* vol. 95, no. 1, pp. 29-37, 2012.

[28] "A credible Bayesian-based trust management scheme for wireless sensor networks," *International Journal of Distributed Sensor Networks,* vol. 11, no. 11, p. 678926, 2015.

[29] "Measuring behavioral trust in social networks," in *In 2010 IEEE international conference on intelligence and security informatics (pp. 150-152). IEEE*, 2010.

[30] L. Wang, K. Petrova and M. L. Yang, "Trust Models in Wireless Sensor Networks for Defending Against Denial-of-Service Attacks: A Literature Review.," *Applied Sciences,* vol. 15, no. 6, p. 3075, 2025.

[31] E. Damsleth and Spjotvoll, "Estimation of trigonometric components in time series.," *Journal of the American Statistical Association,* vol. 77, no. 378, pp. 381-387, 1982.

[32] R. Devi D and Sasikala S., "Ensemble incremental deep multiple layer perceptron model–sentiment analysis application," *International Journal of Web Information Systems,* vol. 17, no. 6, pp. 714-727, 2021.

[33] K. Li, Z. Huang, Y.-C. Cheng and C.-H. Lee, "A maximal figure-of-merit learning approach to maximizing mean average precision with deep neural network based classifiers.," in *In 2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP) (pp. 4503-4507)*, 2014.

[34] O. E. Obisesan, "Machine Learning Models for Prediction of Meteorological Variables for Weather Forecasting," *Int. J. Environ. Clim. Change,* vol. 14, no. 1, pp. 234-252, 2024.

Received: August 07, 2025 

**International Journal of Applied Mathematics**
**Volume 38 No. 7s, 2025**
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Received: August 07, 2025 